

# FALCON PREVENT NEXT-GENERATION ANTIVIRUS

Ideal AV replacement combines the most effective prevention technologies with full attack visibility and simplicity

## INDUSTRY-RECOGNIZED LEGACY AV REPLACEMENT

For organizations struggling with the ineffectiveness and complexity of legacy antivirus solutions, CrowdStrike® Falcon Prevent™ is here to help. Falcon Prevent delivers superior protection with a single lightweight agent that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. Even the largest organizations can be up and running in minutes with Falcon Prevent.

**Certified to replace legacy antivirus products** — Independent testing at AV-Comparatives and SE Labs has certified Falcon Prevent's antivirus capabilities. Falcon Prevent has also been validated for PCI, HIPAA, NIST and FFIEC regulatory requirements.

Named a leader in the 2019 Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) — In addition to being positioned in the Leaders Quadrant, CrowdStrike is furthest for "completeness of vision," which includes Gartner criteria such as innovation, marketing and product strategies, vertical industry and geographic strategies, as well as the validity of the business model as a whole.

### KEY BENEFITS

Prevents all types of attacks

Simplifies operations with signatureless protection and software-as-a-service (SaaS) delivery

Deploys in minutes and immediately begins protecting your endpoints

Replaces legacy antivirus quickly and confidently

Operates seamlessly alongside AV as you migrate to simplify transition

Provides full attack visibility



## CrowdStrike Products

### FALCON PREVENT NEXT-GENERATION ANTIVIRUS

## KEY CAPABILITIES

### STATE-OF-THE-ART PREVENTION

Falcon Prevent protects endpoints against all types of attacks, from commodity malware to sophisticated attacks — even when offline.

- Machine learning and artificial intelligence prevent known and unknown malware, adware and potentially unwanted programs (PUPs)
- AI-powered indicators of attack (IOAs), script control and high-performance memory scanning identify malicious behaviors and prevent fileless attacks and ransomware
- Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities
- Detect and quarantine on write stops and isolates malicious files when they first appear on a host
- Industry-leading threat intelligence is built into the CrowdStrike Security Cloud to actively block malicious activity
- Custom IOAs enable you to define unique behaviors to block
- Quarantine captures blocked files and allows access for investigation
- Script-based execution monitoring inspects and blocks malicious Microsoft Office macros
- Sensor tampering protection stops user or process attempts to manipulate or disable the CrowdStrike Falcon® sensor

### INTEGRATED THREAT INTELLIGENCE

- Automatically determine the scope and impact of threats found in your environment
- Find out if you are targeted, who is targeting you and how to prepare and get ahead
- Use Falcon Prevent integrated with CrowdStrike Falcon Intelligence to:
  - Fully understand the threats in your environment and what to do about them
  - Access malware research and analysis at your fingertips
  - Easily prioritize responses with threat severity assessment
  - Immediately get recovery steps and resolve incidents with in-depth threat analysis

### FULL ATTACK VISIBILITY AT A GLANCE

For unparalleled alert context and visibility, Falcon Prevent:

- Provides details, context and history for every alert
- Unravels an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data
- Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections
- Keeps detection details for 90 days

### SIMPLE, FAST AND LIGHTWEIGHT

Purpose-built in the cloud with a single lightweight-agent architecture, Falcon eliminates complexity and simplifies endpoint security operations.

- Falcon operates without constant signature updates, complex integrations or on-premises equipment
- The lightweight agent bears little impact on endpoints, from initial install to day-to-day use — no reboot is required after installation
- Minimal CPU overhead restores system performance and end-user productivity
- Falcon enables the industry's fastest deployment and instant operationalization — without requiring a reboot after installation
- It is automatically kept up to date with cloud-native architecture and SaaS delivery
- Falcon provides broad platform support across an organization's entire estate of endpoints
- Automated IOA remediation streamlines the removal of artifacts that may lead to reinfection

GARTNER is a registered trademark and service mark of Gartner and Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

## FALCON PREVENT: THE EASIEST AV REPLACEMENT

Better protection

Fast and easy deployment

Optimal performance

Reduced complexity

## ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more:  
<https://www.crowdstrike.com/>

Follow us: [Blog](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

Start a free trial today:  
<https://www.crowdstrike.com/free-trial-guide/>

© 2023 CrowdStrike, Inc. All rights reserved. CrowdStrike, the Falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are marks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.

Start Free Trial  
of Next-Gen AV

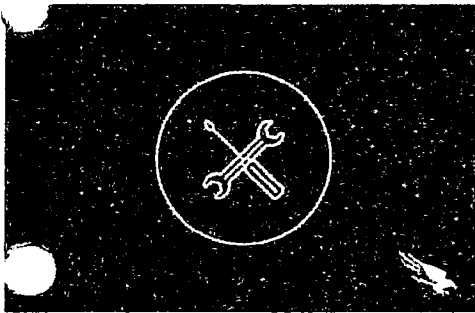
Learn more at [www.crowdstrike.com](http://www.crowdstrike.com)

[BACK TO TECH CENTER](#)

---

# How to Consume Threat Feeds

October 30, 2020   Ted Pan   Tech Center



## Introduction

As part of the CrowdStrike API, the "Custom IOC APIs" allows you to retrieve, upload, update, search, and delete custom indicators of Compromise (IOCs) that you want CrowdStrike to identify.

With the ability to upload IOCs to the endpoints can automatically detect and prevent attacks identified by the indicators provided from a threat feed.

## Prerequisites

To get started with the CrowdStrike API, you'll want to first define the API client and set its scope. Refer to this [guide to getting access](#) to the CrowdStrike API for setting up a new API client key. For the new API client, make sure the scope includes read and write access for IOCs (Indicators of Compromise).

- [Get API Key](#)
- [API Scope](#)
- [API Client](#)
- [API Client Key](#)
- [API Client Secret](#)



# FALCON SIEM CONNECTOR

Leverage Falcon Host data in any SIEM

## Simplify and automate consumption of Falcon Host data into your SIEM

Organizations need to collect and archive log data for purposes ranging from regulatory compliance, to log management, to the aggregation of events from multiple security products. SIEMs (Security Information and Event Management) have become the tool of choice to gather these type of data. But the disparity of log formats and number of connectivity methods between a SIEM and its data sources can make data collection arduous and lengthy for SIEM users.

### OPTIMIZED SECURITY EVENT GATHERING ON THE ENDPOINT

Using Falcon Host in conjunction with the Falcon SIEM Connector offers a fast, simple and reliable way to optimize the collection of relevant security events across hundreds of thousands endpoints. The lightweight Falcon Host Sensor will perform the otherwise hard work of collecting the data from distributed endpoints with no additional infrastructure deployment. Falcon Host Sensors will send that data from your environment into the Cloud. Then, the Falcon SIEM Connector will seamlessly pull that data from the Cloud to your SIEM.

### SIMPLE AND AUTOMATED DATA CONSUMPTION

The Falcon SIEM Connector streamlines and automates the process of gathering Falcon Host data into SIEMs. Instead of having to write custom connectors, customers can now simply deploy and configure the Falcon SIEM Connector to securely retrieve their Falcon Host data from the Cloud and add them into their SIEM.

The Falcon SIEM Connector automatically connects to the CrowdStrike Cloud and normalizes the data in formats that are immediately usable by SIEMs: JSON, Syslog, CEF (common event format) or LEEF (log event extended format).



# CrowdStrike App



**Latest version 2.5.1**  
 May 16, 2018  
 100% Upvotes

**Compatibility**  
 Splunk Enterprise, Splunk Cloud, Splunk Cloud Service, Splunk Cloud for AWS, Splunk Cloud for Azure

**Rating**  
 5 ★★★★★  
 100% Upvotes

**Support**  
 See the Splunk Support Center for more information.

- Summary
- Details
- Installation
- Troubleshooting
- Contact
- Version History

The CrowdStrike Falcon platform is a cloud-based endpoint protection and incident response solution. It provides comprehensive protection for endpoints, servers, and mobile devices. The platform uses machine learning and behavioral analysis to detect and prevent threats in real-time. It also offers a centralized console for managing and responding to incidents across the entire organization.

- Categories
- Created by
- Type
- Downloads
- Featured in Collection
- License
- Splunk Answers
- Resources

**COMPANY**  
 About Splunk  
 Careers  
 Customer Support  
 Legal Notices  
 Newsroom  
 Partners

**PRODUCTS**  
 Fire, Threat & Detection  
 Pricing  
 View All Products  
  
**SPLUNK SITES**  
 China

**CONTACT SPLUNK**  
 Contact Sales  
 Contact Support  
  
**SPLUNK MOBILE**

*Handwritten signature or mark*

# FALCON PREVENT NEXT-GENERATION ANTIVIRUS

Ideal AV replacement combines the most effective prevention technologies with full attack visibility and simplicity

## INDUSTRY-RECOGNIZED LEGACY AV REPLACEMENT

For organizations struggling with the ineffectiveness and complexity of legacy antivirus solutions, CrowdStrike® Falcon Prevent™ is here to help. Falcon Prevent delivers superior protection with a single lightweight agent that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. Even the largest organizations can be up and running in minutes with Falcon Prevent.

**Certified to replace legacy antivirus products** — Independent testing at AV-Comparatives and SE Labs has certified Falcon Prevent's antivirus capabilities. Falcon Prevent has also been validated for PCI, HIPAA, NIST and FFIEC regulatory requirements.

Named a **Leader in the 2021 Gartner Magic Quadrant for Endpoint Protection Platforms (EPP)** — In addition to being positioned in the Leaders' Quadrant, CrowdStrike is furthest for "completeness of vision," which includes Gartner criteria such as current and future market direction, innovation, customer needs, and competitive forces and how well they map to Gartner's view of the market.

### KEY BENEFITS

Prevents all types of attacks

Simplifies operations with signatureless protection and software-as-a-service (SaaS) delivery

Deploys in minutes and immediately begins protecting your endpoints

Replaces legacy antivirus quickly and confidently

Operates seamlessly alongside antivirus as you migrate to simplify transition

Provides full attack visibility

## CrowdStrike Products

### FALCON PREVENT NEXT-GENERATION ANTIVIRUS

## KEY CAPABILITIES

### STATE-OF-THE-ART PREVENTION

Falcon Prevent protects endpoints against all types of attacks, from commodity malware to sophisticated attacks — even when offline.

- Machine learning and artificial intelligence prevent known and unknown malware, adware and potentially unwanted programs (PUPs)
- Behavior-based indicators of attack (IOAs) prevent sophisticated attacks, including ransomware and fileless and malware-free attacks
- Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities
- Detect and quarantine on write stops and isolates malicious files when they first appear on a host
- Threat intelligence prevention blocks activities known to be malicious
- Custom IOAs enable you to define unique behaviors to block
- Quarantine captures blocked files and allows access for investigation
- Script-based execution monitoring inspects and blocks malicious Microsoft Office macros
- Sensor tampering protection stops user or process attempts to manipulate or disable the CrowdStrike Falcon® sensor

### INTEGRATED THREAT INTELLIGENCE

- Automatically determine the scope and impact of threats found in your environment
- Find out if you are targeted, who is targeting you and how to prepare and get ahead
- Use Falcon Prevent integrated with CrowdStrike Falcon X™ to:
  - Fully understand the threats in your environment and what to do about them
  - Access malware research and analysis at your fingertips
  - Easily prioritize responses with threat severity assessment
  - Immediately get recovery steps and resolve incidents with in-depth threat analysis

### FULL ATTACK VISIBILITY AT A GLANCE

For unparalleled alert context and visibility, Falcon Prevent:

- Provides details, context and history for every alert
- Unravels an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data
- Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections
- Keeps detection details for 90 days

### SIMPLE, FAST AND LIGHTWEIGHT

The cloud-native CrowdStrike Falcon platform and lightweight Falcon agent eliminate complexity and simplify endpoint security operations.

- Falcon operates without constant signature updates, complex integrations or on-premises equipment
- The lightweight agent bears little impact on endpoints, from initial install to day-to-day use — no reboot is required after installation
- Minimal CPU overhead restores system performance and end-user productivity
- It works on Day One, deploys in minutes and is immediately operational
- It is automatically kept up to date with cloud-native architecture and SaaS delivery
- Falcon provides broad platform support including Windows, Windows Server, macOS and Linux
- Automated IOA remediation streamlines the removal of artifacts that may lead to reinfection

## FALCON PREVENT: THE EASIEST AV REPLACEMENT

Better protection

Fast and easy deployment

Optimal performance

Reduced complexity

## ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates millions of endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

## Start Free Trial of Next-Gen AV

Learn more at [www.crowdstrike.com](http://www.crowdstrike.com)

© 2021 CrowdStrike, Inc. All rights reserved.

**DISCLAIMER:** Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

# FALCON PREVENT NEXT-GENERATION ANTIVIRUS

Ideal AV replacement combines the most effective prevention technologies with full attack visibility and simplicity

## INDUSTRY-RECOGNIZED LEGACY AV REPLACEMENT

For organizations struggling with the ineffectiveness and complexity of legacy antivirus solutions, CrowdStrike® Falcon Prevent™ is here to help. Falcon Prevent delivers superior protection with a single lightweight agent that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. Even the largest organizations can be up and running in minutes with Falcon Prevent.

**Certified to replace legacy antivirus products** — Independent testing at AV-Comparatives and SE Labs has certified Falcon Prevent's antivirus capabilities. Falcon Prevent has also been validated for PCI, HIPAA, NIST and FFIEC regulatory requirements.

**Named a leader in the 2019 Gartner Magic Quadrant for Endpoint Protection Platforms (EPP)** — In addition to being positioned in the Leaders Quadrant, CrowdStrike is furthest for "completeness of vision," which includes Gartner criteria such as innovation, marketing and product strategies, vertical industry and geographic strategies, as well as the validity of the business model as a whole.

## KEY BENEFITS

Prevents all types of attacks

Simplifies operations with signatureless protection and software-as-a-service (SaaS) delivery

Deploys in minutes and immediately begins protecting your endpoints

Replaces legacy antivirus quickly and confidently

Operates seamlessly alongside AV as you migrate to simplify transition

Provides full attack visibility





## CrowdStrike Products

### FALCON PREVENT NEXT-GENERATION ANTIVIRUS

## KEY CAPABILITIES

### STATE-OF-THE-ART PREVENTION

Falcon Prevent protects endpoints against all types of attacks, from commodity malware to sophisticated attacks — even when offline.

- Machine learning and artificial intelligence prevent known and unknown malware, adware and potentially unwanted programs (PUPs)
- Behavior-based indicators of attack (IOAs) prevent sophisticated attacks, including ransomware and fileless and malware-free attacks
- Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities
- Detect and quarantine on write stops and isolates malicious files when they first appear on a host
- Threat intelligence prevention blocks activities known to be malicious
- Custom IOAs enable you to define unique behaviors to block
- Quarantine captures blocked files and allows access for investigation
- Script-based execution monitoring inspects and blocks malicious Microsoft Office macros
- Sensor tampering protection stops user or process attempts to manipulate or disable the CrowdStrike Falcon® sensor

### INTEGRATED THREAT INTELLIGENCE

- Automatically determine the scope and impact of threats found in your environment
- Find out if you are targeted, who is targeting you and how to prepare and get ahead
- Use Falcon Prevent integrated with CrowdStrike Falcon X™ to:
  - Fully understand the threats in your environment and what to do about them
  - Access malware research and analysis at your fingertips
  - Easily prioritize responses with threat severity assessment
  - Immediately get recovery steps and resolve incidents with in-depth threat analysis

### FULL ATTACK VISIBILITY AT A GLANCE

For unparalleled alert context and visibility, Falcon Prevent:

- Provides details, context and history for every alert
- Unravels an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data
- Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections
- Keeps detection details for 90 days

### SIMPLE, FAST AND LIGHTWEIGHT

The cloud-native CrowdStrike Falcon platform and lightweight Falcon agent eliminate complexity and simplify endpoint security operations.

- Falcon operates without constant signature updates, complex integrations or on-premises equipment
- The lightweight agent bears little impact on endpoints, from initial install to day-to-day use — no reboot is required after installation
- Minimal CPU overhead restores system performance and end-user productivity
- It works on Day One, deploys in minutes and is immediately operational
- It is automatically kept up to date with cloud-native architecture and SaaS delivery
- Falcon provides broad platform support including Windows, Windows Server, macOS and Linux
- Automated IOA remediation streamlines the removal of artifacts that may lead to reinfection

**DISCLAIMER:** Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

**Start Free Trial  
of Next-Gen AV**

Learn more at [www.crowdstrike.com](http://www.crowdstrike.com)

© 2021 CrowdStrike, Inc. All rights reserved.

## FALCON PREVENT: THE EASIEST AV REPLACEMENT

Better protection

Fast and easy deployment

Optimal performance

Reduced complexity

## ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates millions of endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

# FALCON PREVENT NEXT-GENERATION ANTIVIRUS

Ideal AV replacement combines the most effective prevention technologies with full attack visibility and simplicity

## INDUSTRY-RECOGNIZED LEGACY AV REPLACEMENT

For organizations struggling with the ineffectiveness and complexity of legacy antivirus solutions, CrowdStrike® Falcon Prevent™ is here to help. Falcon Prevent delivers superior protection with a single lightweight agent that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. Even the largest organizations can be up and running in minutes with Falcon Prevent.

**Certified to replace legacy antivirus products** — Independent testing at AV-Comparatives and SE Labs has certified Falcon Prevent's antivirus capabilities. Falcon Prevent has also been validated for PCI, HIPAA, NIST and FFIEC regulatory requirements.

**Named a Leader in the 2021 Gartner Magic Quadrant for Endpoint Protection Platforms (EPP)** — In addition to being positioned in the Leaders' Quadrant, CrowdStrike is furthest for "completeness of vision," which includes Gartner criteria such as current and future market direction, innovation, customer needs, and competitive forces and how well they map to Gartner's view of the market.

### KEY BENEFITS

Prevents all types of attacks

Simplifies operations with signatureless protection and software-as-a-service (SaaS) delivery

Deploys in minutes and immediately begins protecting your endpoints

Replaces legacy antivirus quickly and confidently

Operates seamlessly alongside antivirus as you migrate to simplify transition

Provides full attack visibility

## CrowdStrike Products

FALCON PREVENT NEXT-GENERATION ANTIVIRUS

# KEY CAPABILITIES

## STATE-OF-THE-ART PREVENTION

Falcon Prevent protects endpoints against all types of attacks, from commodity malware to sophisticated attacks — even when offline.

- Machine learning and artificial intelligence prevent known and unknown malware, adware and potentially unwanted programs (PUPs)
- Behavior-based indicators of attack (IOAs) prevent sophisticated attacks, including ransomware and fileless and malware-free attacks
- Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities
- Detect and quarantine on write stops and isolates malicious files when they first appear on a host
- Threat intelligence prevention blocks activities known to be malicious
- Custom IOAs enable you to define unique behaviors to block
- Quarantine captures blocked files and allows access for investigation
- Script-based execution monitoring inspects and blocks malicious Microsoft Office macros
- Sensor tampering protection stops user or process attempts to manipulate or disable the CrowdStrike Falcon® sensor

## INTEGRATED THREAT INTELLIGENCE

- Automatically determine the scope and impact of threats found in your environment
- Find out if you are targeted, who is targeting you and how to prepare and get ahead
- Use Falcon Prevent integrated with CrowdStrike Falcon X™ to:
  - Fully understand the threats in your environment and what to do about them
  - Access malware research and analysis at your fingertips
  - Easily prioritize responses with threat severity assessment
  - Immediately get recovery steps and resolve incidents with in-depth threat analysis

## FULL ATTACK VISIBILITY AT A GLANCE

For unparalleled alert context and visibility, Falcon Prevent:

- Provides details, context and history for every alert
- Unravels an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data
- Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK<sup>™</sup>) framework for quick understanding of even the most complex detections
- Keeps detection details for 90 days

## SIMPLE, FAST AND LIGHTWEIGHT

The cloud-native CrowdStrike Falcon platform and lightweight Falcon agent eliminate complexity and simplify endpoint security operations.

