

Falcon for IT: Application Resiliency Without Complexity

Empowering SecOps teams with unified,
intelligent security automation and
operational control

As cyberattacks grow more sophisticated and persistent, maintaining operational continuity is just as critical as preventing breaches. Application resiliency — the ability of applications to recover quickly from failures and maintain secure functionality in all situations — has emerged as a top priority for modern security operations teams. Yet many environments are riddled with agent gaps, misconfigurations, and blind spots that compromise resilience.

Security teams can take practical steps to harden application infrastructure, proactively detect issues, and remediate them swiftly using CrowdStrike Falcon® for IT. With capabilities purpose-built for operational integrity and scalable remediation actions, Falcon for IT empowers SecOps to ensure always-on protection for any applications and agents deemed critical by the organization — making it easier for security teams to ensure those assets remain healthy and continuously operational, without adding operational complexity.

**Secure your environment and ensure continuous protection —
[request a demo of Falcon for IT.](#)**

The New Reality: Application Resiliency Is a Security Imperative

Today's adversaries exploit the weakest links in your IT ecosystem. Misconfigured, outdated, or failed agents create gaps in visibility and protection, giving attackers room to move undetected. Applications that quietly degrade or crash can leave security teams flying blind just when they need clarity most.

Application resiliency is no longer just about uptime — it's about security. When agents fail or critical applications go dark, response times slow and dwell times lengthen. In regulated industries, downtime also risks compliance violations and reputational harm.

Key benefits

- **Auto-detection and deployment** for missing agents
- **Centralized update management** to eliminate outdated agents
- **Configuration enforcement** to standardize and optimize agent settings
- **Real-time failure detection and automated restart** of stopped or failed agents
- **Live dashboards and historical trends** to track the health of critical apps

Security teams must play an active role in ensuring resiliency across applications and infrastructure. They need real-time insight, automated action, and integrated workflows to close the gap between protection and performance.

The 5 Essentials of a Resilient Application Stack

To build a resilient application environment, security teams should focus on five foundational pillars:

Agent Presence

- *Why it matters:* Unprotected endpoints are more vulnerable to attacks.
- *Action:* Continuously detect missing agents and automate installation.

Agent Hygiene

- *Why it matters:* Outdated agents may lack critical operational or security capabilities.
- *Action:* Identify outdated agents and push updates centrally.

Agent Configuration

- *Why it matters:* Misconfigurations cause inconsistent enforcement and degraded protection.
- *Action:* Normalize agent settings and enforce policy compliance.

Agent Continuity

- *Why it matters:* Stopped or failed agents represent gaps for attackers to exploit.
- *Action:* Detect stopped agents in real time and trigger automatic restarts.

Application Health Visibility

- *Why it matters:* If critical applications degrade or crash, business continuity is compromised.
- *Action:* Monitor application health, detect trends, and resolve issues proactively.

Traditional IT tools often fall short, with delayed insights, manual fixes, and fragmented data that slow resolution. Depending on separate IT teams and disjointed toolsets can delay issue detection and remediation. Friction across disconnected workflows adds complexity and risk, ultimately threatening the secure, stable, and efficient operation of the enterprise.

Falcon for IT: Resiliency Without the Complexity, All in a Unified Cybersecurity Platform

CrowdStrike Falcon for IT delivers security-first operational control by giving SecOps teams the tools they need to proactively maintain application and agent health — all from the same platform that powers industry-leading endpoint protection.

Point solutions may offer pieces of the puzzle, but they add cost, complexity, and overhead. They require new agents, consoles, and integrations — and still leave gaps.

Falcon for IT is part of the AI-native **CrowdStrike Falcon® cybersecurity platform**, which provides a unified data fabric, single-agent architecture, and shared visibility across security and operations teams. This convergence enables:

- **Faster time to insight** through correlated data
- **More effective response** through shared context
- **Lower total cost of ownership** through consolidated tooling
- **Rapid time-to-value** by leveraging your existing Falcon sensor, with no new agent required, and seamlessly integrating into your existing Falcon console — delivering instant visibility and remediation capabilities without retooling

With Falcon for IT, security teams don't just detect threats — they ensure the infrastructure is ready to resist them.

Application resiliency is no longer optional — it's foundational. Security operations teams must ensure agents and applications are healthy, functional, and secure at all times.

Falcon for IT delivers intelligent endpoint automation to do just that — on the same platform you trust to stop breaches.

Take the next step: [Request a demo of Falcon for IT](#) and experience application resilience in action.

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/>

