

Falcon Prevent

Protect every endpoint where users, AI agents, and adversaries operate

Stop today's AI-accelerated adversaries

As adversaries evolve and AI applications transform enterprise workflows, the endpoint has become the critical epicenter where human users, autonomous AI agents, and attackers collide. Legacy antivirus cannot defend against fileless attacks, poisoned open-source supply chains, or the abuse of legitimate tools. CrowdStrike® Falcon Prevent™ delivers complete, next-generation antivirus (NGAV) protection across Windows, macOS, and Linux endpoints without complex management or performance drag.

Powered by world-class AI and behavioral analytics, Falcon Prevent stops ransomware, fileless attacks, and zero-day exploits across endpoints. Beyond traditional AV replacement, it tackles modern threat vectors head-on, blocking poisoned open-source packages (including npm and PyPI packages) before malicious code runs and providing targeted application abuse prevention to stop adversary exploitation of dual-use tools like remote monitoring and management (RMM) software.

CrowdStrike is named a Leader in the 2026 Gartner® Magic Quadrant™ for Endpoint Protection for the seventh consecutive time, positioned furthest right for Completeness of Vision and highest for Ability to Execute. Independent testing by AV-Comparatives and SE Labs certifies Falcon Prevent as a full legacy AV replacement, validated for PCI, HIPAA, NIST, and FFIEC compliance.¹

Key benefits

- Stops known and unknown threats including ransomware, fileless, and zero-day attacks
- Protects endpoints online and offline
- Blocks malicious npm and PyPI packages before code runs
- Helps reduce abuse of trusted and dual-use applications
- Deploys quickly with one lightweight sensor
- Replaces legacy antivirus without added infrastructure
- Protection can be extended with CrowdStrike Falcon® Insight XDR using the same lightweight sensor

¹ <https://trust.crowdstrike.com/>

Key capabilities

Stop modern attacks before they take hold

Falcon Prevent combines multiple prevention layers with CrowdStrike Falcon® Adversary Intelligence to stop malicious activity at the point of execution, whether endpoints are connected or offline.

- Leverage on-sensor machine learning and critical threat intelligence to stop known and unknown threats, with protection that continues when the endpoint is offline.
- Block ransomware, fileless attacks, malicious scripts, and exploit activity using behavioral indicators of attack (IOAs), script control, high-performance memory scanning, and exploit mitigation.
- Tailor protection with flexible policies, instantly quarantine malicious files, and prevent attempts to tamper with or disable the Falcon sensor.

Reduce risk from trusted tools and software supply chains

Modern attacks increasingly exploit the tools, applications, and software ecosystems organizations already trust. Falcon Prevent helps stop threats before they can execute.

- Help prevent abuse of legitimate and dual-use applications, including high-risk RMM tools that adversaries commonly exploit.
- Stop threats delivered through poisoned open-source npm or PyPI packages before malicious code can run.
- Reduce exposure for both developer and non-developer endpoints across Windows, macOS, and Linux through the unified Falcon sensor.

Replace legacy antivirus without added complexity

Falcon Prevent delivers modern prevention through a single lightweight sensor, helping organizations move beyond legacy AV without adding infrastructure or operational overhead.

- Deploy rapidly across Windows, macOS, and Linux endpoints, as well as mobile devices with CrowdStrike Falcon® for Mobile and select legacy systems.
- Protect devices online and offline without constant signature updates or on-premises management infrastructure.
- Seamlessly extend protection with Falcon Insight XDR to augment real-time prevention with continuous threat detection and response, without deploying additional sensors.

[Start a Free Trial](#)

Falcon Prevent: Modern endpoint protection made easy

- Industry-leading protection
- Fast and easy deployment
- Optimal performance
- Reduced complexity

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/>

