

Falcon for IT

Ask. Answer. Act.

Challenge: 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 compliance 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 close 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 AI-native 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, organizations can infuse AI and automation into their daily workflows to help break down barriers between IT and security teams.

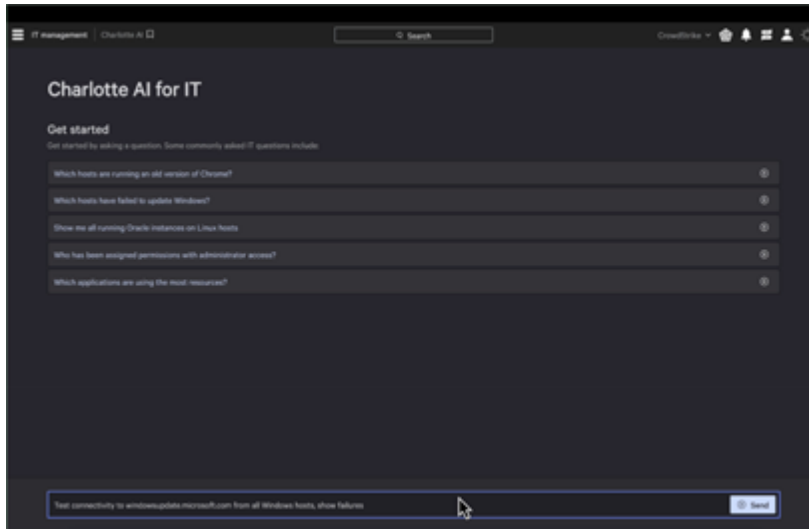
Key benefits

- Get complete visibility into endpoints, servers and cloud workloads with natural language search and a robust query language for fleet management, compliance and performance monitoring.
- Instantly understand the state of any asset to resolve issues faster and rationalize the IT estate.
- Break down barriers between IT and security with powerful response actions — such as policy changes or updating software or machine state — with built-in automation to speed troubleshooting, compliance and forensic investigations.

Key capabilities

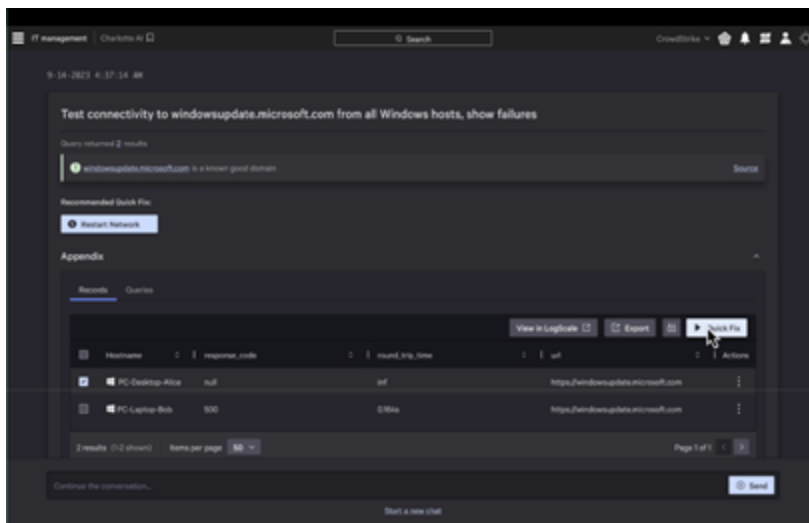
Ask any question.

- Use natural language, generative AI prompts, an easy-to-use query language with 150+ out-of-the-box queries, and scheduled queries to get complete visibility into every asset.
- Streamline the acquisition of compliance, performance and forensic data, including certificate validation, process resource usage and update policy adherence.
- Query any asset running Windows, Linux and macOS by leveraging the flexible osquery language.