- Falcon operates without constant signature updates, complex integrations or on-premises equipment
- The lightweight agent bears little impact on endpoints, from initial install to day-to-day use — no reboot is required after installation
- Minimal CPU overhead restores system performance and end-user productivity
- It works on Day One, deploys in minutes and is immediately operational
- It is automatically kept up to date with cloud-native architecture and SaaS delivery
- Falcon provides broad platform support including Windows, Windows Server, macOS and Linux
- Automated IOA remediation streamlines the removal of artifacts that may lead to reinfection

## FALCON PREVENT: THE EASIEST AV REPLACEMENT

Better protection

Fast and easy deployment

Optimal performance

Reduced complexity

## ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates trillions of endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Start Free Trial  
of Next-Gen AV

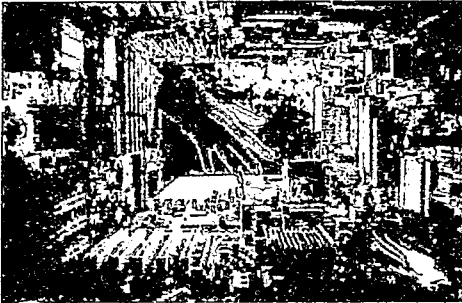
Learn more at [www.crowdstrike.com](http://www.crowdstrike.com)

© 2021 CrowdStrike, Inc. All rights reserved.

**DISCLAIMER:** Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

# CrowdStrike Falcon®: First Endpoint Protection to Integrate Firmware Attack Detection Capability

May 1, 2019 Alex Johnson Endpoint & Cloud Security



Today's endpoint security solutions have been designed primarily to look at the local operating system (OS) and the applications that reside on top of it, remaining blind to computing layers below the OS. This week, CrowdStrike® becomes the first endpoint protection solution provider to integrate firmware attack detection capability, shining a bright light into one of the last remaining dark corners of the modern PC: the BIOS.

As security technologies have become more sophisticated, there are fewer places for adversaries to hide. Technologies such as endpoint detection and response (EDR), machine learning and behavioral detection have greatly enhanced the visibility and awareness organizations have, exposing intrusion techniques that were previously hidden and stopping attacks that would have resulted in a breach. As a result of these advanced defenses, attackers are continuously driven to the fringes, forcing them to hunt for new avenues of infiltration. The BIOS has emerged as a new and unique avenue of attack.

## Why protect the BIOS?

The BIOS (basic input/output system) is firmware that resides in the computer platform itself and runs while a computer boots up, before the operating system is started. BIOS represents a tempting target for attackers for a number of reasons.

### The BIOS Can Enable Persistence

The BIOS of an endpoint represents a highly privileged execution environment, and any vulnerability or malware in the BIOS have serious implications, potentially allowing an attacker to gain full control over all system resources. The BIOS exists well below the OS, ensuring that a successful attack will persist beyond reboots, disk wipes and reimaging. To make matters more complicated, BIOS is seldom patched in most organizations, and known vulnerabilities often remain for years after they are disclosed.

### Standard Security Tools Are Blind to BIOS Attacks

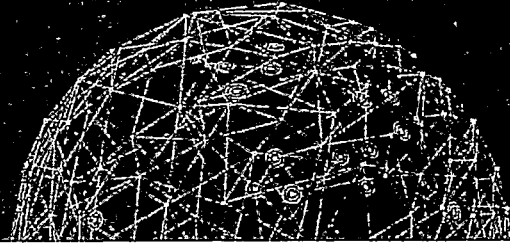
Most of today's security tools are not capable of delivering the visibility that organizations need to detect and thwart BIOS attacks. Typical endpoint security tools provide visibility into user mode, and perhaps the kernel as well. However, the BIOS' position below the operating system means that its contents are not visible to traditional security monitoring tools. In addition, standard security assessment tools such as vulnerability scanners do not provide visibility into BIOS vulnerabilities or configuration.

BIOS and other types of firmware represent a massive exposure, in an area where organizations have very little visibility. This is exactly the type of gap that modern adversaries look to exploit in targeted attacks. The best example of a real-world adversary taking advantage of this visibility gap came to light in September 2018, when it was reported that the adversary



# PREVENTING MALWARE AND BEYOND

## The Power of Falcon Host







### Why Prevention Matters?

As the security industry and its customers have learned the hard way, prevention is not 100 percent effective. Still, prevention adds tremendous value in weeding out the obvious, allowing security teams to focus their efforts and resources on what truly requires their attention. This is why Falcon Host includes the most powerful prevention features designed to stop malware, and in a much broader scope, to stop breaches.

### What Prevention Capabilities Does Falcon Host Provide?

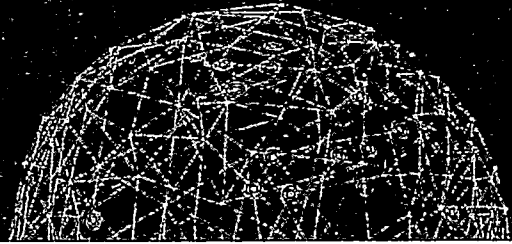
Falcon Host offers prevention against malware. But it expands beyond just malware protection by also offering prevention against advanced targeted attacks and attacks that do not use malware, filling the wide gap left by solutions that primarily focus on malware. Falcon Host uses the right detection and prevention feature at the right time to prevent breaches across the entire attack continuum.

Attack Continuum	 <b>File Based Detection</b> Signature/Traditional AV File Whitelisting File Reputation	 <b>Exploit Blocking</b> Host Intrusion Prevent Appliance Sandbox	 <b>Other Detection</b> IOC detection Forensics SIEM correlation	 <b>Falcon Host*</b> Machine Learning Exploit Blocking Whitelisting Indicators of Attack
<b>ATTACK STARTS</b>				
DELIVERY	•		•	•
INITIAL BEACH HEAD	•			•
<b>ATTACK UNFOLDS</b>				
ESTABLISH PERSISTENCE			•	•
CREDENTIAL THEFT/PRIVILEGE ESCALATION			•	•
LATERAL MOVEMENT/EXPLORATION				•
<b>FINAL OBJECTIVES</b>				
E.G. DATA EXFILTRATION				•

# PREVENTING MALWARE AND BEYOND

## The Power of Falcon Host

CROWDSTRIKE



### Why Prevention Matters?

As the security industry and its customers have learned the hard way, prevention is not 100 percent effective. Still, prevention adds tremendous value in weeding out the obvious, allowing security teams to focus their efforts and resources on what truly requires their attention. This is why Falcon Host includes the most powerful prevention features designed to stop malware, and in a much broader scope, to stop breaches.

### What Prevention Capabilities Does Falcon Host Provide?

Falcon Host offers prevention against malware. But it expands beyond just malware protection by also offering prevention against advanced targeted attacks and attacks that do not use malware, filling the wide gap left by solutions that primarily focus on malware. Falcon Host uses the right detection and prevention feature at the right time to prevent breaches across the entire attack continuum.

Attack Continuum	File Based Detection Signature/Traditional AV File Whitelisting File Reputation	Exploit Blocking Host Intrusion Prevent Appliance Sandbox	IOC Detection IOC detection Forensics SIEM correlation	Falcon Host Machine Learning Exploit Blocking Whitelisting Indicators of Attack
	<b>ATTACK STARTS</b>			
DELIVERY	•		•	•
INITIAL BEACH HEAD	•			•
	<b>ATTACK UNFOLDS</b>			
ESTABLISH PERSISTENCE			•	•
CREDENTIAL THEFT/PRIVILEGE ESCALATION			•	•
LATERAL MOVEMENT/EXPLORATION				•
	<b>FINAL OBJECTIVES</b>			
E.G. DATA EXFILTRATION				•

# What is CrowdStrike? Falcon platform FAQ

Want to see the CrowdStrike Falcon® platform in action? Start with a free trial of next-gen antivirus

## CAPABILITIES

+ What does CrowdStrike Falcon® do?

+ What solutions are offered within the CrowdStrike Falcon® platform?

+ What is Falcon Fusion?

+ What modules do I need to use Falcon Fusion?

+ What is Falcon Prevent?

+ What is Falcon Insight?

+ What is Falcon OverWatch?

+ What is Falcon Discover?

+ Can I use CrowdStrike Falcon® to replace my current AV solution?

+ Is CrowdStrike Falcon® certified for AV replacement?

+ Which products can CrowdStrike Falcon® help me replace?

+ Can CrowdStrike Falcon® be used for compliance requirements?

+ How does CrowdStrike Falcon® compare to other "next-generation" endpoint protection solutions? What makes Falcon unique?

+ Can I use CrowdStrike Falcon® for incident response?

— Can Falcon Prevent block attacks?

Yes, Falcon Prevent offers powerful and comprehensive prevention capabilities. Falcon Prevent can stop execution of malicious code, block zero-day exploits, kill processes and contain command and control callbacks.

# FALCON PREVENT NEXT-GENERATION ANTIVIRUS

Ideal AV replacement combines the most effective prevention technologies with full attack visibility and simplicity

## INDUSTRY-RECOGNIZED LEGACY AV REPLACEMENT

For organizations struggling with the ineffectiveness and complexity of legacy antivirus solutions, CrowdStrike® Falcon Prevent™ is here to help. Falcon Prevent delivers superior protection with a single lightweight agent that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. Even the largest organizations can be up and running in minutes with Falcon Prevent.

**Certified to replace legacy antivirus products** — Independent testing at AV-Comparatives and SE Labs has certified Falcon Prevent's antivirus capabilities. Falcon Prevent has also been validated for PCI, HIPAA, NIST and FFIEC regulatory requirements.

**Named a leader in the 2019 Gartner Magic Quadrant for Endpoint Protection Platforms (EPP)** — In addition to being positioned in the Leaders Quadrant, CrowdStrike is furthest for "completeness of vision," which includes Gartner criteria such as innovation, marketing and product strategies, vertical industry and geographic strategies, as well as the validity of the business model as a whole.

### KEY BENEFITS

Prevents all types of attacks

Simplifies operations with signatureless protection and software-as-a-service (SaaS) delivery

Deploys in minutes and immediately begins protecting your endpoints

Replaces legacy antivirus quickly and confidently

Operates seamlessly alongside AV as you migrate to simplify transition

Provides full attack visibility





## CrowdStrike Products

### FALCON PREVENT NEXT-GENERATION ANTIVIRUS

## KEY CAPABILITIES

### STATE-OF-THE-ART PREVENTION

Falcon Prevent protects endpoints against all types of attacks, from commodity malware to sophisticated attacks — even when offline.

- Machine learning and artificial intelligence prevent known and unknown malware, adware and potentially unwanted programs (PUPs)
- Behavior-based indicators of attack (IOAs) prevent sophisticated attacks, including ransomware and fileless and malware-free attacks
- Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities
- Detect and quarantine on write stops and isolates malicious files when they first appear on a host
- Threat intelligence prevention blocks activities known to be malicious
- Custom IOAs enable you to define unique behaviors to block
- Quarantine captures blocked files and allows access for investigation
- Script-based execution monitoring inspects and blocks malicious Microsoft Office macros
- Sensor tampering protection stops user or process attempts to manipulate or disable the CrowdStrike Falcon® sensor

### INTEGRATED THREAT INTELLIGENCE

- Automatically determine the scope and impact of threats found in your environment
- Find out if you are targeted, who is targeting you and how to prepare and get ahead
- Use Falcon Prevent integrated with CrowdStrike Falcon X™ to:
  - Fully understand the threats in your environment and what to do about them
  - Access malware research and analysis at your fingertips
  - Easily prioritize responses with threat severity assessment
  - Immediately get recovery steps and resolve incidents with in-depth threat analysis

### FULL ATTACK VISIBILITY AT A GLANCE

For unparalleled alert context and visibility, Falcon Prevent:

- Provides details, context and history for every alert
- Unravels an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data
- Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections
- Keeps detection details for 90 days

### SIMPLE, FAST AND LIGHTWEIGHT

The cloud-native CrowdStrike Falcon platform and lightweight Falcon agent eliminate complexity and simplify endpoint security operations.

- Falcon operates without constant signature updates, complex integrations or on-premises equipment
- The lightweight agent bears little impact on endpoints, from initial install to day-to-day use — no reboot is required after installation
- Minimal CPU overhead restores system performance and end-user productivity
- It works on Day One, deploys in minutes and is immediately operational
- It is automatically kept up to date with cloud-native architecture and SaaS delivery
- Falcon provides broad platform support including Windows, Windows Server, macOS and Linux
- Automated IOA remediation streamlines the removal of artifacts that may lead to reinfection

## FALCON PREVENT: THE EASIEST AV REPLACEMENT

Better protection

Fast and easy deployment

Optimal performance

Reduced complexity

## ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates trillions of endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

## Start Free Trial of Next-Gen AV

Learn more at [www.crowdstrike.com](http://www.crowdstrike.com)

© 2021 CrowdStrike, Inc. All rights reserved.

**DISCLAIMER:** Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

CrowdStrike Falcon Insight XDR: Extended Detection and Response (XDR)

# The world's leading AI-powered platform for unified EDR and XDR

Stop breaches with pioneering detection and response across all key attack surfaces

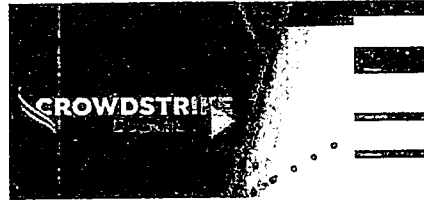
Start free trial

Attend hands-on workshop

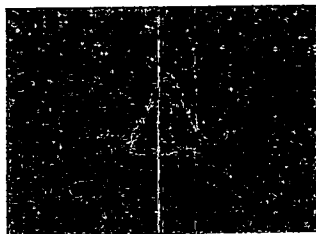
CROWDSTRIKE DELIVERS 100% COVERAGE. MITRE Engenuity ATT&CK® Evaluations: Enterprise

## See Falcon Insight XDR in action

Stealthy adversaries are moving even faster with break-out time down to just 70 minutes. See how Falcon Insight XDR delivers enterprise-wide visibility, detects advanced threats, and responds automatically across your environment.

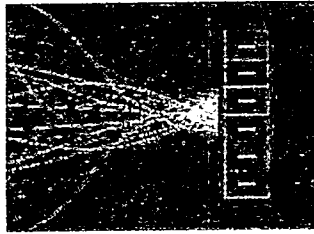


## Falcon Insight XDR key capabilities



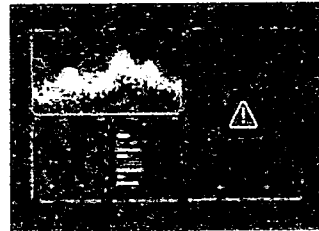
### Full attack visibility

The easy-to-understand Falcon console paints the complete picture of an attack for rapid decision-making. Powerful enterprise-wide search - across your endpoint estate, the Falcon platform and third-party data sources - enables proactive, freeform hunting across your entire environment from day one.



### Simple, fast and lightweight

The single lightweight agent deploys in minutes and is immediately operational - no reboot required. Automated updates and broad operating system coverage help reduce blindspots and operational complexity.



### Industry-leading threat intel

Built-in world-class threat intelligence bolsters detection and supercharges your SOC. From automatic sandbox submissions to in-depth actor profiles, get complete understanding of the threat and adversary behind it.

Handwritten signature or mark

# FALCON OVERWATCH MANAGED THREAT HUNTING

See and stop hidden advanced attacks

## FALCON OVERWATCH — STOPPING THE MEGA BREACH

Falcon OverWatch™ is CrowdStrike's managed threat hunting service, built on the CrowdStrike Falcon® platform. OverWatch provides deep and continuous human analysis, 24/7, to relentlessly hunt for anomalous or novel attacker tradecraft that is designed to evade standard security technologies.

OverWatch is comprised of an elite team of cross-disciplinary specialists who harness the massive power of the CrowdStrike Threat Graph®, enriched with CrowdStrike threat intelligence, to continuously hunt, investigate and advise on sophisticated threat activity in customer environments. Armed with cloud-scale telemetry and detailed tradecraft on more than 130 adversary groups, OverWatch provides unparalleled ability to see and stop the most advanced threats.

OverWatch contacted me a week ago to tell me that they had identified some activity that was associated with a known server hijacking organization. They all allowed us to go in and address that as a goal. Initially, OverWatch very quickly responded and said, "Here is the information that we know about this." Their actions motivated us to take more of our server, so that the black market for spammer and other bad actors to use."

**Mark Sauer**

Chief Information Security Officer, The Hill

## KEY BENEFITS

**See and stop hidden advanced attacks:** The OverWatch team hunts relentlessly to see and stop the stealthiest sophisticated threats: the 1% of 1% of threats that blend in silently and lead to a breach if they remain undetected.

**Achieve maximum effectiveness and efficiency:** OverWatch delivers the best results by augmenting skilled analysts with the most advanced technology. CrowdStrike's elite human experts use cloud-scale data, custom tools and up-to-the-minute threat intelligence to hunt with unprecedented speed and scale.

**Gain a seamless extension of your team:** As a core component of the Falcon platform, OverWatch delivers results for organizations of all sizes, operating as a seamless extension of your team — minimizing overhead, complexity and cost.

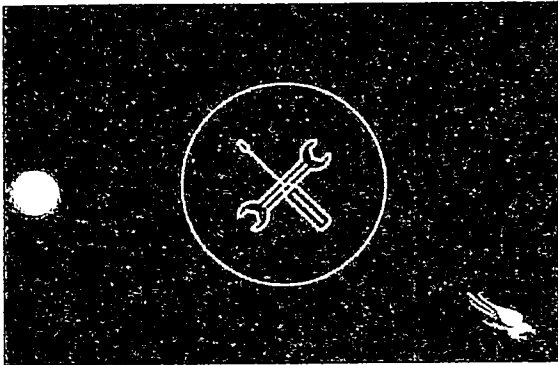


[BACK TO TECH CENTER](#)

---

## How to Hunt for Threat Activity with Falcon Endpoint Protection

January 1, 2022 [Peter Ingebjerg](#) [Tech Center](#)



The greatest minds in cybersecurity are at Fal.Con in Las Vegas, Sept. 18-21.

[Register now](#) to build skills at hands-on workshops and learn from skilled threat hunters.


Introduction to Threat Hunting with Falcon Endpoint Protection

CrowdStrike Falcon® offers a powerful set of features that can be used to hunt for threat activity in your environment. The Falcon agent is constantly monitoring and recording endpoint activity and streaming it to the cloud and CrowdStrike's Threat Graph. The data includes things like process execution, network connections, file system activity, user information, service details, script activity and admin tool usage. Storing this data in the Threat Graph ensures that the data is always available (even while endpoints are offline) and also ensures that it can be searched in real time and retrospectively – even the largest environments can get results in seconds.

CrowdStrike Falcon® provides multiple approaches to threat hunting. In this article, we will review workflows that begin with indicator searches as well as custom event searches.

