

Falcon for macOS

Next-generation endpoint protection for Mac endpoints against malware and beyond

Powerful, easy and integrated Mac security

CrowdStrike Falcon® endpoint protection for macOS unifies the technologies required to successfully stop breaches. 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.

Key product capabilities

Unmatched next-gen endpoint protection technologies

- **Protects against various types of attacks:** CrowdStrike Falcon for macOS protects your organization against commodity and zero-day malware, ransomware, exploits and advanced malware-free, fileless attacks — keeping you ahead of the rapidly changing tactics, techniques and procedures (TTPs) used by today's adversaries, even when systems are offline.
- **Combines the best prevention technologies:** For ultimate protection, Falcon combines technologies such as machine learning for malware protection on- and off-sensor, indicator of attack (IOA) behavioral blocking, custom IOA blocking, Mac script control, detecting and quarantining on write, allowlisting, and detections based on threat intelligence reputation.
- **Unifies protection with a single lightweight-agent architecture:** Falcon uniquely integrates powerful best-in-class prevention, detection and response across the most critical areas of enterprise risk to provide continuous breach prevention in a single agent.

Unrivalled visibility for accelerated threat detection and response

- **Offers intelligent endpoint detection and response (EDR) capabilities:** Falcon for macOS detects advanced threats and malicious activities automatically, using IOAs to instantly identify attacker behavior and send prioritized alerts to the Falcon UI, eliminating time-consuming research and manual searches.
- **Enables continuous monitoring and visibility:** It provides full details and raw events to enable proactive and managed threat hunting and forensic investigations. It stores event data and answers queries in five seconds or less, even across billions of events.

Key benefits

Protect your Mac environment against known and unknown malware, fileless attacks, adware and potentially unwanted programs (PUPs)

Gain unparalleled real-time and historical visibility on Mac events and activities

Eliminate ransomware

Proactively hunt for threats

Automatically integrate with threat intelligence to maximize defenses and proactively respond to threats

Ensure seamless integration with your existing investments

Falcon for macOS

- **Allows you to respond and remediate with confidence:** Powerful response actions allow you to contain and investigate compromised systems, including on-the-fly remote access to take immediate action.
- **Provides valuable context and information:** Using integrated threat intelligence, Falcon for macOS delivers the complete context of an attack, including attribution.

Immediate time-to-value

- **Saves time, effort and money:** Falcon for macOS is part of the cloud-native Falcon platform and does not require any on-premises management infrastructure.
- **Delivers unmatched scalability:** CrowdStrike's design enables the industry's fastest deployment and instant operationalization — without requiring a reboot after installation.
- **Has zero impact on the endpoint:** Only CrowdStrike provides full, automated protection across endpoints without impacting endpoint performance and end-user productivity.

Unmatched macOS capabilities

- **CrowdStrike Falcon® Device Control:** Empowers analysts with intuitive and granular control to defend against external USB devices.
- **CrowdStrike Falcon® Firewall Management:** Reduces complexity and simplifies management to enable effective protection against network threats.
- **CrowdStrike Falcon® Intelligence:** Accelerates analyst investigation with specialized macOS intelligence beyond what happened, revealing the "who, why and how" behind an attack.
- **CrowdStrike Falcon® Zero Trust Assessment:** Enhances visibility of the overall endpoint health through a single metric with recommendations to improve security posture.
- **CrowdStrike Falcon® Forensics:** Efficiently collects and analyzes forensic data for cybersecurity incidents and periodic compromise assessments.
- **Falcon Discover:** Enables effective IT hygiene with detailed visibility of applications, assets and user accounts.

Protects your Macs against all threat types

Falcon provides protection against both malware and malware-free threats, and known and unknown threats, whether they originate from outside or inside your organization. It uses a revolutionary approach designed from the ground up to match both the human and technical challenges of existing and future threats.

No signature updates required

Falcon for macOS uses machine learning to prevent both known and unknown malware, providing the highest level of protection without requiring daily and cumbersome updates.

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.**

Follow us: [Blog](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

© 2023 CrowdStrike, Inc.
All rights reserved.