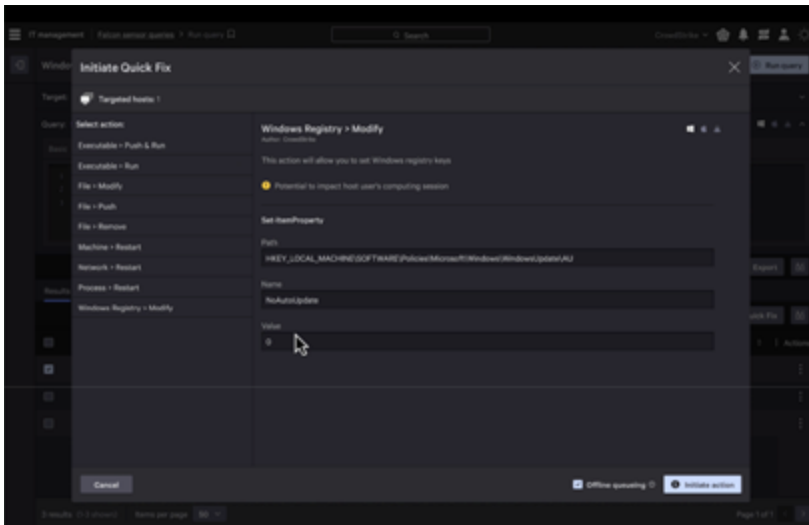
Get the answers you need – fast.

- Instantly understand the current state of all enterprise assets — such as unauthorized software, outdated machines, patch status and irregular resource usage — to rationalize the IT estate.
- Execute forensic analysis using real-time query results and Falcon sensor data, mapped through asset connections and correlated within CrowdStrike Falcon® Next-Gen SIEM for clear IT and security insights.
- Swiftly enact registry modifications or file management tasks, streamlining issue resolution for IT administrators and enhancing system and application performance.



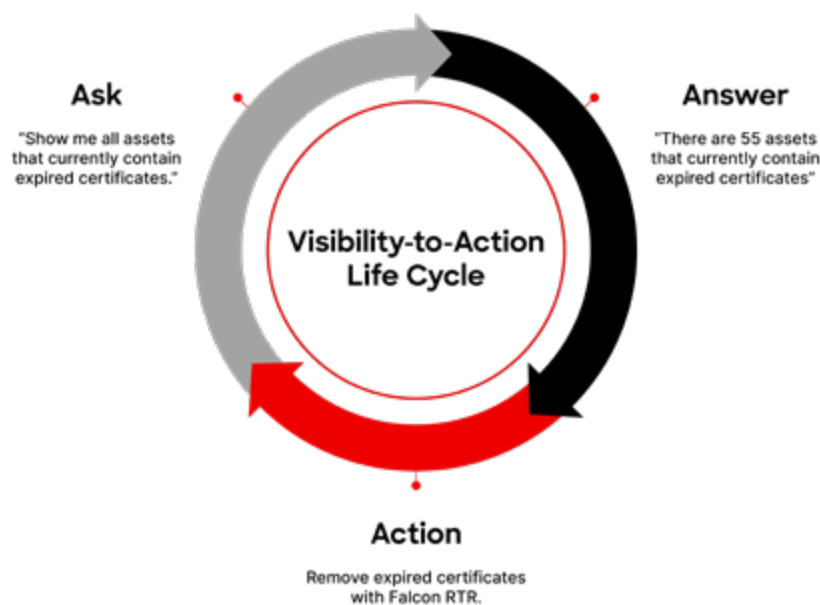
Take action.

- Optimize your IT estate with scheduled queries to automatically detect anomalies, unauthorized changes and compliance deviations.
- Rapidly fix issues by taking actions with Falcon Real Time Response (RTR) like changing policies, updating software or machine state, moving/removing files, running an executable, changing registry keys and more, directly on endpoints, servers and cloud workloads with an out-of-the-box Quick Fix library.
- Integrate Falcon for IT osquery commands 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.



Supercharge IT and security workflows with Falcon for IT

Falcon for IT helps IT teams achieve their desired outcomes throughout the “visibility-to-action” life cycle, from ask, to answer, to action. Organizations can ask any question on demand using generative AI prompts, a robust query language and 150+ out-of-the-box queries for common questions. Detailed, accurate query results are ready in near real time for IT teams to consume and get ready to act on. Finally, IT and security teams can take immediate action on any asset with any operating system.



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/>

