

Falcon for IT on GovCloud

Ask. Answer. Act.

Challenge: Public Sector IT teams are faced with incomplete visibility, manual processes and silos

IT and security teams are tasked with a growing number of priorities, from managing and securing exponential growth in the number of assets under their supervision to keeping up with a multitude of compliance requirements and enabling a hybrid workforce. To address these priorities, organizations have used a growing number of point products, leading to agent and hardware sprawl. Compounding the problem, barriers and silos between IT and security teams slow down workflows, hurt end-user experiences and create gaps in security for adversaries to exploit. With adversaries utilizing AI and automation more frequently to propagate attacks, the need is greater than ever to ensure IT and security teams are working closely together to eliminate security gaps and rapidly investigate and respond to threats.

Additionally, compliance and security stand out as paramount concerns. IT and security teams have struggled with manual data gathering processes, an incomplete picture of compliance and security posture, and disjointed workflows for addressing problems.

It's time for a new approach.

Solution: Ask. Answer. Act.

CrowdStrike Falcon® for IT, a module of the CrowdStrike Falcon® platform, enables IT and security teams to query their entire IT estate across endpoints, servers and cloud workloads, get quick and accurate answers, and take decisive action. It helps organizations streamline key use cases like fleet management, compliance, forensic investigations and performance monitoring with CrowdStrike's single, lightweight Falcon agent.

With Falcon for IT on GovCloud, public organizations can infuse powerful automation into their daily workflows to break down barriers between IT and security teams and gain unified visibility.

Key benefits

- Get complete visibility into endpoints, servers and cloud workloads with a robust query language for fleet management, compliance and performance monitoring.
- Instantly understand the state of any asset to resolve issues in real time, rationalize the IT estate and achieve superior ROI with a single lightweight agent.
- Unify IT and security workflows with powerful response actions — such as policy changes or updating software or machine state — with built-in automation to speed troubleshooting, compliance monitoring and forensic investigations.

Key capabilities

Ask any question.

- Query any asset running Windows, Linux and macOS by leveraging the flexible osquery language.
- Create custom queries or leverage 150+ out-of-the-box queries for on-demand and scheduled data collection to get complete visibility into every asset.
- Streamline the acquisition of compliance, performance and forensic data, including certificate validation, process resource usage and software update policy adherence.

The screenshot shows the CrowdStrike Falcon console interface. At the top, there's a tab labeled "Windows 11 Readin...". Below it, the title "Windows 11 Readiness - Upgrade Eligibility Status" is displayed. The target is set to "Windows (65)". A dropdown menu for "Platform" is set to "Windows". The query is displayed in a code editor:

```
Query: SELECT r.data, CASE WHEN r.data LIKE 'Red' THEN 'Ineligible for Windows 11 Upgrade' WHEN r.data LIKE 'Orange' THEN 'Incompatible Software Installed - Reduced Functionality Likely Upon Upgrade' WHEN r.da...
1 SELECT r.data,
2 CASE
3   WHEN r.data LIKE 'Red' THEN 'Ineligible for Windows 11 Upgrade'
4   WHEN r.data LIKE 'Orange' THEN 'Incompatible Software Installed - Reduced Functionality Likely Upon Upgrade'
5   WHEN r.data LIKE 'Yellow' THEN 'Incompatible Software Installed - Application Must Be Uninstalled To Proceed'
6   WHEN r.data LIKE 'Green' THEN 'Eligible for Windows 11 Upgrade'
7   ELSE 'Unknown Status'
8 END AS upgrade_eligibility,
9 CASE
10  WHEN win11.data LIKE '%Windows 11%' THEN 'Windows 11 Installed'
11  ELSE win11.data
12 END AS installation_status
```

Get the answers you need — fast.

- Instantly understand the current state of all assets — identify unauthorized software, outdated machines, patch status and irregular resource usage — to standardize and secure your enterprise.
- Execute compliance checks and forensic analysis using real-time query results powered by the single lightweight Falcon sensor for scalable, performant data collection.
- Correlate insights within CrowdStrike Falcon® Next-Gen SIEM for comprehensive IT and security visibility.

The screenshot shows the CrowdStrike Falcon console interface. At the top, there's a tab labeled "Hosts with expired...". Below it, the title "Hosts with expired certificates" is displayed. The target is set to "Windows (808), Mac (6), Linux (317)". The query is displayed in a code editor:

```
Query: SELECT * FROM certificates WHERE not_valid_after < CURRENT_TIMESTAMP;
```

Below the query, the status is shown as "Completed 100%". A progress bar indicates the status of the query results: Completed (912), Offline (211), Failed (8), and Expired (0).