Video

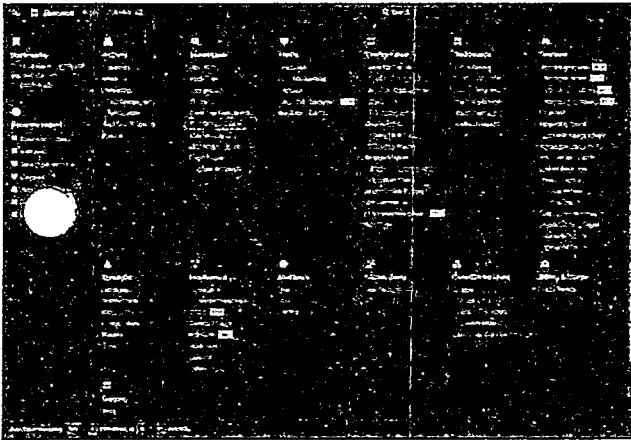


Hey! What brings you to our corner of the internet today? 

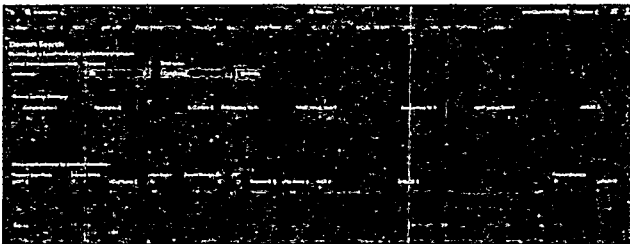
### Indicator Searches

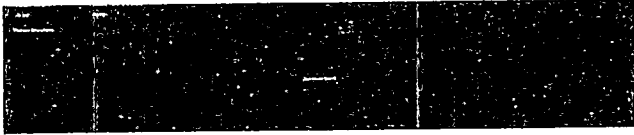
The Investigate App options allow administrators to search for indicators of compromise in their environment. This aids in understanding exposure to known threats, while also providing the ability to drill-down and pivot to explore the context around malicious activity. The CrowdStrike Threat Graph then ensures that you get immediate results from both online and offline systems no matter how large your organization. In this section, we will demonstrate two of the available indicator searches.

Under the Investigate App, select "Bulk Domain Search".

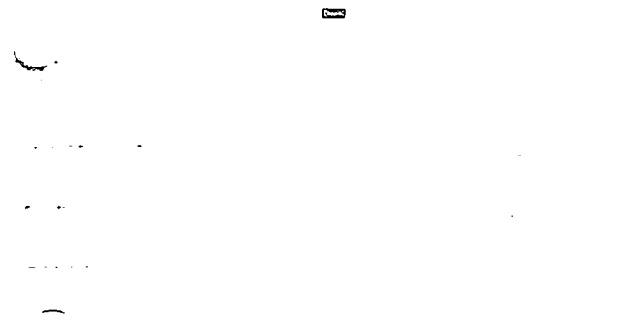


Searches can be done individually or on multiple domains. Note that multiple domains should be separated by a space. After specifying a time range, click "Submit" to begin the search. The search will query all of your data in the Threat Graph and report any system in your environment has ever connected to one of these domains. A quick way to get sample results can be a search for `www.google.com`. In this example, we see that six different hosts have connected to `conti.news`.





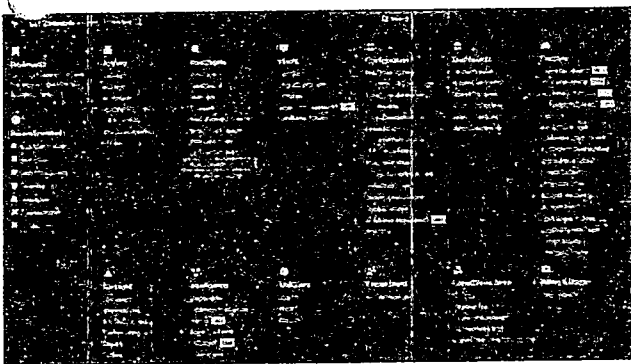
Clicking on one of the impacted hostnames will bring you to a screen that shows all activity on that system. In this example, we learn that this is a cloud host running Windows 7. This screen would also report if there were any detections on this host in the last seven days.



### Event Search

The Event Search functionality is for power users who want to access all of their data in the CrowdStrike Threat Graph. The flexible query language can handle complex searches that are often required for more advanced threat hunting. In this section, we will review two advanced hunting queries from our [Hunting and Investigation](#) documentation. This document is available to all CrowdStrike customers via the UI.

Under the Investigate menu, select "Event Search".



# Hunting and Investigation

Last updated: Sep. 16, 2023

## Introduction

The Hunting Guide for Windows teaches you how to hunt for adversaries, suspicious activities, suspicious processes, and vulnerabilities on the Windows platform using Falcon.

Falcon contains a suite of powerful search tools that allow you to analyze, explore, and hunt for suspicious or malicious activity in your environment. These tools include the pre-made search dashboards in the various Falcon apps as well as the ability to run custom queries on the [Events Search | Investigate/events/en-US/app/eam2/search](#) page in the Investigate App. This guide focuses on both using custom queries to hunt, but will also direct you to use Falcon's pre-made dashboards when it makes most sense.

If at any time you have questions or encounter technical issues not covered in this guide or in the Troubleshooting section, contact [Support \(https://supportportal.crowdstrike.com/\)](https://supportportal.crowdstrike.com/).

For info about XDR hunting and investigation, see [Falcon XDR | /documentation/page/c4ca5fed/extended-detection-and-response-xdr](#).

## Before you begin

### System dependencies

This guide contains information about how to hunt using Falcon and is tailored specifically towards users running the Falcon sensor on Windows devices. However, a lot of the ideas and concepts also apply to users running the Falcon sensor on Mac or Linux. Depending on the sensor platform, however, the names and descriptions of certain events as well as custom query syntax will vary. We recommend that you read and refer to the [Events Data Dictionary | /documentation/page/e3ce0b24/events-data-dictionary](#) to learn more about specific events and their variations across platforms. The Events Data Dictionary also contains additional custom queries not found in this document that could be useful when hunting.

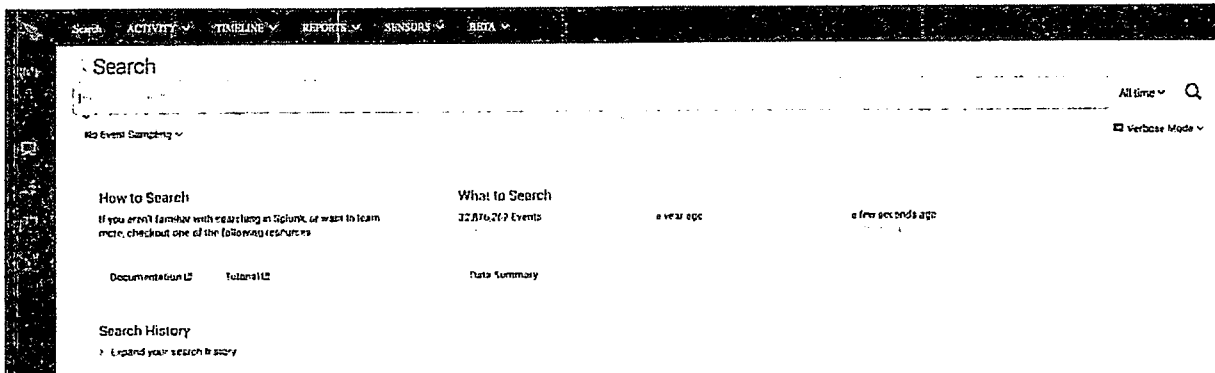
### Browser dependencies

CrowdStrike currently supports the Google Chrome browser for use with the Falcon web interface. Other browsers might work, but we do not support other browsers at this time.

## Hunting with Falcon

### Overview

Hunting with Falcon is straightforward. By using either the pre-made dashboards and reports or by using custom queries on the Events Search page, you can search for specific events and data points across one, several, or all hosts running the Falcon sensor in your environment. The data returned in an Events Search query is from the last 30 days of sensor activity, though most of the queries you run will need to be narrowed down to a smaller timeframe so that results are usable. You then use your search results to understand and evaluate security events happening in your environment.



Before you start hunting with Falcon, however, there are a few concepts and best practices that you should familiarize yourself with, beginning with the queries themselves.

## Best practices

### Write specific queries

All queries in Falcon are powered by the Splunk query language. This document focuses less on teaching you Splunk syntax and more on the various behaviors and activities you will be hunting. To learn more about Splunk and Splunk syntax, we recommend that you read the [Official Splunk Documentation](http://docs.splunk.com/Documentation/Splunk/6.0.5/SearchReference/Whatsinthismanual) [http://docs.splunk.com/Documentation/Splunk/6.0.5/SearchReference/Whatsinthismanual] and the [Splunk Enterprise Quick Reference Guide](http://docs.splunk.com/Documentation/Splunk/6.0.5/SearchReference/SplunkEnterpriseQuickReferenceGuide) [http://docs.splunk.com/Documentation/Splunk/6.0.5/SearchReference/SplunkEnterpriseQuickReferenceGuide].

Even if you aren't a Splunk expert, this guide makes it easy to understand what each query does and how you can modify queries to get more value out of them. Let's start with a simple example.

Show me a list of processes that executed from the Recycle Bin for a specific AID

```
aid=aid ImageFileName=*$Recycle.Bin* event_simpleName=ProcessRollup2 | stats values(name)
values(MD5HashData) values(ComputerName) values(ImageFileName) count by aid
```

Most of the queries in this document can simply be copied and pasted into Events Search with minimal modification required by the user. However, when you see capitalized values, you will need to provide a value before you can run the query.

In the example above, you should provide an "agent ID" (or "AID" for short), which is a unique ID given to each Falcon sensor. Adding the AID to the query limits the scope of your query to the sensor with that AID and greatly reduces the time and computational cost of your search.

Thus, the above query might end up looking like this:

```
aid="a9e3b67c7883497f6d18fdd1517b177d" ImageFileName=*$Recycle.Bin* event_simpleName=ProcessRollup2 |
stats values(name) values(MD5HashData) values(ComputerName) values(ImageFileName) count by aid
```

Using the AID in this fashion is just one way to drill down to a specific host. You can also use host name (ComputerName="foo") in the same fashion.

This is just one example, but shows how specificity matters greatly when writing Splunk queries. The more specific you can be when writing a query, the fewer results you will have to sort through and the faster the query will run.

Let's see how a simple query can be made more useful for you with a few simple modifications. Below is an example query that returns a large amount of data and takes a long time to run. This query returns a list of SuspiciousDnsRequest events, the domains to which the requests were made, the host names from which the requests were made, and the number of times the requests were made:

```
event_simpleName=SuspiciousDnsRequest | stats values(ComputerName) count by DomainName
```

The amount of results returned by this query and the time that it takes to run make this query difficult to work with. We can fix both of this by making our query more specific.

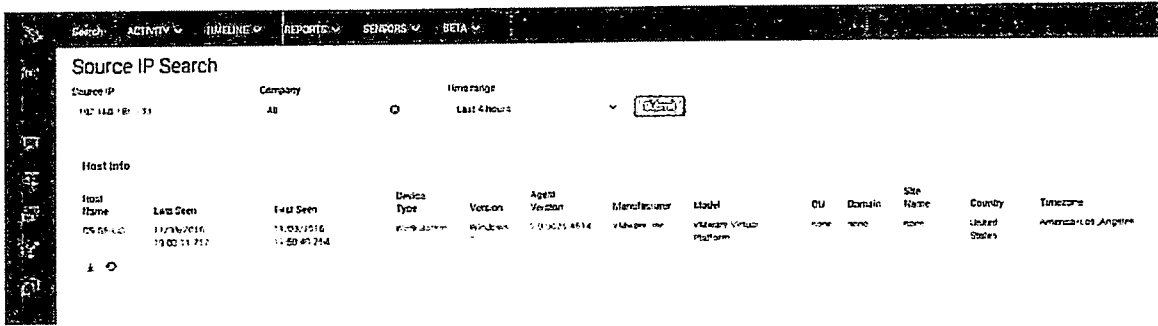
Let's start reducing the number of results by limiting the query to a single AID, which would return a list of SuspiciousDnsRequest events that occurred on the host running the Falcon sensor with that particular AID:

```
aid="a9e3b67c7883497f6d18fdd1517b177d" event_simpleName=SuspiciousDnsRequest | stats values(ComputerName)
count by DomainName
```

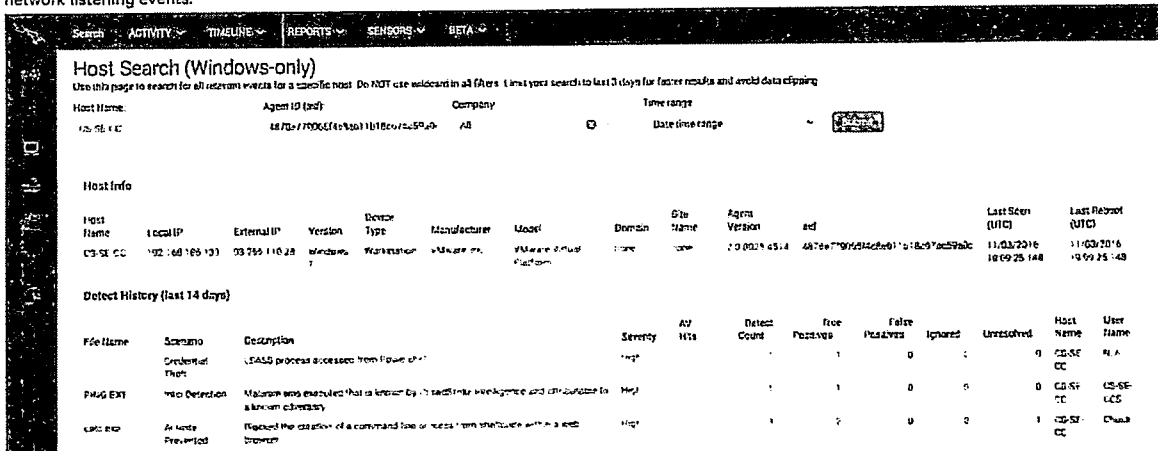
Next, we can further reduce our results list by specifying a timeframe. Instead of searching across 30 days of data, let's search for instances of this event in the last 24 hours using the "earliest" and "latest" keywords:

```
aid="a9e3b67c7883497f6d18fdd1517b177d" event_simpleName=SuspiciousDnsRequest earliest=-24h latest=now |
stats values(ComputerName) count by
DomainName
```

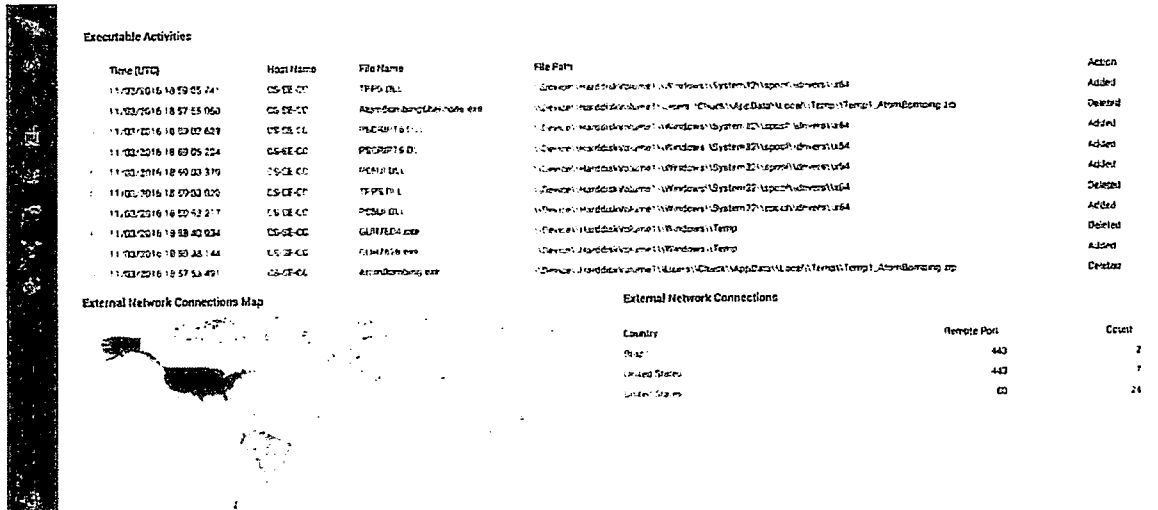




3. Next, click one of the host names in the list. This opens the Host Search page with a pre-populated search for that host. In the results, you will see a wide range of data including basic host information, detect history for the host, a list of unresolved detects for the host, and a list of network connection and network listening events.



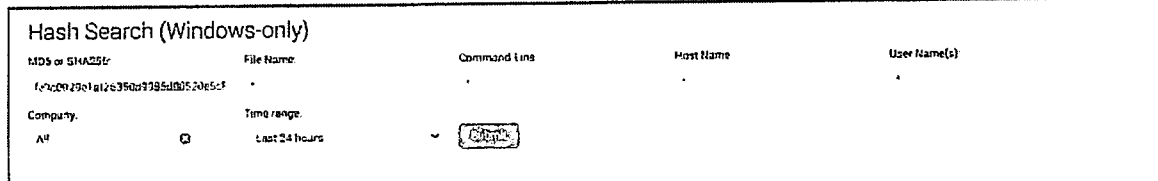
You can even view a world map of external network connections for that host.



## Hunting walkthrough: Hash IOC

Let's walk through an example of how the Falcon web interface helps you hunt when starting with a hash IOC.

1. Sign in to the Falcon web interface and open the [Hash Search f/investigate/events/en-US/app/eam2/investigate\\_hash](#) page.
2. Enter the MD5 or SHA256 that you are searching for and specify a time range. You can search by file name, command line string, host name, or user name.



In the search results, you will see the Process Execution History section for the hash (historical summary of execution details such as the total number of executions) as well as a Process Executions section, which breaks out each individual instance that the hash was executed, the time of execution, and

**Problem****Solution**

show up in the search results.

Something specific is erroneously showing up in the results.

Identify which piece of data should not be there and revisit the portion of the syntax that you feel should exclude that from your search results. This will help you isolate which part of your query's syntax is causing you to receive results where there should be none. There could also be an issue with your config. Contact Support if the issue continues.

## Appendix A: Investigate App Pages

The [Investigate App](#) ([/investigate/](#)) lets you search for specific hashes, file names, command-line arguments, IP addresses, and specific computers and users. These searches help you quickly collect relevant information during incident triage and hunting.

**Note:** When you set a time range for your Investigate searches, we recommend using a time range of **3 days** or shorter. Longer time ranges can take several minutes to display.

## Host Search

Use Host Search to search for events across all Windows and Mac hosts in your environment. Due to differences in these platforms, some items might not be available for both Windows and Mac.

Searchable activity includes:

- Host info
- Map of external network connections
- List of external network connections (by country, including the port and the # of connections)
- Detection history (last 14 days)
- Unresolved Detects (last 7 days)
- Local and External IPs (last 7 days)
- Unique Users Logged on (last 7 days)
- Unique ASEP values updated
- Unique ASEP keys updated
- Unique Executables Written
- Unique Injected Threads
- Unique DLL Injections
- Browser-injected Threads from Unsigned Modules
- Unique Java-injected Threads
- Command History
- Process Executions
- Admin Tool Usage
- Possible Scripting Activities
- DNS Requests
- Network Connections
- Network Listening

- RAR/Zip File Written
- Scripts Written
- Executable Activities
- Removable Media Usage

## Hash Search

Use Hash Search to search for events by hash across all Windows and Mac hosts in your environment. Due to differences in these platforms, some items might not be available for both Windows and Mac.

