

FALCON DISCOVER FOR SECURITY OPERATIONS

Gain holistic, real-time visibility across all applications assets and accounts within your environment to maintain robust IT & security hygiene.

SEE WHO, WHAT, & WHERE ENTITIES ARE ACCESSED WITHIN YOUR ORGANIZATION

Falcon Discover, CrowdStrike's IT hygiene solution offers central visibility and entity inventory around applications, assets and accounts spread across your enterprise. Security operations teams use Falcon Discover to efficiently manage and maintain their organizations environments to ensure the health of their systems and to maintain a defensible security posture. Organizations should actively manage and implement security processes that allow them to efficiently see across a broad range of entities - and target those entities that reflect suspicious behavior or activity for managed and unmanaged assets.

Since Falcon Discover¹ sits within the Falcon platform, it is easy and efficient to cross reference suspicious data and to connect with broader SecOps for context around vulnerabilities and other incidents. Discover leverages the same lightweight agent architecture used for the Falcon platform.

KEY CAPABILITIES

GAIN CENTRAL VISIBILITY ACROSS APPLICATIONS, ASSETS, & ACCOUNTS

Falcon Discover offers central visibility into what and how assets are being used, monitoring accounts, and tracking application installations. This IT hygiene solution allows your team to quickly see and review via dashboards that target in on:

KEY BENEFITS

1. Track and monitor all relevant entities across your environment.
2. Maintain audit and compliance requirements with automated and exported reports.
3. Leverage the CrowdStrike platform for added context around suspicious activity and vulnerabilities.
4. Gain holistic visibility into managed and unmanaged entities - even those that are not managed by a Falcon sensor.
5. Create custom alerts to help your security team to focus on areas relevant to your organization.

¹ Falcon Discover requires CrowdStrike Falcon Insight™.

FALCON DISCOVER FOR SECURITY OPERATIONS

Assets:

- See assets within your environment that have been added or removed
- Use Falcon Discover to locate new assets to install the Falcon sensor
- Review drive encryption status
- Track resource usage for your organization's systems over time
- Manage and track all assets across different CIDS

Accounts:

- Monitor what accounts are being used
- Track to see if domain or local credentials are accessed
- Monitor password changes

Applications:

- Track installed applications
- See what assets are being used for applications and how they are being utilized

TRACK ENTITY INVENTORY ACROSS ENVIRONMENTS IN REAL TIME

A critical part of IT hygiene is establishing and maintaining security controls for all of your organization's entities within an environment. Falcon Discover offers greater convenience and visibility for security teams to track inventory across all major entity types, applications, asset and accounts - in real-time. With this real-time data, teams can maintain:

Up-to-date Inventory - track what hosts are using what applications, accounts and assets at any given time.

Unmanaged/Unauthorized applications - See what applications could be vulnerable to an attack, and which devices are running outdated or unauthorized software.

Unmanaged/Unsupported assets - See data about each asset type within hosts, and target which assets are not being monitored.

Track software usage - across your entire organization.

Consolidate on costs - by pinpointing on underutilized application licenses.

UTILIZE ROBUST DASHBOARDS AND REPORTING FOR FASTER RESPONSE

Security operations staff often have only a limited number of hours each week to monitor all the hundreds of thousands of entities that exist within an organization's environment. Even if your team only focuses on those entities that indicate a vulnerable opening, or potential abuse of an account - monitoring can quickly eat up all resources and time available. Since Falcon Discover offers data in real-time and a robust set of reporting capabilities, your staff can enjoy the immediate benefits of accurate reporting that is fully automated. Use Falcon Discover to:

- Create specialized permissioned roles for broader IT teams.
- Use dashboards for specific data targeting assets, applications and accounts in your organization.
- Create and save filters that include or exclude relevant information.
- Build and save dashboards for later access.
- Organize data to display table columns relevant to your monitoring needs.
- Sort data for export to highlight what's most important for stakeholders.
- Use the BIOS Prevalence dashboard to gain visibility into which hosts need investigation.

PREVENTATIVE SECURITY AND BEYOND

Security starts with discovering where you're not protected, so you can close the gaps and be better prepared to face threats. Falcon Discover provides the visibility and information that security and IT teams need to ensure comprehensive defense against today's sophisticated threats.

FALCON DISCOVER FOR SECURITY OPERATIONS

MAINTAIN COMPLIANCE OBLIGATIONS

Following audit and compliance requirements should not come at the expense of your security team's limited time. Falcon Discover allows your organization to easily meet requirements by extending reporting abilities to track and maintain compliance. Exporting reports for system resources, BIOS, operating system security, accounts, applications and drive encryption make it fast and simple to disclose all relevant information to governing bodies.

ABOUT CROWDSTRIKE

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

Powered by the CrowdStrike Security Cloud, 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 enables customers to benefit from 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/>

© 2022 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.