The results are displayed in a table with columns: Hostname, common_name, subject, issuer, ca, self_signed, and Actions. The table shows three rows of results:

Hostname	common_name	subject	issuer	ca	self_signed	Actions
GLARE-...	Thawte Time...	ZA, Western ...	ZA, Western ...	-1	1	⋮
GLARE-...	DigiCert SHA...	US, DigiCert L...	US, DigiCert L...	-1	0	⋮
SULK-F...	DigiCert EV C...	US, DigiCert L...	US, DigiCert L...	-1	0	⋮

At the bottom, it shows "3,854 results (1-20 shown)" and "Items per page 20".

Take action.

- Rapidly fix issues by taking actions at scale with built-in Falcon for IT Quick Actions. Deploy emergency patches, change policies, update software or machine state, move or remove files, run an executable, change registry keys and more directly on endpoints, servers and cloud workloads.
- Optimize your IT estate and save time with scheduled tasks to automatically detect and remediate anomalies, unauthorized changes and compliance deviations.
- Integrate Falcon for IT asset context across the Falcon platform and with third-party tools like ServiceNow and Jira to automate and complete remediation loops, maximizing efficiency and automation in IT and security operations.

Initiate RTR quick action

Targeted hosts: 1

Select action:

- Move file or directory
- Put executable on host and run it
- Remove file or directory
- Remove software packages
- Run a custom script**
- Run executable
- Update software packages
- Windows registry: Delete keys or values
- Windows registry: Set keys or values

Run a custom script

This action executes a custom script that is already defined in cloud storage.

- Modifies or deletes data on host
- Potential impact: host user's computing session

Enter details

Windows

Script name
patch-kb5044293.ps1
The script name in cloud storage to be executed

Timeout (optional)
3600
Timeout in seconds

Command line (optional)

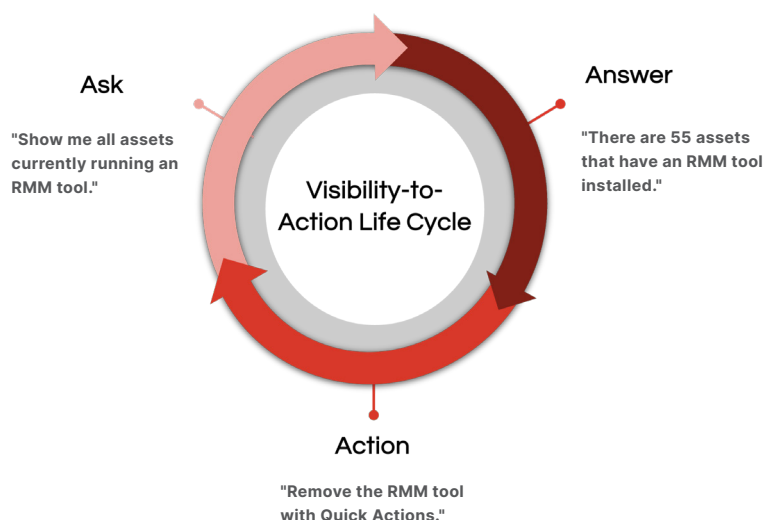
Command line arguments

Mac

Cancel ☐ Offline queueing **Initiate action**

Supercharge IT and security workflows with Falcon for IT

Falcon for IT helps IT and security teams achieve their desired outcomes throughout the “visibility-to-action” life cycle, from ask, to answer, to action. Ask any question on demand with more than 150 out-of-the-box queries for common questions. Analysts can also create custom complex queries with a robust SQL query language. Detailed, accurate query results are collected in real time alongside historical data populated through dashboard visualizations. Falcon for IT empowers IT and security teams to gain instant visibility into their enterprise, take swift action and validate changes in real time all within the CrowdStrike Falcon platform, without requiring additional infrastructure or impacting performance.



CrowdStrike Compliance and Certification

CrowdStrike strongly supports the mission of civilian government, the military and the intelligence community. The CrowdStrike Falcon platform is hosted on AWS GovCloud and is Federal Risk and Authorization Management Program (FedRAMP)-authorized, providing government agencies the complete protection and visibility they need to mitigate risk and eliminate threats on federal, state and local levels.

Start free trial →

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/>

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