Searchable hash information includes:

- Hash Written History (SHA256-only)
- Module Load History
- Process Execution History
- Detect History (last 14 days)
- Unresolved Detects (last 7 days)
- Process Executions

You can export the data to a PDF by clicking the **Export PDF** button on the right side of the screen.

## User Search

Use User Search to search for user activity across all Windows and Mac hosts in your environment. Due to differences in these platforms, some items might not be available for both Windows and Mac. Results in this report are filtered if:

- The user logging on is one of the well-known security identifiers. (see Microsoft's [documentation \(https://support.microsoft.com/en-us/help/243330/well-known-security-identifiers-in-windows-operating-systems\)](https://support.microsoft.com/en-us/help/243330/well-known-security-identifiers-in-windows-operating-systems))
- The logon session is NOT an interactive session or a service account.

Though the results are filtered, the raw events for these logons are still captured in Event Search

Searchable user activity includes:

- Logon Activities (last 30 days)
- Detect History (last 30 days)
- Unresolved Detects (last 7 days)
- Process Executions
- Admin Tool Usage
- Files written (JAR, OLE, OOXML, PDF, RAR, RTF, ZIP, dumps)

## Source IP Search

Search for host information by IP. Source IP search allows you to use wildcards (for example, 192\*).

## Bulk Hash Search

Search for multiple hashes (MD5/SHA256/SHA1\*) and detect/process execution history. Bulk Hash Search allows you to use wildcards (for example, c32\*).

\*SHA1 is deprecated (<https://supportportal.crowdstrike.com/s/article/Support-Announcement-Deprecation-of-SHA1-support-in-Falcon>) as of Falcon sensor 5.11.

## Bulk Domain Search



Search for detect and process execution history involving a domain or list of domains. Bulk Domain Search allows you to use wildcards (for example, evil~~dom~~\*).

## Event Search

The Event Search page is where you can find pre-made reports and pre-made searches that allow you to view data collected from your endpoints. This page also provides you with a powerful custom search tool that allows you to analyze, explore, and hunt for suspicious or malicious activity in your environment.

Tip: Read our [Events Data Dictionary \[documentation/page/e3ce0b24/events-data-dictionary\]](#) for specific data on key CrowdStrike events that you find when using the Event Search page.

The Event Search page is divided into several different sections:

- **Search:** Provides direct access to Falcon endpoint metadata, where events can be queried and processed using Splunk, a powerful query language. Use this view when the prebuilt Falcon dashboards and reports do not contain the desired results, or when you want to write a custom query. However, the stock dashboards in the Falcon console will be sufficient most of the time. For detailed information on CrowdStrike events and how to search for them, see the [Events Data Dictionary \[documentation/page/e3ce0b24/events-data-dictionary\]](#).
  - **Scheduled searches:** Create event searches that run automatically and recur on a schedule that you set. You can download and share the search results, and your specified recipients can receive notifications each time a scheduled search completes. Configure notifications to be sent when a search produces results, when a search produces no results, or both. For more info, see [Scheduled Searches \[documentation/page/a4275adf/scheduled-searches-for-edr\]](#).
- **Activity:** Provides four different dashboard views:
  - **Detection Activity page** This feature applies only to Managed Security Service Providers (MSSP) partners and customers with multiple Customer IDs (CID). This page, available at Investigate > Hunt > Detection Activity, allows users to view all detections associated with all CIDs they have access to. While viewing the Detection Activity page, users can click any detection to open Falcon UI Process Explorer in a new browser tab to view the detection without the need to manually toggle to the correct CID. Users can perform triage actions such as assigning detection, adding comments, contain host, resolve detection, etc. When finished triaging the detection, users can close the browser tab and return to the Detection Activity page to continue working on the next detection. Note that some applications on the left navigation menu such as Dashboards, Users, and so on are not available on the auto-toggled browser tab.
  - **Linux Sensors:** Provide a comprehensive view of activities on Linux hosts.
  - **Mac Sensors:** Provide a comprehensive view of activities on Mac hosts.
- **Timeline:** Provides the ability to generate a "Host Timeline" and a "Process Timeline." This allows you to view all relevant events for a specific computer or all events associated with any user-specified process execution.
- **Reports:** Offers various canned reports surrounding activities that typically indicate suspicious activity occurring on a system. Available reports are listed below.
  - **Files Written to Removable Media:** Search for file written activities to removable media.
  - **Machine Learning Prevention:** View malware that would have been blocked in your environment during the last 30 days based on different Machine Learning Prevention settings (Cautious, Moderate, or Aggressive).
  - **PowerShell Hunt:** Allows users to search for suspicious PowerShell activities.
  - **Prevention Policy Audit Trail:** View audit trail for all policies.
  - **Hunting Reports:** Provides fast access to automated hunting queries in the "Search" view. Hunting report options:
    - Command Line and ASEP Activity from Network-capable Processes

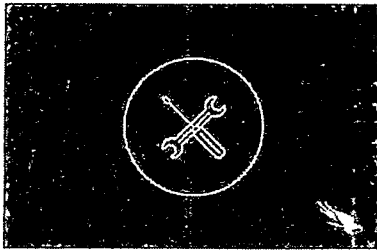




Fields: Windows, macOS, Linux, Falcon Container

Field	Description
TargetProcessId	The <code>ProcessId</code> of a target process in <code>ProcessId</code> format. This field exists in almost all events, and it represents the ID of the process that is responsible for the activity of the event in focus. For example, the <code>TargetProcessId</code> of a process that performed a file operation is <code>InjectedInread</code> event.
SourceProcessId	On Windows, the <code>ParentProcessId</code> field is used to be the same as <code>SourceProcessId</code> since a different parent can be spawned for <code>ProcessId</code> . On Mac, <code>SourceProcessId</code> is the <code>responsible_pid</code> which is used by KFD to note the process in request to this KFD process.
SourceThreadId	UT ID of thread from existing process. See the description of the <code>SourceProcessId</code> field for more details.
ParentProcessId	The process ID of the parent process.
ImageFileName	The full path to a file (executable PE file). The content of this field provides more information as to its meaning. For <code>ProcessRollup2</code> events, this field may point to the main executable for the created process.
ZoneIdentifier	The identifier for the network zone of the host. <b>Values:</b> <ul style="list-style-type: none"> <li>• LOCAL_MACHINE (1)</li> <li>• INTRANET (2)</li> <li>• TRUSTED_SITES (3)</li> <li>• INTERNET (3)</li> <li>• RESTRICTED_SITES (4)</li> </ul>
HostUri	
ReferrerUri	
ParentBaseFileName	
GrandParentBaseFileName	
AuthenticodeHashData	<b>Values:</b> <ul style="list-style-type: none"> <li>• SIGNATURE_FLAG_NONE (0x00000000)</li> <li>• SIGNATURE_FLAG_MACHINE (0x00000001)</li> <li>• SIGNATURE_FLAG_TEST (0x00000002)</li> <li>• SIGNATURE_FLAG_MACHINE_SIGNED (0x00000004)</li> <li>• SIGNATURE_FLAG_CATALOG (0x00000008)</li> <li>• SIGNATURE_FLAG_MACHINE_SIGNED_CATALOG (0x0000000C)</li> <li>• SIGNATURE_FLAG_MACHINE_SIGNED_CATALOG_TEST (0x00000010)</li> <li>• SIGNATURE_FLAG_MACHINE_SIGNED_CATALOG_TEST (0x00000014)</li> </ul>

## How to Hunt for Threat Activity with Falcon Endpoint Protection



The greatest minds in cybersecurity are at Fal.Con in Las Vegas, Sept. 18-21.

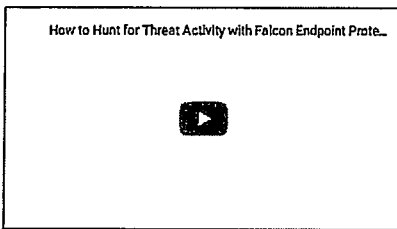
[Register now](#) to build skills at hands-on workshops and learn from skilled threat hunters.

### Introduction to Threat Hunting with Falcon Endpoint Protection

CrowdStrike Falcon® offers a powerful set of features that can be used to hunt for threat activity in your environment. The Falcon agent is constantly monitoring and recording endpoint activity and streaming it to the cloud and CrowdStrike's Threat Graph. The data includes things like process execution, network connections, file system activity, user information, service details, script activity, and admin tool usage. Storing this data in the Threat Graph ensures that the data is always available (even while endpoints are offline) and also ensures that it can be searched in real time and retrospectively – even the largest environments can get results in seconds.

CrowdStrike Falcon® provides multiple approaches to threat hunting. In this article, we will review workflows that begin with indicator searches as well as custom event searches.

### Video



### Indicator Searches

The Investigate App options allow administrators to search for indicators of compromise in their environment. This aids in understanding exposure to known threats, while also providing the ability to drill-down and pivot to explore the context around malicious activity. The CrowdStrike Threat Graph then ensures that you get immediate results from both online and offline systems no matter how large your organization. In this section, we will demonstrate two of the available indicator searches.

Under the Investigate App, select "Bulk Domain Search".

*Handwritten signature or initials.*



MITRE ATT&CK HEAT MAP, 1 OF 3

Initial Access		Execution		Persistence		Privilege Escalation	
Technique	Sub-technique	Technique	Sub-technique	Technique	Sub-technique	Technique	Sub-technique
Exploit Public-Facing Application	Domain Accounts	Windows Command Shell	Powercat	Local Accounts	Domain Accounts	Local Accounts	Domain Accounts
	Local Accounts		Powercat		Local Accounts		Local Accounts
Phishing	Default Accounts	Windows Management Instrumentation	Unlink Shell	Default Accounts	Default Accounts	Default Accounts	Default Accounts
	Default Accounts		Unlink Shell		Default Accounts		Default Accounts
Spearphishing Attachment	Spearphishing Attachment	Visual Basic	Visual Basic	Scheduled Task/Job	Scheduled Task	Process Injection	Dynamic-Link Library Injection
	Spearphishing Attachment		Visual Basic		Scheduled Task		Process Injection
Spearphishing Link	Spearphishing Link	Python	Python	Cron	Cron	Process Injection	Process Hollowing
	Spearphishing Link		Python		Cron		Process Injection
Spearphishing via Service	Spearphishing via Service	JavaScript	JavaScript	Local Account	Local Account	Process Injection	Portable Executable Injection
	Spearphishing via Service		JavaScript		Local Account		Process Injection
External Remote Services	External Remote Services	Windows Management Instrumentation	Windows Management Instrumentation	Domain Account	Domain Account	Process Injection	Thread Execution Hijacking
	External Remote Services		Windows Management Instrumentation		Domain Account		Thread Execution Hijacking
Drive-by Compromise	Drive-by Compromise	Scheduled Task/Job	Scheduled Task	Server Software Component	Web Shell	Scheduled Task/Job	Scheduled Task
	Drive-by Compromise		Scheduled Task/Job		Web Shell		Scheduled Task
Trusted Relationships	Trusted Relationships	Cron	Cron	Account Manipulation	SSH Authorized Keys	Cron	Cron
	Trusted Relationships		Cron		SSH Authorized Keys		Cron
System Services	System Services	Service Execution	Service Execution	Accessibility Features	Accessibility Features	System Services	System Services
	System Services		Service Execution		Accessibility Features		System Services
User Execution	User Execution	Malicious File	Malicious File	Image File Execution Options Injection	Image File Execution Options Injection	User Execution	Elevated Execution with Prompt
	User Execution		Malicious File		Image File Execution Options Injection		Elevated Execution with Prompt
Exploitation for Client Execution	Exploitation for Client Execution	Malicious Link	Malicious Link	Event Triggered Execution	Windows Management Instrumentation Event Subscription	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism
	Exploitation for Client Execution		Malicious Link		Windows Management Instrumentation Event Subscription		Abuse Elevation Control Mechanism
Inter-Process Communication	Inter-Process Communication	Dynamic Data Exchange	Dynamic Data Exchange	Boot or Logon Autostart Execution	Component Object Model Hijacking	Sudo and Sudo Caching	Sudo and Sudo Caching
	Inter-Process Communication		Dynamic Data Exchange		Component Object Model Hijacking		Sudo and Sudo Caching
Shared Modules	Shared Modules	Dynamic Data Exchange	Dynamic Data Exchange	Registry Run Keys/Startup Folder	Registry Run Keys/Startup Folder	Accessibility Features	Accessibility Features
	Shared Modules		Dynamic Data Exchange		Registry Run Keys/Startup Folder		Accessibility Features
Create or Modify System Process	Create or Modify System Process	Event Triggered Execution	Event Triggered Execution	Security Support Provider	Security Support Provider	Image File Execution Options Injection	Image File Execution Options Injection
	Create or Modify System Process		Event Triggered Execution		Security Support Provider		Image File Execution Options Injection
External Remote Services	External Remote Services	Windows Service	Windows Service	Event Triggered Execution	Windows Management Instrumentation Event Subscription	Event Triggered Execution	Windows Management Instrumentation Event Subscription
	External Remote Services		Windows Service		Windows Management Instrumentation Event Subscription		Windows Management Instrumentation Event Subscription
DLL Search Order Hijacking	DLL Search Order Hijacking	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	DLL Search Order Hijacking	DLL Search Order Hijacking	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution
	DLL Search Order Hijacking		Boot or Logon Autostart Execution		DLL Search Order Hijacking		Boot or Logon Autostart Execution
DLL Side-Loading	DLL Side-Loading	Security Support Provider	Security Support Provider	Create or Modify System Process	Create or Modify System Process	Security Support Provider	Security Support Provider
	DLL Side-Loading		Security Support Provider		Create or Modify System Process		Security Support Provider
Path Interception by Search Order Hijacking	Path Interception by Search Order Hijacking	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation
	Path Interception by Search Order Hijacking		Exploitation for Privilege Escalation		Exploitation for Privilege Escalation		Exploitation for Privilege Escalation
Office Template Macros	Office Application Startup	Office Template Macros	Office Application Startup	Office Template Macros	Office Template Macros	Office Template Macros	Office Template Macros
	Office Application Startup		Office Template Macros		Office Template Macros		Office Template Macros
Browser Extensions	Browser Extensions	Hijack Execution Flow	Hijack Execution Flow	Hijack Execution Flow	Hijack Execution Flow	Hijack Execution Flow	Hijack Execution Flow
	Browser Extensions		Hijack Execution Flow		Hijack Execution Flow		Hijack Execution Flow
Compromise Client Software Binary	Compromise Client Software Binary	Group Policy Modification	Group Policy Modification	Group Policy Modification	Group Policy Modification	Group Policy Modification	Group Policy Modification
	Compromise Client Software Binary		Group Policy Modification		Group Policy Modification		Group Policy Modification
Access Token Manipulation	Access Token Manipulation	Access Token Manipulation	Access Token Manipulation	Access Token Manipulation	Access Token Manipulation	Access Token Manipulation	Access Token Manipulation
	Access Token Manipulation		Access Token Manipulation		Access Token Manipulation		Access Token Manipulation

*[Handwritten signature]*





MITRE ATT&CK HEAT MAP, 2 OF 3

Defense Evasion		Credential Access		Discovery		Lateral Movement		
Technique	Sub-technique	Technique	Sub-technique	Technique	Sub-technique	Technique	Sub-technique	
Masquerading	Domain Accounts	OS Credential Dumping	LSASS Memory	System Owner/User Discovery	Domain Account	Remote Services	Remote Desktop Protocol	
	Local Accounts		Security Account Manager	Remote System Discovery			SMB/Windows Admin Shares	
	Default Accounts		NTDS	Account Discovery			SSH	
Impair Defenses	Match Legitimate Name or Location	Brute Force	Atc/password and /etc/shadow	System Information Discovery	Local Account	Lateral Tool Transfer	Distributed Component Object Model	
	Masquerade Task or Service		LSA Secrets	Process Discovery			VNC	
	Remove System Utilities		Cached Domain Credentials	System Network Configuration Discovery			Windows Remote Management	
Indicator Removal on Host	File Deletion	Unsecured Credentials	DCSync	File and Directory Discovery	Domain Groups	Use Alternate Authentication Material	RDP Hacking	
	Clear Windows Event Logs		Password Spraying	Permission Groups Discovery			Pass the Hash	
	Network Share Connection Removal		Password Guessing	System (Network) Connections Discovery			Exfiltration of Remote Services	
Signed Binary Proxy Execution	Timestamp	Credentials from Password Stores	Private Keys	System (Network) Connections Discovery	Local Groups	Query Registry		
	Clear Linux or Mac System Logs			CredentiaIs in Files			Domain Trust Discovery	
	Clear Command History			Windows Credential Manager			Network Service Scanning	
Process Injection	Disable or Modify Tools	Steal or Forge Kerberos Tickets	Kerberoasting	Software Discovery	Security Software Discovery	Network Share Discovery		
	Customize or Modify System Firewall			Group Policy Preferences			System Time Discovery	
	Run322			Credentials from Web Browsers			Network Sniffing	
Modify Registry	Registry32	Input Capture	Web Portal Capture	System Time Discovery	System Time Discovery	Password Policy Discovery		
	Masquer			Windows Credential Manager			System Service Discovery	
	Dynamic-link Library Injection			Keylogging			System Time Discovery	
Obfuscated Files or Information	Process Hollowing	Network Sniffing	Steal Web Session Cookie	Network Sniffing	Password Policy Discovery			
	Portable Executable Injection			Thread Execution Hijacking				
	Thread Execution Hijacking							
Hide Artifacts	Compile After Delivery	Software Packing	Indicator Removal from Tools	Hidden Files and Directories				
	Software Packing			Hidden Users				
	Indicator Removal from Tools			NTFS File Attributes				
File and Directory Permissions Modification	Hidden Window	Linux and Mac File and Directory Permissions Modification	Hidden Users	NTFS File Attributes				
	Hidden Files and Directories			Windows File and Directory Permissions Modification				
	Hidden Users							
Deobfuscate/Decode Files or Information	Windows File and Directory Permissions Modification	Bypass User Account Control	Elevated Execution with Prompt	Windows File and Directory Permissions Modification				
	Deobfuscate/Decode Files or Information			Setuid and Setgid				
	Setuid and Setgid			Setuid and Setgid				
Abuse Elevation Control Mechanism	Setuid and Setgid	Setuid and Setgid	Setuid and Setgid	Setuid and Setgid				
	Setuid and Setgid			Setuid and Setgid				
	Setuid and Setgid			Setuid and Setgid				
Hijack Execution Flow	DLL Search Order Hijacking	DLL Search Order Hijacking	DLL Side-Loading	DLL Search Order Hijacking				
	DLL Side-Loading			DLL Side-Loading				
	DLL Side-Loading			DLL Side-Loading				
Trusted Developer Utilities Proxy Execution	Path Interception by Search Order Hijacking	Path Interception by Search Order Hijacking	Path Interception by Search Order Hijacking	Path Interception by Search Order Hijacking				
	Path Interception by Search Order Hijacking			Path Interception by Search Order Hijacking				
	Path Interception by Search Order Hijacking			Path Interception by Search Order Hijacking				
BITS Jobs	MSBuild	MSBuild	MSBuild	MSBuild				
	MSBuild			MSBuild				
	MSBuild			MSBuild				
Domain Policy Modification	Group Policy Modification	Group Policy Modification	Group Policy Modification	Group Policy Modification				
	Group Policy Modification			Group Policy Modification				
	Group Policy Modification			Group Policy Modification				
Indirect Command Execution	Pass the Hash	Pass the Hash	Pass the Hash	Pass the Hash				
	Pass the Hash			Pass the Hash				
	Pass the Hash			Pass the Hash				
Access Token Manipulation	Exploitation for Defense Evasion	Exploitation for Defense Evasion	Exploitation for Defense Evasion	Exploitation for Defense Evasion				
	Exploitation for Defense Evasion			Exploitation for Defense Evasion				
	Exploitation for Defense Evasion			Exploitation for Defense Evasion				



# What is CrowdStrike? Falcon platform FAQ

Want to see the CrowdStrike Falcon® platform in action? Start with a free trial of next-gen antivirus  
[View Demo](#)

## CAPABILITIES

+ What does CrowdStrike Falcon® do?

