

Falcon for IT

Intelligent endpoint automation
converging security and IT operations

Challenges

Security and IT teams operate across increasingly distributed environments, where endpoints must remain secure, compliant, and operationally resilient at all times. Devices are initially configured to meet organizational standards, but configurations drift as software changes, updates are delayed, and settings are modified. At the same time, teams must rapidly identify and remediate vulnerabilities before adversaries can exploit them, while continuously validating compliance and operational readiness across the fleet.

These operational demands are made more difficult by the traditional divide between security and IT tooling. Disconnected point products create blind spots, manual workflows, and operational friction, making it difficult to maintain consistent visibility and enforce standards at scale.

Without a unified approach, organizations face three persistent challenges:

- Incomplete visibility caused by fragmented IT and security tools
- Slow, manual workflows that span multiple products
- Increased operational risk driven by inconsistent compliance verification and vulnerability remediation

These challenges are driving organizations to consolidate security platforms and modernize endpoint operations. CrowdStrike Falcon® for IT enables organizations to move from fragmented visibility and manual processes to unified, policy-driven endpoint operations at scale.

Key benefits

Operational Impact: Move from fragmented tools to unified, policy-driven endpoint operations.

- Accelerate issue resolution with real-time, enterprise-wide querying
- Continuously validate compliance and configuration posture
- Reduce manual effort with automated, policy-driven remediation
- Lower operational risk with centralized governance and auditability
- Consolidate security and IT workflows on a single platform

Solution overview

Falcon for IT extends the CrowdStrike Falcon® platform to unify endpoint security and IT operations within a single, integrated experience. Built on the lightweight Falcon sensor already deployed across the environment, Falcon for IT enables organizations to operationalize endpoint management directly within the Falcon platform — eliminating the need for disconnected tools and additional sensors.

Falcon for IT enables real-time endpoint operations, transforming comprehensive visibility into policy-driven, automated workflows at scale. Teams can interrogate any endpoint, continuously validate posture, and execute corrective actions from the same console used to secure the enterprise. By converging visibility and response in one platform, organizations eliminate tool sprawl, reduce manual effort, improve cross-team collaboration, and lower both security exposure and operational risk.

Key capabilities

Real-Time Querying at Scale

Run ad hoc and scheduled queries across the entire Windows, macOS, and Linux fleet in seconds, without deploying additional sensors or collectors. CrowdStrike Charlotte AI™ lowers the barrier for analysts and IT operators by enabling natural language search, helping teams quickly interrogate endpoints and retrieve operational, compliance, and forensic data in real time.

Unified Dashboards and Reporting

Continuously validate configuration standards and operational posture across distributed environments using prebuilt and customizable dashboards. Generate audit-ready compliance reports without manual data collection. Operational metrics are aligned with security context, helping teams understand endpoint posture alongside broader risk signals.

Unified Security and IT Telemetry

Unify security and IT telemetry within CrowdStrike Falcon® Next-Gen SIEM, with rich endpoint telemetry ingested as native first-party data at no additional cost. This real-time operational context strengthens event correlation, enriches compliance reporting, and accelerates investigations by eliminating reliance on external data sources. By bringing detailed endpoint state directly into the Falcon data model, teams gain deeper visibility and improve analyst efficiency.

Automated Actions and Policy-Driven Remediation

Execute actions at scale across endpoints, servers, and cloud workloads with role-based access controls to ensure authorized change management. Policy-driven remediation enforces configuration standards and security requirements continuously, and all actions are centrally logged and auditable, providing transparency and accountability across teams.

Accelerate time-to-value with prebuilt content packs

Falcon for IT includes prebuilt content packs: operational blueprints that combine curated queries, dashboards, and automated remediation workflows to accelerate operational outcomes across security and IT teams. Developed and continuously refined by CrowdStrike experts, these content packs operationalize the most impactful security and IT functions across modern enterprises.

Content packs go beyond faster execution. They standardize common processes, reduce scripting errors, and create scalable, repeatable operations that teams can confidently execute across distributed environments. By embedding governance and automation into everyday workflows, Falcon for IT helps organizations strengthen security posture while improving operational consistency.

Content packs enable teams to operationalize high-impact workflows, including:

- Application health monitoring and automated repair
- Continuous compliance verification and drift remediation
- Detection and removal of unauthorized or high-risk software
- Endpoint performance monitoring and issue resolution
- File indexing and deep artifact visibility
- Visibility into software bill of materials and software supply chain

By packaging data collection, reporting, and remediation into reusable workflows, Falcon for IT reduces manual effort, improves consistency, and scales policy-driven operations across the enterprise.

Key outcomes

Security Investigations

Conduct real-time, enterprise-wide endpoint queries to support threat hunting, forensic validation, and operational troubleshooting. Interrogate system state across distributed environments without deploying additional tools, accelerating root cause analysis and informed decision-making.

Compliance and Reporting

Continuously collect and validate endpoint data to demonstrate compliance, maintain accurate asset inventories, and reduce audit preparation time. Deliver audit-ready reports and clear visibility into configuration posture across the enterprise.

Security Risk Reduction

Remediate misconfigurations and out-of-compliance settings through policy-driven corrective actions that reduce exploitable exposure. When integrated with CrowdStrike Falcon® Exposure Management, AI-powered, adversary-informed exposure prioritization guides these workflows, enabling teams to act on the highest-risk vulnerabilities and exposures at scale.

Operational Risk Reduction

Execute policy-driven queries and remediation actions at scale with granular role-based access controls, centralized policy management, and full audit logging. Intelligent guardrails — including scoped targeting, distribution over time, and performance thresholds — ensure changes are executed safely across distributed environments. By embedding governance into every action, Falcon for IT reduces operational risk while maintaining control and minimizing business disruption.

Supercharge security and IT operations

Falcon for IT enables organizations to replace fragmented endpoint management tools with a unified, AI-native platform that delivers intelligent automation across security and IT operations.

With a single lightweight sensor, native platform integration, and policy-driven automation, organizations can modernize endpoint operations while reducing complexity, cost, and enterprise risk.

Learn how Falcon for IT can help your organization scale intelligent endpoint automation and reduce enterprise risk.

[Request a Demo](#)[Learn More](#)

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/>

