

# 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 including next-generation antivirus, endpoint detection and response (EDR), IT hygiene, 24/7 threat hunting and threat intelligence. They are integrated and delivered via a single lightweight agent to provide continuous breach prevention across all of your Mac endpoints.

## 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, indicator of attack (IOA) behavioral blocking, custom IOA blocking, allowlisting and detections based on threat intelligence reputation.
- **Uses a single, lightweight agent:** Falcon uniquely integrates powerful best-in-class prevention, detection and response with IT hygiene capabilities to provide continuous breach prevention in a single agent.

## 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

### UNRIVALED VISIBILITY FOR ACCELERATED THREAT DETECTION AND RESPONSE

- **Offers intelligent 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.
- **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.

- **Deploys in minutes:** CrowdStrike customers can deploy the cloud-delivered Falcon agent across up to 70,000 endpoints in less than a single day.
- **Is immediately operational:** With unmatched detection and visibility from Day One, Falcon for macOS hits the ground running, monitoring and recording on installation without requiring reboots, fine-tuning, baselining or complex configuration.
- **Has zero impact on the endpoint:** With only a lightweight agent on the endpoint, searches take place in the CrowdStrike Threat Graph™ database without any performance impact on endpoints or the network.

### BROAD SUPPORT: KEXT TO SYSTEM EXTENSIONS

- **Supports kext and system extensions:** Falcon for macOS supports kernel extensions and system extensions, offering the same levels of visibility, detection and protection.
- **Covers all macOS versions:** A single Falcon agent covers all supported macOS versions including Big Sur, with system extensions and backward compatibility with Mojave and Catalina, where Falcon will use the older kext approach as necessary.
- **Automatically reconfigures:** For upgrades to newer macOS versions, the Falcon agent automatically reconfigures itself to use the Apple system extension method for Big Sur and above.

### PROTECTS YOUR MACS AGAINST ALL THREAT TYPES

Falcon provides protection against both malware and malware-free, 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® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 4 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.