+ What solutions are offered within the CrowdStrike Falcon® platform?

+ What is Falcon Fusion?

+ What modules do I need to use Falcon Fusion?

+ What is Falcon Prevent?

+ What is Falcon Insight?

+ What is Falcon OverWatch?

+ What is Falcon Discover?

+ Can I use CrowdStrike Falcon® to replace my current AV solution?

+ Is CrowdStrike Falcon® certified for AV replacement?

+ Which products can CrowdStrike Falcon® help me replace?

+ Can CrowdStrike Falcon® be used for compliance requirements?

+ How does CrowdStrike Falcon® compare to other "next-generation" endpoint protection solutions? What makes Falcon unique?

+ Can I use CrowdStrike Falcon® for incident response?

— Can Falcon Prevent block attacks?

Yes, Falcon Prevent offers powerful and comprehensive prevention capabilities. Falcon Prevent can stop execution of malicious code, block zero-day exploits, kill processes and contain command and control callbacks.



# FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

## FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

## KEY PRODUCT CAPABILITIES

### SIMPLIFY DETECTION AND RESOLUTION

- ▣ **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- ▣ **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- ▣ **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- ▣ **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

## KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

## CrowdStrike Products

### FALCON ENDPOINT DETECTION AND RESPONSE (EDR)

- ▣ **Respond decisively:** Act against adversaries in real time to stop attacks before they become breaches. Powerful response actions allow you to contain and investigate compromised systems, and Falcon Real Time Response capabilities provide direct access to endpoints under investigation. This allows security responders to run actions on the system and eradicate threats with surgical precision.

### GAIN FULL-SPECTRUM VISIBILITY IN REAL TIME

- ▣ **See the big picture in real time:** CrowdScore delivers a simple metric that helps an organization understand its threat level in real time. This makes it easy for security leaders to quickly understand if they are under attack and assess the severity of the threat so they can coordinate the appropriate response.
- ▣ **Capture critical details for threat hunting and forensic investigations:** Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.
- ▣ **Get answers in seconds:** The CrowdStrike Threat Graph® database stores event data and answers queries in five seconds or less, even across trillions of events.
- ▣ **Recall for up to 90 days:** Falcon Insight provides a complete record of endpoint activity over time, whether your environment consists of fewer than 100 endpoints or more than 500,000.
- ▣ **Streamline IT and security operations:** Falcon Fusion is a unified cloud-scale

security orchestration, automation and response (SOAR) framework, providing customizable and easy-to-use automation to simplify enterprise security workflows.

- ▣ **Understand endpoint security posture:** Falcon Insight provides a Zero Trust Assessment (ZTA) that determines endpoint health across the organization. With real-time security posture assessment, you can easily identify and update sensor policies and OS settings that are out-of-date or increase risk. Share assessment scores with CrowdStrike Zero Trust ecosystem partners for real-time conditional access enforcement.

### REALIZE IMMEDIATE TIME-TO-VALUE

- ▣ **Save time, effort and money:** Cloud-enabled Falcon Insight is delivered by the CrowdStrike Falcon platform and does not require any on-premises management infrastructure.
- ▣ **Deploy in minutes:** CrowdStrike customers can deploy the cloud-delivered Falcon agent to more than 100,000 endpoints globally in less than 24 hours.
- ▣ **Be immediately operational:** With unmatched detection and visibility from Day One, Falcon Insight hits the ground running, monitoring and recording on installation without requiring reboots, finetuning, baselining or complex configuration.
- ▣ **Experience no impact on the endpoint:** With only a lightweight agent on the endpoint, searches take place in the Threat Graph database without any performance impact on endpoints or the network.

## INDUSTRY RECOGNITION

CrowdStrike is recognized as a leader in endpoint protection solutions by industry analysts, independent testing organizations and security professionals. Visit the [CrowdStrike Industry Recognition webpage](#) for more information.

## ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Start Free Trial  
of Next-Gen AV

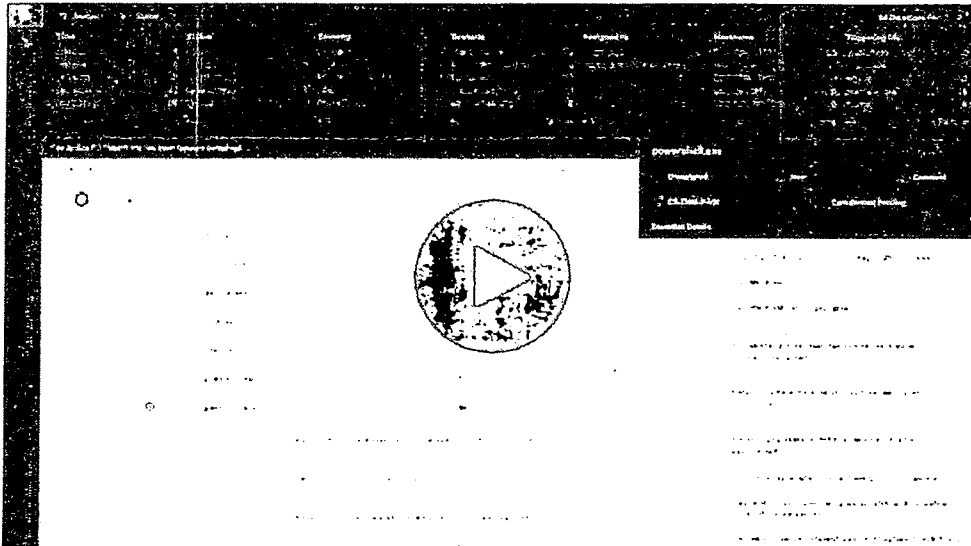
Learn more at [www.crowdstrike.com](http://www.crowdstrike.com)

© 2021 CrowdStrike, Inc. All rights reserved.



Reference: <https://www.crowdstrike.com/resources/videos/how-to-contain-an-infected-system/>

## HOW TO NETWORK CONTAIN AN INFECTED SYSTEM WITH CROWDSTRIKE FALCON



In this video, we will show you how to use the network containment feature in CrowdStrike Falcon to isolate an infected system from the network. This feature is designed to prevent malware from spreading across the network and to help administrators contain a breach. The video covers the steps to identify an infected system, select the appropriate network, and apply the containment policy. It also discusses the benefits of network containment, such as reducing the attack surface and preventing lateral movement. For more information, visit <https://www.crowdstrike.com/resources/videos/how-to-contain-an-infected-system/>.

### More to explore

- [CrowdStrike Falcon - Introduction](#)
- [Respond to a CrowdStrike Falcon Endpoint Protection Event](#)
- [Identify a CrowdStrike Falcon Endpoint Protection Event](#)
- [Respond to a CrowdStrike Falcon Endpoint Protection Event](#)

CrowdStrike Falcon® capability is also referred to as “network quarantine” or “network isolation” and is typically used by administrators to remove an infected (or possibly infected) system from the network. This removes the ability for malware to spread or for an attacker to move laterally across the network. With CrowdStrike Falcon®, once a system is network contained, it can only make network connections to the CrowdStrike cloud infrastructure or to local IPs that are specified by the administrator. It is also possible to un-contain a system after the system is verified as clean.

A handwritten signature or mark, possibly initials, located at the bottom right of the page.

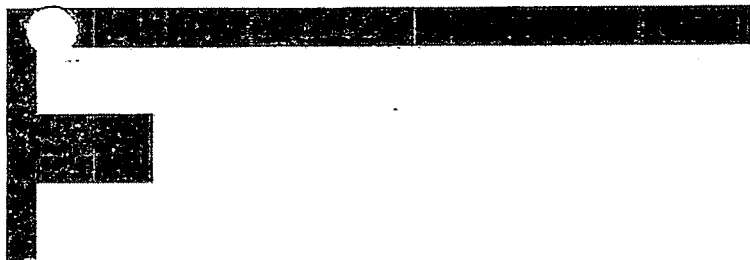
## Preventing malware with custom blocking

There are cases when you might want to block applications because you are certain that you never want them to run in your environment.

Falcon allows you to upload hashes from your own black or white lists. To enable this, navigate to the Configuration App, Prevention hashes window, and click on "Upload Hashes" in the upper right-hand corner. Note that you can also automate the task of [importing hashes with the CrowdStrike Falcon® API](#).

### Configuration App

---



Then we can either browse to a file or paste a list directly into the windows. The list can be a text file with one MD5 or SHA256 hash per line. All valid MD5 and SHA256 hashes will be uploaded. Rows with non-MD5/SHA256 hash format will be ignored.

The list of hashes must meet the following criteria:

- Formatted as a plain text (.txt) file
- Contains up to 3,000 MD5 and SHA256 hashes (per file)
- Contains one MD5 or SHA256 hash per line



# FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

## FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

## KEY PRODUCT CAPABILITIES

### SIMPLIFY DETECTION AND RESOLUTION

- ▣ **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- ▣ **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- ▣ **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- ▣ **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

## KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep real-time forensics and sophisticated visualizations

Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

## CrowdStrike Products

### FALCON ENDPOINT DETECTION AND RESPONSE (EDR)

- **Respond decisively:** Act against adversaries in real time to stop attacks before they become breaches. Powerful response actions allow you to contain and investigate compromised systems, and Falcon Real Time Response capabilities provide direct access to endpoints under investigation. This allows security responders to run actions on the system and eradicate threats with surgical precision.

### GAIN FULL-SPECTRUM VISIBILITY IN REAL TIME

- **See the big picture in real time:** CrowdScore delivers a simple metric that helps an organization understand its threat level in real time. This makes it easy for security leaders to quickly understand if they are under attack and assess the severity of the threat so they can coordinate the appropriate response.
- **Capture critical details for threat hunting and forensic investigations:** Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.
- **Get answers in seconds:** The CrowdStrike Threat Graph® database stores event data and answers queries in five seconds or less, even across trillions of events.
- **Recall for up to 90 days:** Falcon Insight provides a complete record of endpoint activity over time, whether your environment consists of fewer than 100 endpoints or more than 500,000.
- **Streamline IT and security operations:** Falcon Fusion is a unified cloud-scale

security orchestration, automation and response (SOAR) framework, providing customizable and easy-to-use automation to simplify enterprise security workflows.

- **Understand endpoint security posture:** Falcon Insight provides a Zero Trust Assessment (ZTA) that determines endpoint health across the organization. With real-time security posture assessment, you can easily identify and update sensor policies and OS settings that are out-of-date or increase risk. Share assessment scores with CrowdStrike Zero Trust ecosystem partners for real-time conditional access enforcement.

### REALIZE IMMEDIATE TIME-TO-VALUE

- **Save time, effort and money:** Cloud-enabled Falcon Insight is delivered by the CrowdStrike Falcon platform and does not require any on-premises management infrastructure.
- **Deploy in minutes:** CrowdStrike customers can deploy the cloud-delivered Falcon agent to more than 100,000 endpoints globally in less than 24 hours.
- **Be immediately operational:** With unmatched detection and visibility from Day One, Falcon Insight hits the ground running, monitoring and recording on installation without requiring reboots, finetuning, baselining or complex configuration.
- **Experience no impact on the endpoint:** With only a lightweight agent on the endpoint, searches take place in the Threat Graph database without any performance impact on endpoints or the network.

## INDUSTRY RECOGNITION

CrowdStrike is recognized as a leader in endpoint protection solutions by industry analysts, independent testing organizations and security professionals. Visit the [CrowdStrike Industry Recognition webpage](#) for more information.

## ABOUT CROWDSTRIKE

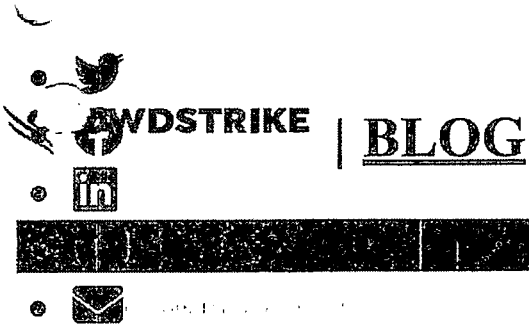
CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Start Free Trial  
of Next-Gen AV

Learn more at [www.crowdstrike.com](http://www.crowdstrike.com)

© 2021 CrowdStrike, Inc. All rights reserved.





## Real Time Response Policies

The default Real Time Response policy allows for basic functionality on managed endpoints. Falcon administrators can create and modify those policies to enable the right level of response actions as needed within the organization or for specific endpoint groups. [Detailed documentation](#) on Real Time Response policies is available in the Falcon UI.

## Conclusion

Real Time Response is a powerful tool that gives security administrations the ability to remotely access systems for administration tasks, remediation actions or forensics collection, etc. without requiring physical access to the system. For more information on the CrowdStrike solution,

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



# FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Streamlining the threat detection and response lifecycle with speed, automation and unrivaled visibility

## FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. All endpoint activity is also streamed to the CrowdStrike Falcon® platform so that security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

## KEY PRODUCT CAPABILITIES

### SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

## KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep real-time forensics and sophisticated visualizations

Respond and remediate with confidence

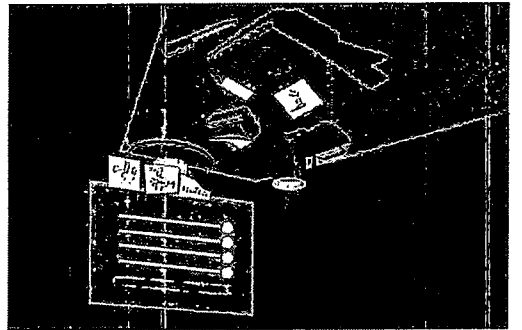
See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

### CrowdStrike Services Offers Incident Response Tracker for the DFIR Community

CrowdStrike Services is releasing a tracker spreadsheet to assist the Digital Forensics and Incident Response (DFIR) community during incident response investigations



- The CrowdStrike Incident Response Tracker is a convenient spreadsheet that includes sections to document indicators of compromise, affected accounts, compromised systems and a timeline of significant events
- Download the Incident Response Tracker spreadsheet

During a recent client engagement for a laptop exercise (LTX), it became apparent that the client did not have a methodology for tracking indicators and building an incident timeline. The CrowdStrike Services team wanted to provide more information to our clients on how incidents can and should be tracked, but nothing was available in the public domain that was simple to implement and could be immediately leveraged by responders. To address this gap, we are releasing the CrowdStrike Incident Response Tracker spreadsheet, which is organized into a number of tabs to record various classes of incident-related events in a structured and repeatable manner.

Typical forensic investigations typically involve reviewing system images, memory snapshots, logs and other data sources. This results in volumes of evidence tracking, hashing and technical findings across many workstreams.

Though effective response results on many elements working harmoniously together, accurately recording and communicating investigative findings is arguably the most critical. One way to do so is to utilize a structured incident response tracker for each investigation that can be used to consolidate and communicate pertinent information in a repeatable fashion. The section below describes how the CrowdStrike Incident Response (IR) Tracker can be utilized and some of the ways it can make managing an incident just a little bit easier.

#### CrowdStrike IR Tracker Overview

The benefit of using a tool like the CrowdStrike IR Tracker is that it provides a single place for synthesizing key incident information, including:

- A consolidated incident timeline that forms the basis of the incident narrative
- Incident indicators (e.g., IP addresses, domain names, malware names/hashes, registry entries, etc.)
- Affected account details and systems of interest
- Incident metadata such as key contacts, meeting details, collected evidence items and incident-related requests and tasks

Specifically, the CrowdStrike IR Tracker consists of the following tabs:

- Investigation Notes: Area for tracking investigation information such as related incident tickets, conference room and teleconference bridge details, etc.
- Contact Info: External and internal contact information for relevant response personnel
- Timeline: Chronological list of attacker activity and related events
- Systems: Systems accessed or compromised by the threat actor(s)
- Accounts: Accounts exposed or compromised by the threat actor(s)
- Host Indicators: File names, directory paths, cryptographic hashes, registry entries, etc., of interest to the investigation (more detail provided below)
- Network Indicators: External IP addresses, URLs, domain names, user agent strings, etc., of interest to the investigation (more detail provided below)
- Request and Task Tracker: Area for tracking incident-related requests and tasks
- Evidence Tracker: Area for tracking evidence collected during the investigation
- Forensic Keywords: Incident-specific keywords to facilitate forensic analysis
- Investigative Queries: Incident-specific queries for SIEM, log correlation and investigative platforms to facilitate investigative analysis

An overview of three of our favorite and most heavily leveraged IR Tracker tabs are described below.

#### Host Indicators Tab

First, the Host Indicators tab is used to record the suspected and confirmed host indicators for the incident. Common examples of host indicators include file names and paths, file hashes, file sizes, service names and registry keys. Having this information readily available for the investigation teams speeds up the analysis and investigation processes. Recording host indicators in a single location gives the team the ability to search for these across additional data sets and pivot to associated indicators from further analysis, and it provides inputs for detection and prevention tools such as a security information and event management (SIEM) or endpoint detection and response (EDR) platform.

CROWDSTRIKE BLOG

Home Videos Categories Sign Free Trial

How the TTPs of the Incident

A fictitious example timeline extract is shown below. There is a lot of information in this very short timeline extract, but we can see that there has been credential access through a number of utilities, webshells, reconnaissance tools and lateral movement. We can also see the times of activity from the threat actor(s) on multiple systems, ranging from Sept. 16, 2021, through Sept. 28, 2021.

Analyst	Date	Status/Tag	System Name	Date/Time (UTC)	Type	Activity	Evidence Source	Data/Comment	ATT&CK Alliances
Analyst1	2021/09/25	Confirmed	SYSTEM-WEB	2021-09-16T01:53:43.254Z	FN Creation	C:\logs\cmd.exe	MFT	Memcatz	Credential Access
Analyst2	2021/09/25	Confirmed	SYSTEM-WEB	2021-09-16T01:35:42.151Z	FN Creation	C:\logs\cmd.exe	MFT	ProcDump	Credential Access
Analyst2	2021/09/25	Confirmed	SYSTEM-WEB	2021-09-16T01:56:46.68Z	FN Creation	C:\logs\cmd.exe	MFT	Webshell	Persistence
Analyst2	2021/09/25	Confirmed	SYSTEM-WEB	2021-09-16T01:58:45.123Z	FN Creation	C:\logs\cmd.exe	MFT	Memcatz	Credential Access
Analyst3	2021/09/25	Confirmed	SYSTEM-WEB	2021-09-16T01:07:17.819Z	FN Creation	C:\logs\PSEXEC.exe	MFT	PSEXEC	Discovery
Analyst3	2021/09/25	Confirmed	SYSTEM-WEB	2021-09-16T02:14:17.716Z	FN Creation	C:\logs\cmd.exe	MFT	Notepad	Discovery
Analyst3	2021/09/26	Confirmed	SYSTEM-WEB	2021-09-16T02:19:15.009Z	FN Creation	C:\logs\cmd.exe	MFT	TA Utility	
Analyst1	2021/09/26	Confirmed	SYSTEM-WEB	2021-09-16T08:27:03.400Z	FN Creation	C:\logs\cmd.exe	MFT	Dsget	Discovery
Analyst2	2021/09/26	Confirmed	SYSTEM-WEB	2021-09-16T08:27:45.21Z	FN Creation	C:\logs\cmd.exe	MFT	Dsquery	Discovery
Analyst1	2021/09/27	Confirmed	SYSTEM-WEB	2021-09-16T09:16:27.587Z	FN Creation	C:\logs\cmd.exe	MFT	WinRAR	Collection
Analyst3	2021/09/27	Confirmed	SYSTEM-WEB	2021-09-16T01:13:19.199Z	FN Creation	C:\data\inetpub\wwwroot\uploads\cmd.exe	MFT	Usgy	
Analyst1	2021/09/27	Confirmed	SYSTEM-WEB	2021-09-16T01:54:19.466Z	FN Creation	C:\data\inetpub\wwwroot\uploads\cmd.exe	MFT	Notepad	Discovery
Analyst2	2021/09/26	Suspicious	DESKTOP-JR7G2IH	2021-09-26T18:54:07.350Z	File Created	pathname: C:\Windows\PSEXESVC.exe ; TimeDateStamp: 2021-09-26T18:54:00Z ; cert: (optional: The file is signed and the signature was verified) cert_sgnr: Microsoft Corporation   original_filename: psexec.exe   productname: Sysinternals PSEXEC   productversion: 2.2	PEfile	Lateral Movement using PSEXEC	Lateral Movement

The word of warning — and the constant trap that all investigators deal with every day — is the data formatting in the CrowdStrike IR Tracker. Our strongest recommendation is to ensure that all dates are converted to UTC time (00:00) and in ISO 8601 date format. An example of this format is the following date and time: "2021-09-26T18:54:07.350Z." This same date format and consistency in time zone ensures that when we sort the timeline, the data is sorted chronologically. If there is a mess of date formats from different time zones to take into account, we will have a hard time understanding the threat actor's path through the network. If UTC time zone and ISO 8601 time format are always used in the timeline, then life will be a little bit easier. When running a complex investigation, having something that is easier matters, and frankly, when it comes to incidents, being accurate and efficient is paramount.

Conclusion

With this consolidated and organized information, we can focus on helping the organization identify the impact to business assets, and in conjunction with legal counsel, identify any regulatory reporting requirements. The CrowdStrike IR Tracker also helps ensure that the root cause of the incident gets identified, so your organization can remediate the vulnerabilities that were exploited and led to the incident. To make the incident easier to understand for business, we often create attack diagrams or graphical timelines from the consolidated Timeline tab. CrowdStrike often creates these diagrams to succinctly explain incidents for clients that have experienced extensive data breaches of hundreds of systems or over multiple years. Finally, it is recommended to use an online collaboration spreadsheet technology such as Office 365 or Google Sheets. Using collaboration tools provides an efficient means for different people to update an online document concurrently and minimizes the risk of versioning issues. Data is also updated in near real time, which helps teams communicate effectively. Some of the repetitive copy and paste tasks can be automated with the scripting features provided by the collaboration technology, but we will leave that for a follow-up blog, and we are happy to hear your ideas on how to minimize the effort on keeping the tracker up to date. The CrowdStrike IR Tracker itself is not a panacea to cure all ills of the IR process, but rather a tool that, if used correctly, can greatly increase efficiency of collaboration between individuals and teams. Like all tools, it must be used correctly, and one of the key tenets of the CrowdStrike IR teams is our "tracker hygiene." We know that if the CrowdStrike IR Tracker is not maintained then the results are going to be poor. The tracker gives back, but it can only give back from the effort that is put into it by ALL team members, ALL of the time. Maintaining the tracker for the incident takes work and discipline, but it is our belief that it is very much worth the effort. CrowdStrike is sharing the CrowdStrike Incident Response Tracker Template to give the DFIR community a starting point for collecting and recording incident artifacts in a consolidated and organized fashion. It is our hope that this resource is a useful baseline for building upon within your own organization — or when an IR tracker is needed on short notice.

Additional Resources

- To request more information or speak with a CrowdStrike Services representative, contact your account manager.
- Learn about the powerful, cloud-native CrowdStrike Cloud Managed Security Solutions that protect your business.
- Get inside story from our CrowdStrike Falcon Expert Program to see for yourself how true next-gen AV performs against today's most sophisticated threats.



Related Content



Handwritten signature

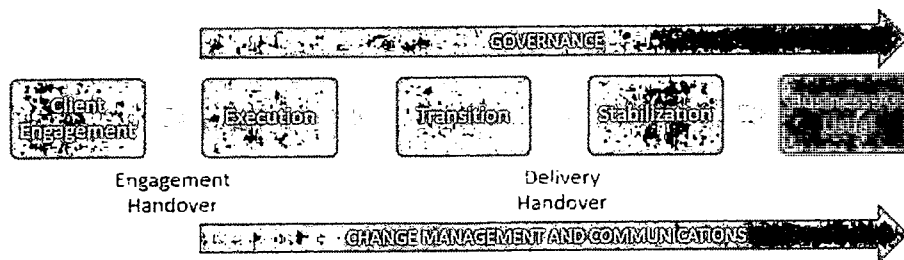
**A.3 Security Information  
and Event Management  
(SIEM)**



## PROJECT MANAGEMENT PROGRAM PLAN FOR GOVERNMENT INSURANCE CLUSTER

To ensure the compliance and delivery of the requirements by the Government Insurance Cluster, **TRENDS** will provide a Project Management Program below:

Trends will use a two-pronged approach for project management. The project phases are planned to use the Waterfall Project Management methodology while the actual tasks execution utilizes Agile Methodology.



### 1. Client Engagement.

During the Post Qualification Evaluation, Trends will demonstrate the salient features of the proposed Shared Cyber Defense solution at the Project Site or via online.

Trends will assign the needed Project Manager and technical resources and will conduct kickoff activity to ensure that every team member understands the engagement approach. All facets of the project including manner of implementation, scope, requirements, and acceptance criteria will be discussed during the kickoff activity.

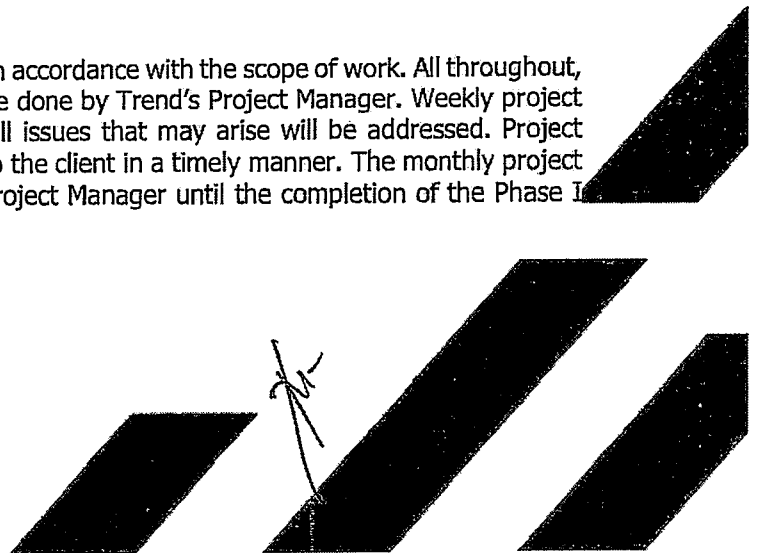
### 2. Execution.

Trends will implement the proposed solution in accordance with the scope of work. All throughout, monitoring of implementation activities will be done by Trend's Project Manager. Weekly project meetings will be conducted to ensure that all issues that may arise will be addressed. Project status updates and reports will be provided to the client in a timely manner. The monthly project monitoring report will be discussed by the Project Manager until the completion of the Phase I

### Trends & Technologies, Inc.

6th Floor Trafalgar Plaza  
105 H.V. Dela Costa Street, Salcedo Village  
Makati City 1227 Philippines

Phone: +63 2 8811 8181 Fax: +63 2 8814 0130  
www.trends.com.ph



and Phase II of the project, as defined in the Delivery Time/ Completion Schedule. The Project Manager shall be required to be onsite in any agency, by schedule, if necessary.

### ***3. Transition.***

Client onboarding will be done by Trends Service Transition Team to establish the service delivery processes and to ensure completeness of SOC visibility and familiarization with clients' processes and network behaviors.

Guided by the CIS Controls Framework, Trends will conduct Information Security Maturity Assessment which is a comprehensive gap analysis and risk assessment of an organization's readiness to detect, prevent, contain, and respond to threats to information systems. This takes on a holistic look on the organization's people, process, and technology to provide insights and understand vulnerabilities, identify, and prioritize remediation activities and demonstrate compliance.

Under CSC Control 17. Incident Response Management for Information Security Maturity Assessment, Trends will review agencies Incident Response Plan (IRP) which would guide the agencies on the creation, enhancement, and documentation of incident response playbooks, policies, and guidelines such as, but not limited to:

- Escalation process
- Incident containment process
- Incident eradication process
- Incident recovery process
- Incident identification process
- Process flow

Once the solution has been implemented, Trends will conduct process discovery and workshop, develop use cases, create playbooks and runbooks, and conduct tabletop exercises with the client. Trends will map security playbook and runbooks for applicable security use cases to guide client on their incident response. The playbooks and runbooks shall be signed off by the client and a signed Certificate of Completion and Acceptance (COCA) shall be issued to Trends by the client.

### ***4. Stabilization.***

Trends will validate that the systems are able to detect and respond to potential threats. Trends will perform fine tuning and comprehensive testing to verify the effectiveness of the security measures put in place. During the stabilization period, the SLA will not be in effect. The SLA will become mandatory during the Business-As-Usual (BAU) period.

Once the Stabilization period ends, there should be a signed Certificate of Completion of Stabilization Period issued to Trends by the client.

### ***5. Business-As-Usual.***

Once tools and technologies are installed and relevant stakeholders signed off the Certificate of Completion of Stabilization Period, Trends Operation Center will provide proactive monitoring, detection, and response to security incidents and cyber threats of Government Insurance Cluster.

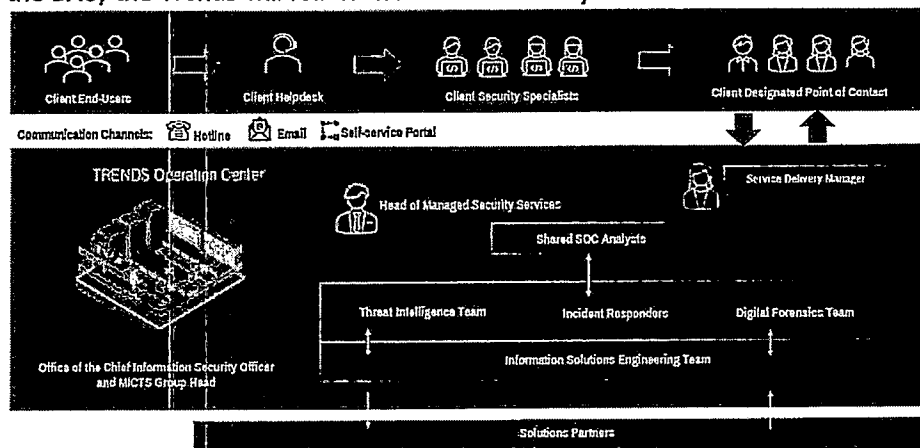


Trends will provide individual agency, web-based dashboards for accessing their agency information about alerts, attacks, track remediation on incidents, generate and extract reports which can be presented near real-time or over a period of time.

Moreover, Trends, through its cloud SIEM platform, will ensure the availability of the ingested raw logs twelve (12) months with comprehensive searchability. The logs, including evidence of security incidents, should be tamper proof and made available for legal and regulatory purposes, as required. The logs beyond the retention period shall be archived and given monthly to the agencies in an agreed format. Agencies will provide a storage repository for the archived logs.

Service Delivery Architecture

During the BAU, the Trends will follow the Service Delivery Architecture below:



Trends Security Operation Center (SOC) team will perform 24x7x365 monitoring services performed remotely at Trends Operations Center (TOC) located in Trends-MICTS Head Office Makati City, Philippines.

Trends will assign a Service Delivery Manager (SDM) to facilitate the delivery of the managed services and serve as the initial point of contact for any escalation. On the other hand, the agencies will also assign their respective SDM as the initial point of contact including tracking and validating of requests.

The agencies can report incidents to their helpdesk support. Only their helpdesk support is allowed to report the incidents to Trends SOC team for verification and authentication purposes.

Should there be any incidents not captured on the monitoring tool, the agency can report the incident through their SDM or helpdesk support, and contact Trends with the following details:

- Hotline: 8811-8181 extn: 8703, 8708, 8710 8715, 8716 and 8727
- Trends-SOC Email: [soc@trends.com.ph](mailto:soc@trends.com.ph)



- Ivanti ticket: <https://mictsv2-ism.trends.com.ph/HEAT/>

Manpower Resources

Trends will have a dedicated 24x7x365 team assigned to the Government Insurance Cluster, composed of the following with their respective roles and responsibilities:

<b>Personnel</b>	<b>Roles and Responsibilities</b>
SOC Manager or Tier 4 Analyst (1)	In charge of strategy, priorities and the direct management of SOC staff when major security incidents occur.  Responsible for the management of the MSOC operations for the agency and cluster.
Tier 3 Analyst (1)	Responsible for managing critical incidents. Responsible for actively hunting for threats and assessing the vulnerability of the business. 1. Manage High Severity Triage 2. Incident Response and Forensics Capabilities 3. Threat Containment (Using Existing EDR or agreed process) 4. Reporting and Post Incident Review 5. Use Case Development 6. Threat Searches 7. New Correlation Rules
Tier 2 Analyst (1)	Responsible for conducting further analysis and deciding on a strategy for containment. 1. Proactive Searches/ Threat Hunting 2. Qualification of Incident Priority/Severity 3. Investigation via SIEM/Analytics Platform and other accessible sources 4. Rule Tuning 5. Ad hoc Vulnerability Advisory & Research 6. Threat Containment (Using Existing EDR or agreed process) 7. Incident Response/Recommendations
Tier 1 Analysts (2)	Responsible for the following tasks: 1. Monitoring via existing SIEM/Analytics Platform 2. Funneling of alerts (noise elimination) 3. Incident Validation 4. Case Management 5. Threat Containment (Using Existing EDR or agreed process) – with guidance from L2 and up 6. General Communication 7. Weekly Summary Reports

Furthermore, Trends will also ensure that there will be alternate personnel deployed to the Insurance Cluster should the primary personnel be unavailable for whatever reason.

Reports and Meetings

- **Monthly Service Performance Report.**

The assigned dedicated local SOC Manager that will oversee that SOC and conduct regular monthly service performance review and reporting to client's management. The monthly service performance report which contains the status of cases and the assistance needed from the client, will be submitted and discussed by the SOC Manager. The monthly service performance report will include the following:

- SLA Performance
- Correlated Events Overview
- Correlated Events Graph Distribution Overtime
- Correlated Events and Rules Triggered Summary
- Summary of Incident Ticker per Use Cases Incident Management

- **Regular Email Advisory and Intelligence Summary Reports**

Trends will also provide regular email advisory and intelligence summary reports on the latest local and international news, latest cyber threats, and updates in Cyber security space, including detected information on the intention to target agencies or other government industries, major activist campaigns, and indications of activism against the agencies, financial and health sector, and the government.

However, a **special report or notice to the agencies** immediately, should there be any information or detection of targeted attacks against the agencies, the government or the sectors of the concerned agencies.

- **Monthly Service Performance Review Meeting.**

Led by the SOC Manager, Trends shall conduct monthly meetings with the agencies IT stakeholders to review SOC performance and discuss the overall IT security posture of the agencies, including fine-tuning of configurations and provision of best practices advice, to aid in continuous improvement.

Furthermore, Trends will also facilitate SOC security briefings to IT and CxOs and key decision-makers to discuss the intelligence summary reports and to share emerging technology trends and the risks associated with it, new regulations, complexity and sophistication of threats, requirement for companies to cyber-resilient among others.

*[Handwritten signature]*

- Top threat lists
  - Threat type to event
  - Threat type to event
- Overall number of security events listed

### Common use cases

You can use investigations and reports to quickly assess your overall posture and SOC operations. This gives you team and executive real-time insight into operational security and how incidents are being managed. Having easy access to this (higher) level of information allows for quick action and reporting and keeps the key stakeholders informed as they

### Aim and strategy

- Real-time visibility: See security events in real-time through extensive dashboards and visualizations. This enables you to quickly detect anomalies, investigate incidents, and respond to threats as they happen.
- Actionable insights: The investigations and reports in Splunk Enterprise Security provide actionable insights into security events, assisting security analysts to identify patterns and trends that may indicate a potential security breach.
- Customizable reports: Splunk Enterprise Security comes with a range of built-in reports that cover a variety of security use cases, but you can also customize these reports to meet your specific needs. This can help you get a more accurate and comprehensive view of your security posture.
- Compliance reporting: Splunk Enterprise Security provides built-in compliance reporting capabilities, allowing you to easily generate reports that demonstrate compliance with regulatory requirements such as PCI DSS, HIPAA, and GDPR.
- Integration with third-party tools: Splunk Enterprise Security integrates with a wide range of third-party tools, including threat intelligence feeds, vulnerability scanners, and incident response platforms. These integrations allow you to correlate security events across multiple data sources, and respond to threats more quickly and effectively.

Some of the key benefits are:

Splunk Enterprise Security provides a number of benefits in terms of detection and response that can help organizations detect and respond to security breaches more effectively.

- Home > Security > Use Case Explorer for Security > Prescribed Actions > Visualizations and reports > Prescriptive Adoption Motion - Visualizations and reports

lantern.splunk.com/.../Prescribed Actions - Visualizations and reports > Prescriptive Adoption Motion - Visualizations and reports

- Investigative: Access a flexible workspace for analysts to explore and investigate security events and incidents.
  - Compliance: Assess your compliance posture, allowing you to monitor compliance with regulatory standards and best practices.
  - Risk Analysis: Understand the risk associated with different assets at your IT infrastructure, allowing you to prioritize your security efforts based on the level of risk.
  - Identity: Access user and identity-related activity across your IT infrastructure.
  - Network: Get network activity across your IT infrastructure, including activity related to network intrusion attempts and data exfiltration.
  - Endpoint: View endpoint activity across your IT infrastructure, including activity related to malware infections and other security threats.
  - Threat Activity: Get a real-time view of threat activity across your IT infrastructure, allowing you to identify potential threats and respond to them quickly.
  - Incident Review: View a comprehensive view of all security incidents and threat analysis to old from time-reversed incidents to investigate and respond to security threats.
- Splunk Enterprise Security includes a number of built-in dashboards that provide real-time visibility into security events and help security analysts identify and respond to security threats. Here are some of the key dashboards:

## Prescriptive Adoption Motion - Visualizations and reports

- Home > Security > Use Case Explorer for Security > Prescribed Actions > Visualizations and reports > Prescriptive Adoption Motion - Visualizations and reports

How often do they view?

splunk.com/.../Prescribed Actions - Visualizations and reports > Prescriptive Adoption Motion - Visualizations and reports

lantern.splunk.com/.../Prescribed Actions - Visualizations and reports > Prescriptive Adoption Motion - Visualizations and reports

Splunk Cloud Platform

# Reporting Manual

Download manual as PDF ([/index.php?title=Documentation:SplunkCloud:Report:Createandeditreports:8.1.2012&action=pdfbook&version=9.0.2305&product=SplunkCloud](#))

Product

Splunk Cloud Platform™

Version

9.0.2305 (latest FedRAMP release) (latest release)

Documentation (/Documentation) / Splunk Cloud Platform (/Documentation/SplunkCloud)  
 / Reporting Manual (/Documentation/SplunkCloud/latest/Report)  
 / Create and edit reports (/Documentation/SplunkCloud/latest/Report/Createandeditreports)

Download topic as PDF ([/index.php?title=Documentation:SplunkCloud:Report:Createandeditreports:8.1.2012&action=pdfbook&version=9.0.2305&topic=1&product=SplunkCloud](#))

## Create and edit reports

When you create a search or a pivot that you would like to run again or share with others, you can save it as a report. This means that you can create reports from both the Search and the Pivot sides of the Splunk platform.

Once you create a report you can:

- View the results that the report returns on the report viewing page or Splunk Mobile. You can get to the viewing page for a report by clicking the name of the report on the Reports listing page. See [View reports in Splunk Mobile](#) (<http://docs.splunk.com/Documentation/Alerts/2.36.0/Alerts/ViewReports>) in the *Download and Use Splunk Mobile* manual to learn more about viewing reports on your mobile device.
- Open the report and edit it so that it returns different data or displays its data in a different manner. Your report opens in either Pivot or Search, depending on how it was created.

In addition, if your permissions enable you to do so, you can:

- Change the report permissions to share it with other Splunk users. See [Set report permissions](#), (<http://docs.splunk.com/Documentation/Splunk/9.1.1/Report/Managereportpermissions>) in this manual.
- Schedule the report so that it runs on a regular interval. Scheduled reports can perform actions each time they run, such as sending report results via email to a set of stakeholders. See [Schedule reports](#), (<http://docs.splunk.com/Documentation/Splunk/9.1.1/Report/Schedulereports>) in this manual.
- Accelerate slow-completing reports built in Search. See [Accelerate reports](#), (<http://docs.splunk.com/Documentation/Splunk/9.1.1/Report/Acceleratereports>) in this manual.
- Embed scheduled reports in external websites. See [Embed scheduled reports](#), (<http://docs.splunk.com/Documentation/Splunk/9.1.1/Report/Embedscheduledreports>) in this manual.
- Add the report to a dashboard as a dashboard panel. See [Add panels to dashboards](#) (<http://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Viz/AddPanels>) in the *Dashboards and Visualizations* manual.

**Note:** Permissions for reports built via Pivot must match those of the data model that was used to construct them. See "Permissions for Pivot-based reports," ([http://docs.splunk.com/Documentation/Splunk/9.1.1/Report/Managereportpermissions#Permissions\\_for\\_Pivot-based\\_reports](http://docs.splunk.com/Documentation/Splunk/9.1.1/Report/Managereportpermissions#Permissions_for_Pivot-based_reports)), in this manual.

## Manually create a report in Splunk Web

You can create reports via Splunk Web four ways:

- From Search, by saving a search as a report
- From Pivot, by saving a pivot as a report
- By selecting **Settings > Searches, reports, and alerts** and clicking **New Report** to add a new report.
- From a dashboard, by converting an inline-search-powered dashboard panel to a report.

See the following subsections for more information about these report creation methods.

### Save a search or pivot as a report from the Search or Pivot views

When you design a search or pivot that returns useful results, you can save it as a report. The report retains any formatting that you set up for the original search, including chart visualizations and event list display options.

**Note:** You can only save a search as a report when it is running, paused, finalized, or completed.

1. Run a search or design a pivot that is worth saving as a report.
2. Click **Save As** and select **Report** to save the search or pivot as a report. The report retains any formatting that you set up for the original search, including chart visualizations and event list display options.
3. Provide a unique **Title** for the report. Supported characters for titles are a-z, A-Z, 0-9, or \_.
4. (Optional) Provide a **Description** of the report.
5. (Optional) Add a time range picker to the report. A time range picker allows users without write permissions to rerun the report over a different time range without actually editing it.

splunk > (https://www.splunk.com)

Splunk Cloud Platform™

# Search Tutorial

Download manual as PDF (Index.php?title=Documentation:SplunkSearchTutorial>Aboutdashboards:8.2.0&action=pdfbook&version=9.0.2305&product=SplunkCloud)

Product

Splunk Cloud Platform™

Version

9.0.2305 (latest FedRAMP release) (latest release)

Documentation (/Documentation) / Splunk Cloud Platform™ (/Documentation/SplunkCloud) / Search Tutorial (/Documentation/SplunkCloud/latest/SearchTutorial) / About dashboards (/Documentation/SplunkCloud/latest/SearchTutorial/Aboutdashboards)

Download topic as PDF (Index.php?title=Documentation:SplunkSearchTutorial>Aboutdashboards:8.2.0&action=pdfbook&version=9.0.2305&topic=18&product=SplunkCloud)

## About dashboards

Dashboards are views that are made up of panels. The panels can contain modules such as search boxes, fields, charts, tables, and lists. Dashboard panels are usually connected to reports.

After you create a search visualization or save a report, you can add it to a new or existing dashboard. There is also a Dashboard Editor that you can use to create and edit dashboards. The Dashboard Editor is useful when you have a set of saved reports that you want to quickly add to a dashboard.

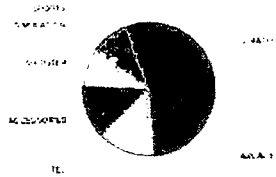
### Buttercup Games - Purchases

Reports on Buttercup Games purchases data

Time range

Previous views Hide from

Top Purchases by Category



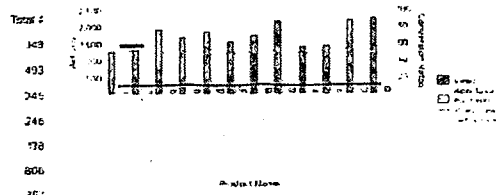
Here is an example of dashboard.

Purchasing trends

- Category C
- ACCESSORIES
- ARCADE
- STRATEGY
- SIMULATION
- SPORTS
- STRATEGY
- ICE

Purchases Trend C

Comparison of Actions and Conversion Rates by Product



(/File:7.1.0\_morepanels\_rearrange2-compressor.png)

## Change dashboard permissions

You can grant access to a dashboard from the Dashboard Editor. However, your user role and capabilities defined for that role might limit the type of access you can define.



splunk > (<https://www.splunk.com>)

Splunk Cloud Platform™

## Getting Data In

Download manual as PDF ([/index.php?title=Documentation:Splunk:Data:WhatSplunkcanmonitor:7.0.0&action=pdfbook&version=9.0.2305&product=SplunkCloud](#))

Product

Splunk Cloud Platform™

Version

9.0.2305 (latest FedRAMP release) (latest release)

[Documentation \(/Documentation\)](#) / [Splunk Cloud Platform™ \(/Documentation/SplunkCloud\)](#) / [Getting Data In \(/Documentation/SplunkCloud/latest/Data\)](#) / [What data can I index? \(/Documentation/SplunkCloud/latest/Data/WhatSplunkcanmonitor\)](#)

Download topic as PDF ([/index.php?title=Documentation:Splunk:Data:WhatSplunkcanmonitor:7.0.0&action=pdfbook&version=9.0.2305&topic=1&product=SplunkCloud](#))

### What data can I index?

The Splunk platform can index ([/Splixicon:Index](#)) any kind of data. In particular, the Splunk platform can index any and all IT streaming, machine, and historical data, such as Microsoft Windows event logs, web server logs, live application logs, network feeds, metrics ([/Splixicon:Metric](#)), change monitoring, message queues, archive files, and so on.

#### Types of data sources in Splunk Cloud Platform

Splunk Cloud Platform provides tools to configure many kinds of data inputs, including those that are specific to particular application needs. Splunk Cloud Platform also provides the tools to configure any arbitrary data input types. In general, you can categorize Splunk Cloud Platform inputs as follows:

- Files and directories
- Network events
- Windows sources
- HTTP Event Collector (HEC)
- Metrics

##### Files and directories

A lot of data comes directly from files and directories. You can use universal ([/Splixicon:Universalforwarder](#)) and heavy forwarders ([/Splixicon:Heavyforwarder](#)) to monitor those files and directories and send them to Splunk Cloud Platform. As a best practice, install universal forwarders on every machine where you want to monitor files and directories and send that data to a heavy forwarder which then sends the data to Splunk Cloud Platform. To monitor files and directories, see [Get data from files and directories \(<http://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Data/MonitorFilesAndDirectories>\)](#).

##### Network events

You might want to collect data from network ports, such as network data from machines that run syslog. To do this in Splunk Cloud Platform, use a heavy or universal forwarder to collect the network data and then send that data to Splunk Cloud Platform. To get data from network ports, see [Get data from TCP and UDP ports \(<http://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Data/Monitornetworkports>\)](#).

##### Windows sources

To get data from Windows sources into Splunk Cloud Platform, install the Splunk Add-on for Windows on your universal forwarder. In this scenario, you can use a deployment server to deliver the Splunk Add-on for Windows to the Windows machines you want to monitor. The add-on collects the data and sends it to Splunk Cloud Platform.

For additional information on getting Windows data into Splunk Cloud Platform, see [Get Windows Data Into Splunk Cloud Platform \(<http://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Admin/WindowsGD>\)](#) in the Splunk Cloud Platform *Admin Manual*.

##### HTTP Event Collector

In Splunk Cloud Platform, you can use the HTTP Event Collector to get data directly from a source with the HTTP or HTTPS protocols. For more information, see [The HTTP Event Collector endpoint \(<http://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Data/UseetheHTTPEventCollector>\)](#).

##### Metrics

You can also get metrics data from your technology infrastructure, security systems, and business applications. For more information, see [Metrics \(<http://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Metrics/Overview>\)](#).

#### Types of data sources in Splunk Enterprise

Because Splunk Enterprise is on-premises, you can either get data into the instance directly or use universal or heavy forwarders to get data in. In general, you can categorize Splunk Enterprise inputs as follows:

- Files and directories
- Network events
- Windows data

# Cloud Security at Splunk

## Cloud Infrastructure

Splunk uses a range of technologies to prevent unauthorized access or compromise of Splunk's network, servers or applications, which include, such things as logical and physical controls to segment data, systems and networks. Splunk monitors demarcation points used to restrict access such as firewalls and security group enforcement points. Remote users must authenticate with two-factor authentication prior to accessing Splunk networks containing customer content.

## Splunk Employee Access Control

Splunk grants system privileges and permissions to users with "least privilege" principle. Customer tasks are logically separated from each other. Splunk leverages the benefits of virtualization at the server, storage and network layers to ensure that there is strict

separation for each customer instance. Logical access policies and procedures delineate Splunk's required activities and responsibilities for credential management, user access provisioning, privileged access, monitoring and intrusion detection.

Role-based access and audit controls allow our customers to manage the activities Splunk users can take and what data tools and dashboards they can access.

- ▶ Learn more about configuring role-based user access and audit controls.
- ▶ To learn how you can role map to your organization's data access policies for different classes of users, you can also use Lightweight Directory Access Protocol (LDAP) or Security Assertion Markup Language (SAML) groups to different roles.

## Splunk Employee and User Authentication

Authorized users supporting the delivery of Splunk services must identify and authenticate to the network, applications and platforms using their user ID and password. Splunk's enterprise password management system requires minimum password parameters, SSH key authentication and enterprise password management applications are used to manage access to the production environment and two-factor authentication (2FA) is required for remote access and privileged account access for customer content production systems.

Splunk supports single sign-on (SSO) integrations (SAML v2) with compliant identity providers such as Okta, PingFederate, Azure AD, ADFS, SA SiteMinder, OneLogin, Centrify, SecureAuth, IdentityMe, Oracle OpenSSO, Google SAML 2 provider and Optimal ID. Splunk also integrates with other authentication systems, including LDAP, Active Directory and e Directory.

- ▶ Learn how to configure single sign-on in on-premises environments with SAML
- ▶ Learn how to configure single sign-on in Splunk Cloud with SAML

## Data Anonymization

Splunk supports advanced anonymization to remove confidential data from data analysis results and queries.

## Secure Data Access and Processing

Splunk Cloud includes secure data processing through access controls, logging and monitoring, availability, threat and vulnerability management, encryption, incident management and third party audit. For more detail on the administrative, technical and physical safeguards Splunk deploys to protect customer content, see the Splunk Cloud Platform Security Addendum (CSA).

### On this page

- Cloud Infrastructure
- Splunk Employee Access Control
- Splunk Employee & User Authentication
- Data Anonymization
- Secure Data Access and Processing
- Data Segregation
- Data Encryption in Transit
- Data Encryption At Rest
- Asset Management and Disposal
- Change Management
- Vendor Risk Management
- Personal Security
- Physical Security
- Disaster Recovery Plan
- Threat and Vulnerability Management
- Intrusion Detection
- Logging and Monitoring
- Splunk Incident Response Framework (SIRF)

### Additional Resources

#### More for security

- ▶ Corporate Security
- ▶ Product Security



## Data Segregation

Spunk Cloud environments enforce logical separation of customer data.

### Data Encryption In Transit

Spunk Cloud uses industry standard SSL/TLS 1.2 (Secure Socket Layer/Transport Layer Security) encryption for data in transit. All networked and web sessions are secured in this manner. Email notifications are secured by opportunistic TLS encryption on email gateways.

### Data Encryption At Rest

Spunk Cloud stores data encryption at rest using Advanced Encryption Standard (AES) 256-bit encryption. Encryption at rest is available as a premium service enhancement that customers can purchase.

## Asset Management and Disposal

Spunk maintains an inventory of cloud infrastructure assets that it regularly updates and reconciles. Documented build procedures are used for installation and maintenance of production servers. Upon expiration or termination of contract, Spunk retains customer content for 30 days, after which documented data disposal practices are used for the secure disposal of content as set forth in the relevant customer agreement.

## Change Management

Spunk follows the standard change management procedures for application, infrastructure and product-related changes. Changes undergo review and testing, including security and code reviews, regression testing and user acceptance testing, before approval for implementation. Spunk employs changes during maintenance windows which are set forth in the relevant Support Program.



splunk> (<https://www.splunk.com>)

Splunk Cloud Platform™

## Getting Data In

Download manual as PDF ([/index.php?title=Documentation:Splunk:Data:WhatSplunkcanmonitor:7.0.0&action=pdfbook&version=9.0.2305&product=SplunkCloud](#))

Product

Splunk Cloud Platform™

Version |

9.0.2305 (latest FedRAMP release) (latest release)

Documentation (/Documentation) / Splunk Cloud Platform™ (/Documentation/SplunkCloud) / Getting Data In (/Documentation/SplunkCloud/latest/Data)  
/ What data can I index? (/Documentation/SplunkCloud/latest/Data/WhatSplunkcanmonitor)

Download topic as PDF ([/index.php?title=Documentation:Splunk:Data:WhatSplunkcanmonitor:7.0.0&action=pdfbook&version=9.0.2305&topic=4&product=SplunkCloud](#))

### What data can I index?

The Splunk platform can index (/Splexicon:Index) any kind of data. In particular, the Splunk platform can index any and all IT streaming, machine, and historical data, such as Microsoft Windows event logs, web server logs, live application logs, network feeds, metrics (/Splexicon:Metric), change monitoring, message queues, archive files, and so on.

#### Types of data sources in Splunk Cloud Platform

Splunk Cloud Platform provides tools to configure many kinds of data inputs, including those that are specific to particular application needs. Splunk Cloud Platform also provides the tools to configure any arbitrary data input types. In general, you can categorize Splunk Cloud Platform inputs as follows:

- Files and directories
- Network events
- Windows sources
- HTTP Event Collector (HEC)
- Metrics

##### Files and directories

A lot of data comes directly from files and directories. You can use *universal forwarders* (/Splexicon:Universalforwarder) and *heavy forwarders* (/Splexicon:Heavyforwarder) to monitor those files and directories and send them to Splunk Cloud Platform. As a best practice, install universal forwarders on every machine where you want to monitor files and directories and send that data to a heavy forwarder which then sends the data to Splunk Cloud Platform. To monitor files and directories, see [Get data from files and directories](#) (<http://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Data/MonitorFilesAndDirectories>).

##### Network events

You might want to collect data from network ports, such as network data from machines that run syslog. To do this in Splunk Cloud Platform, use a heavy or universal forwarder to collect the network data and then send that data to Splunk Cloud Platform. To get data from network ports, see [Get data from TCP and UDP ports](#) (<http://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Data/Monitornetworkports>).

##### Windows sources

To get data from Windows sources into Splunk Cloud Platform, install the Splunk Add-on for Windows on your universal forwarder. In this scenario, you can use a deployment server to deliver the Splunk Add-on for Windows to the Windows machines you want to monitor. The add-on collects the data and sends it to Splunk Cloud Platform.

For additional information on getting Windows data into Splunk Cloud Platform, see [Get Windows Data into Splunk Cloud Platform](#) (<http://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Admin/WindowsGDI>) in the Splunk Cloud Platform *Admin Manual*.

##### HTTP Event Collector

In Splunk Cloud Platform, you can use the HTTP Event Collector to get data directly from a source with the HTTP or HTTPS protocols. For more information, see [The HTTP Event Collector endpoint](#) (<http://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Data/UsetheHTTPEventCollector>).

##### Metrics

You can also get metrics data from your technology infrastructure, security systems, and business applications. For more information, see [Metrics](#) (<http://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Metrics/Overview>).

#### Types of data sources in Splunk Enterprise

Because Splunk Enterprise is on-premises, you can either get data into the instance directly or use universal or heavy forwarders to get data in. In general, you can categorize Splunk Enterprise inputs as follows:

- Files and directories
- Network events
- Windows data

# Discover Apps

Collections Apps

Find an app

When you see an app you're interested in, click here.

Showing 1-18 of 90 Results

PLATFORM

VERSION

PRODUCT

SPLUNK SOAR

VERSION

PRODUCT

CATEGORY

- IT Operations
- Security, Fraud & Compliance
- Business Analytics
- Uptime
- IoT & Industrial Data
- DevOps
- Directory Service
- Email
- Firewall
- Endpoint
- Generic
- Identity Management
- Information
- Investigative
- Network Access Control
- Network Device
- Network Security
- Reputation
- Sandbox
- SIEM
- Threat Intel
- Ticketing
- Virtualization
- Vulnerability Scanner

- Directory Service
- Email
- Firewall
- Endpoint

- Directory Service
- Email
- Firewall
- Endpoint

- Directory Service
- Email
- Firewall
- Endpoint

- Directory Service
- Email
- Firewall
- Endpoint

- Directory Service
- Email
- Firewall
- Endpoint

- Directory Service
- Email
- Firewall
- Endpoint

- Not Supported
- Splunk Supported
- Developer Supported

- This app uses the Windows endpoint investigation actions that are implemented in Windows endpoint investigation actions.
- This app integrates with Microsoft System Center Operations Manager (SCOM) to execute investigative actions.
- This app integrates with Microsoft System Center Configuration Manager (SCCM) to execute investigative actions.

- This app integrates with Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.

- This app integrates with the Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.

- This app integrates with the Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.

- This app integrates with the Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.

- This app integrates with the Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.

- This app integrates with the Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.

- This app integrates with the Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.
- This app integrates with the Windows Remote Management (WinRM) to execute various actions.

Sort by

PLATFORM

SOAR Cloud, SOAR On-Prem

RATING

★★★★★ (2)

DESCRIPTION

This app supports various investigations and containment actions on Carbon Black App Control (formerly Blis) and Carbon Black Defense (formerly Signal) App to retrieve and send data.

By Splunk Inc.

splunk

PLATFORM

SOAR Cloud, SOAR On-Prem

RATING

★★★★★ (10)

DESCRIPTION

This app integrates with the Windows Remote Management (WinRM) to execute various actions.

By Splunk Inc.

PLATFORM

SOAR Cloud, SOAR On-Prem

RATING

★★★★★ (10)

DESCRIPTION

This app integrates with Microsoft System Center Configuration Manager (SCCM) to execute investigative actions and containment, and corrective actions.

By Splunk Inc.

PLATFORM

SOAR Cloud, SOAR On-Prem

RATING

★★★★★ (1)

DESCRIPTION

This app supports incident updates and incident ingestion from Symantec Data Loss Prevention installation.

By Splunk Inc.

PLATFORM

SOAR Cloud, SOAR On-Prem

RATING

★★★★★ (1)

DESCRIPTION

This app integrates with the Windows Remote Management (WinRM) to execute various actions.

By Splunk Inc.

Splunk® App for Content Packs

# Overview of the Splunk App for Content Packs

Download manual as PDF ([Index.php?title=Documentation.ContentPackApp.Overview.2.0.0&action=pdfback&version=2.0.0&product=ContentPackApp](#))

Product

Splunk® App for Content Packs

Version

2.0.0 (latest release)

Documentation (/Documentation) / Splunk® App for Content Packs (/Documentation/ContentPackApp) / Overview of the Splunk App for Content Packs (/Documentation/ContentPackApp/latest/Overview) / Overview of the Splunk App for Content Packs (/Documentation/ContentPackApp/latest/Overview/Overview)

Download topic as PDF ([Index.php?title=Documentation.ContentPackApp.Overview.Overview.2.0.0&action=pdfback&version=2.0.0&topic=1&product=ContentPackApp](#))

# Overview of the Splunk App for Content Packs

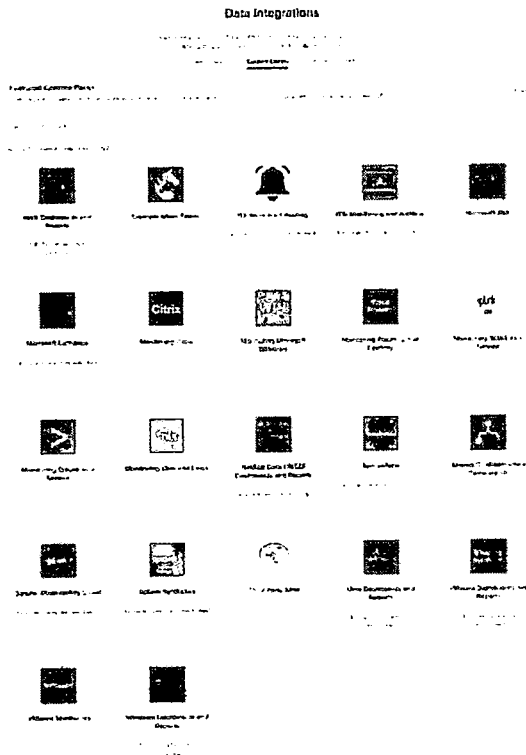
Splunk Content Packs provide prepackaged content that you can use to quickly set up your Splunk IT Service Intelligence (ITSI) or IT Essentials Work (ITE Work) environment. This content can include configured KPI base searches, service templates, saved glass tables, and other objects for use within ITSI or ITE Work.

The Splunk App for Content Packs lets you to access content packs, preview their contents, and install them in your environment. Download the Splunk App for Content Packs on Splunkbase (<https://splunkbase.splunk.com/app/5391/>). The Splunk App for Content Packs is compatible with ITSI and ITE Work versions 4.9.0 and higher. As new content packs become available or existing content packs are updated, you can download the most recent version of the Splunk App for Content Packs to get this new content. When you install an updated version of a content pack, you can see which objects are new to the content pack.

After you've installed the Splunk App for Content Packs, you can go to Configuration > Data Integrations. Depending on your version of ITSI or ITE Work select Content Library to see the available content packs.

Once installed, the objects within a content pack are configurable. If you want to change the frequency of a search frequency, adjust latency, or change calculation methods, you can edit the objects directly.

Most content packs process data collected through the use of Splunk add-ons. Add-ons collect host, network, and other data from computers that you install them on and map that data to a data model. Add-ons power the data underlying the metrics for each content pack. For more information, see About Splunk add-ons (<http://docs.splunk.com/Documentation/AddOns/released/Overview/AboutSplunkAdd-ons>) in the Splunk Add-ons manual.



(/File:Featured-contentpacks.png)

## Compatibility with ITSI and ITE Work

Splunkbase Version	ITE Work	ITSI
2.0.0	4.17.x	4.17.x
1.9.0	4.15.x, 4.16.x, 4.17.x	4.15.x, 4.15.x, 4.17.x
1.8.0	4.14.x, 4.15.x	4.14.x, 4.15.x
1.7.0	4.13.x, 4.14.x	4.13.x, 4.14.x



How can we help you?

Home > Security > Use Case Explorer for Security > Foundational Visibility > Security monitoring

## Security monitoring

Security Essentials



As a security analyst, you need to do the following to monitor your organization effectively:

- Enhance your attack surface coverage to include on-premises, hybrid, and multi-cloud environments
- Investigate and analyze with a comprehensive view across all your data sources for faster detection and response
- Ingest and normalize structured or unstructured data at scale, and use flexible data routing and storage options for cost optimization
- Rapidly extract value from data sources you already use with an open ecosystem of integrations and apps
- Leverage detailed security detections and data analytic stores that help get you to the answers without consuming excess time and resources or leaving risks unaddressed

Splunk Security Essentials meets these needs and improves security operations and investigations with an extensive library of over 900 pre-built detections and data recommendations for a multitude of Splunk environments: from Splunk Cloud Platform to Splunk Enterprise Security, and our Splunk SOAR offerings. These features enable organizations to implement content on demand and adapt to a dynamic security environment.

Home > Security > Use Case Explorer for Security > Foundational Visibility > Security monitoring

### Key features

SSE provides out-of-the-box security use cases and actionable security content to begin addressing threats and assessing gaps quickly and efficiently. You can leverage the wide-ranging use case library to eliminate gaps in defensive posture, implement detections, measure and justify new sources of data based on coverage of threats and risks to the business. Additionally, the deep integration with MITRE ATT&CK and Cyber Kill Chain helps you configure ES by pushing attributions to the Incident Review Dashboard, assess the level of coverage to ATT&CK tactics and techniques, and integrate risk-based events and alerting.

- **Security content library**
  - Browse, bookmark and deploy over 900 security detections with a few clicks
  - Find the right security content by filtering via use case, threat, data source or cybersecurity framework
  - Stay ahead of threats with content that pulls the latest detections from Splunk Threat Research Team.
- **Cybersecurity frameworks**
  - Automatically map your data to cybersecurity frameworks such as MITRE ATT&CK and Cyber Kill Chain
  - Measure your business posture against the frameworks and easily identify gaps to strengthen your defenses
  - Drill down on MITRE tactics, techniques, and threat groups to understand what detections are tied to different phases of the Kill Chain
- **Data and content introspection**
  - Inspect and analyze data and security content already in your environment
  - Gain a better understanding of your Splunk environment, as well as how your data is and can be Common Information Model (CIM) compliant
  - Enrich your existing security content with tags and metadata such as threat and data source categories, MITRE ATT&CK notes, and more
- **Security data journey**
  - Develop a maturity roadmap with security and data recommendations
  - Track and measure your progress through the Security Data Journey
  - Implement best practices and detections with the data you're already collecting
  - Prioritize ingestion of new data sources to increase coverage and reduce risks

In addition, you can curate your own content library by using the bookmarks feature in SSE. You can build a repository of security content for planning, know if you have data missing to make the content effective, track its implementation status, and export content in a variety of methods to easily integrate into another Splunk.



splunk> (<https://www.splunk.com>)

Splunk® Enterprise Security

# Use Splunk Enterprise Security

Download manual as PDF (/index.php?

title=Documentation:ES:User:Domaindashboards:7.0.1&action=pdfbook&version=7.2.0&product=ES)

## Product

Splunk® Enterprise Security

## Version

7.2.0 (latest release)

---

Documentation (/Documentation) / Splunk® Enterprise Security (/Documentation/ES)

/ Use Splunk Enterprise Security (/Documentation/ES/latest/User)

/ Introduction to the dashboards available in Splunk Enterprise Security

(/Documentation/ES/latest/User/Domaindashboards)

Download topic as PDF (/index.php?

title=Documentation:ES:User:Domaindashboards:7.0.1&action=pdfbook&version=7.2.0&topic=1&product=ES)

## Introduction to the dashboards available in Splunk Enterprise Security

Splunk Enterprise Security includes more than 100 dashboards that provide integrated views and communicate key data that might be customized and shared with intended end users. Splunk Enterprise Security dashboards identify and investigate security incidents, reveal insights in your events, accelerate incident investigations, monitor the status of various security domains, and audit your incident investigations and your ES deployment.

The specific dashboards that will be most useful to you depend on how you plan to use Splunk Enterprise Security.

### Identify and investigate security incidents

You can identify and investigate security incidents with a suite of dashboards and workflows. Splunk Enterprise Security uses **correlation searches** (/Splexicon:Correlationsearch) to identify **notable events** (/Splexicon:Notableevent) in your environment that represent security incidents.

- Security Posture provides a high-level overview of the notable events in your environment over the last 24 hours. Identify the security domains with the most incidents, and the most recent activity. See Security Posture dashboard (<http://docs.splunk.com/Documentation/ES/7.2.0/User/SecurityPosturedashboard>).
- Incident Review shows the details of all notable events identified in your environment. Triage, assign, and review the details of notable events from this dashboard. See Incident Review (<http://docs.splunk.com/Documentation/ES/7.2.0/User/IncidentReviewdashboard>).



Free Splunk

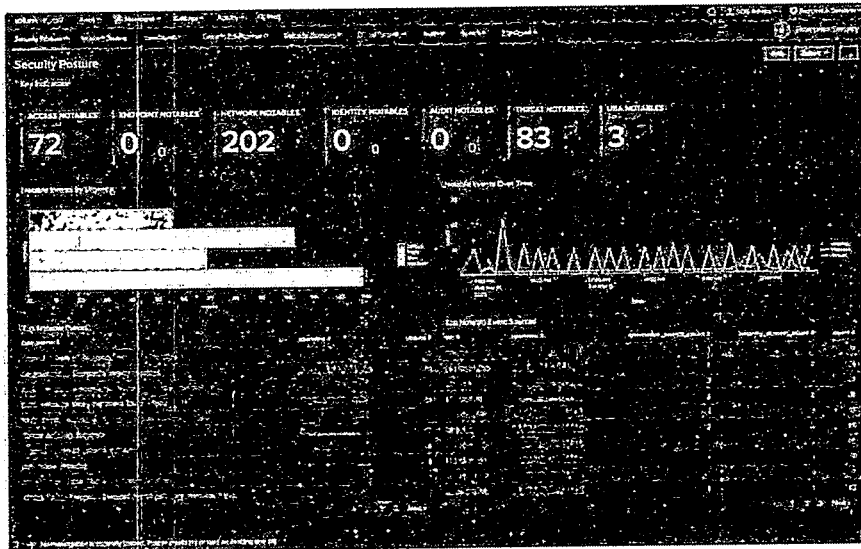


SECURITY

# Splunk Enterprise Security

Access data-driven insights, combat threats, protect your business and mitigate risk at scale with ML-powered analytics you can act on.

Take a Guided Tour



## How It Works

Splunk Gets the Hat Trick

Splunk named a Leader in SIEM across three analyst reports

Show Me >





Free Splunk

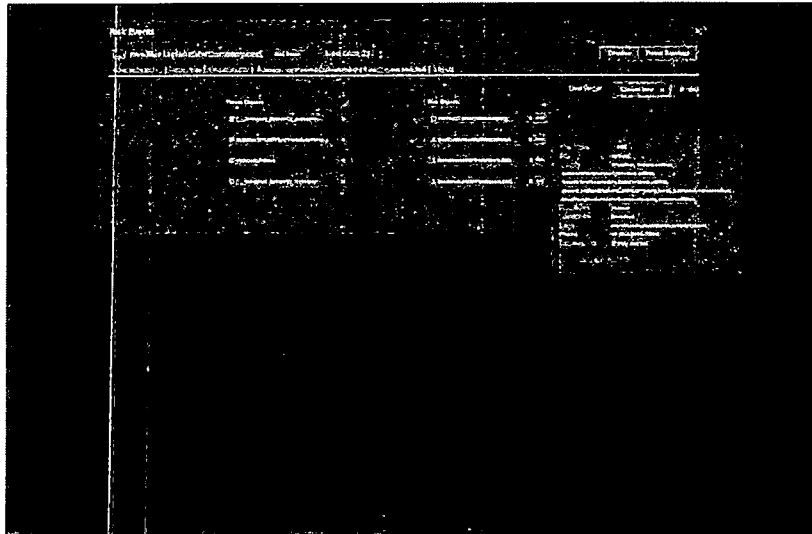


# Greater visibility and rapid detection

## Fast, ML-powered threat detection

Defend against threats with advanced security analytics, machine learning and threat intelligence that focus detection and provide high-fidelity alerts to shorten triage times and raise true positive rates.

[Risk-Based Alerting in Enterprise Security >](#)




## Full visibility across your environment

Break down data silos and gain actionable intelligence by ingesting

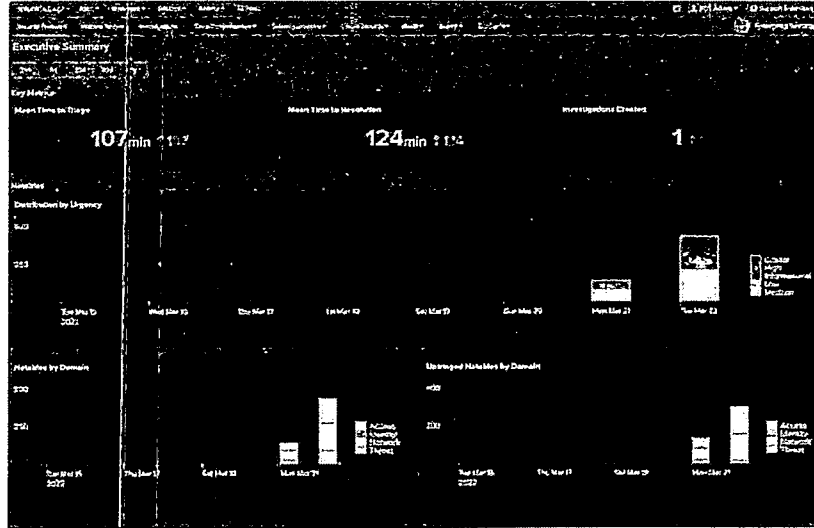
**Splunk Gets the Hat Trick**  
 Splunk named a Leader in SIEM across three analyst reports

[Show Me >](#)





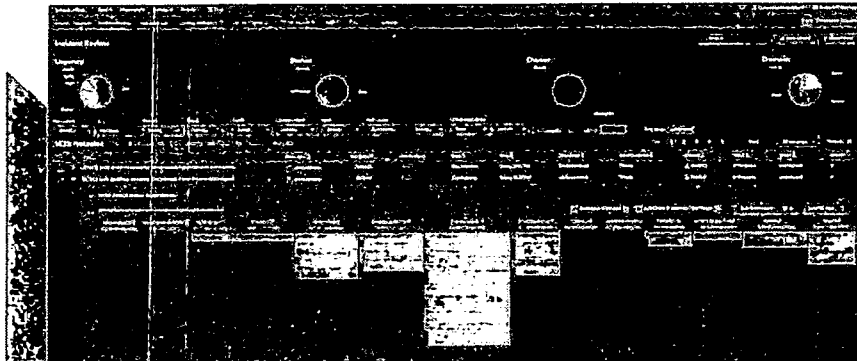
Free Splunk



## Efficient investigations

Gather all the context you need and initiate flexible investigations with security analytics at your fingertips. The built-in open and extensible data platform boosts productivity and drives down fatigue.

[See Common Enterprise Security Use Cases >](#)



**Splunk Gets the Hat Trick**  
Splunk named a Leader in SIEM across three analyst reports

[Show Me >](#)

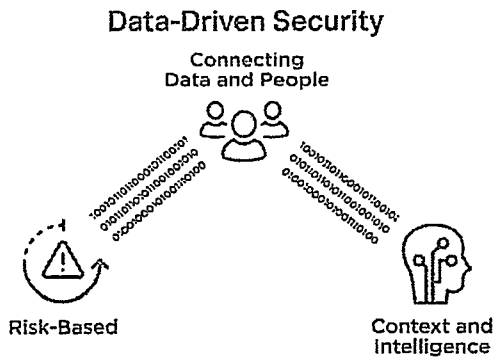




# Splunk Enterprise Security

Data-driven insights for full breadth visibility, detection and investigation

- Gain full visibility and improve security posture across your multi-cloud, hybrid, and on-premises environment
- Accelerate threat detection and investigation using risk-based alerting, integrated threat intelligence, and out-of-the-box security content
- Quickly gather context from your technology investments with a flexible data platform and integrations across multi-vendor tools and technologies



Your security team faces a dynamic threat landscape, emerging adversary tactics, and evolving business demands. But to meet these challenges, your team needs data-driven capabilities, contextual insights and accurate rapid threat detection techniques. These capabilities can help you reduce mean-time-to-detection and make informed decisions to strengthen business outcomes.

Splunk Enterprise Security (ES) is a data-centric, modern security information and event management (SIEM) solution that delivers data-driven insights for full-breadth visibility into your security posture so you can protect your business and mitigate risk at scale. With unparalleled search and reporting, advanced analytics, integrated intelligence, and pre-packaged security content, Splunk ES accelerates threat detection and investigation, letting you determine the scope of high-priority threats to your environment so you can quickly take action. Splunk ES is built on an open and scalable data platform that allows you to stay agile in the face of evolving threats and business needs.

Splunk ES helps security teams – of all sizes and levels of expertise – to streamline security operations. It provides:

- 1400+ out-of-the-box detections that align to industry frameworks such as MITRE ATT&CK, NIST, CIS 20, and Kill Chain
- Actionable intelligence with associated normalized risk scores and the necessary context from intelligence sources that are required in order to detect, prioritize, and investigate security events
- Real-time detections for suspicious and malicious behaviors using cloud-based streaming analytics
- 2700+ security and IT integrations built by Splunk, partners, and community members to make it easy to introduce your security tools and data sources into Splunk
- 80% reduction in alert volume to reduce alert fatigue, provide clarity and prioritization for analysts, and close cases in minutes instead of weeks
- Operationalize the MITRE ATT&CK Framework with a visualization matrix that highlights the tactics and techniques observed in risk events to save time when investigating events
- Quickly discover the scope of an incident and respond accurately with a comprehensive view of the malicious executables and threat actors observed on machines and users
- Support for every deployment type through cloud, multi-cloud, on-premises, and hybrid to match business needs and growth

