CROWDSTRIKE

FALCON PREVENT NEXT-GENERATION ANTIVIRUS

Ideal AV replacement combines the most effective prevention technologies with full attack visibility and simplicity

INDUSTRY-RECOGNIZED LEGACY AV REPLACEMENT

For organizations struggling with the ineffectiveness and complexity of legacy antivirus solutions, CrowdStrike Falcon® Prevent is here to help. Falcon Prevent delivers superior protection with a single lightweight-agent architecture that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. Falcon Prevent enables customers to deploy tens of thousands of agents at once — with no reboots necessary to install or change security settings.

<u>Certified to replace legacy antivirus products</u> — Independent testing at AV-Comparatives and SE Labs has certified Falcon Prevent's antivirus capabilities. Falcon Prevent has also been validated for PCI, HIPAA, NIST and FFIEC regulatory requirements.

Positioned as a Leader in 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for Third Consecutive Time — In addition to being positioned in the Leaders quadrant, CrowdStrike is positioned furthest to the right for Completeness of Vision.

KEY BENEFITS

Prevents all types of attacks

Simplifies operations with signatureless protection and software-as-a-service (SaaS) delivery

Deploys in minutes and immediately begins protecting your endpoints

Replaces legacy antivirus quickly and confidently

Operates seamlessly alongside antivirus as you migrate to simplify transition

Provides full attack visibility

KEY CAPABILITIES

STATE-OF-THE-ART PREVENTION

Falcon Prevent protects endpoints against all types of attacks, from commodity malware to sophisticated attacks — even when offline.

- Machine learning and artificial intelligence prevent known and unknown malware, adware and potentially unwanted programs (PUPs)
- AI-powered indicators of attack (IOAs), script control and high-performance memory scanning identify malicious behaviors and prevent fileless attacks and ransomware
- Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities
- Detect and quarantine on write stops and isolates malicious files when they first appear on a host
- Industry-leading threat intelligence is built into the CrowdStrike Security Cloud to actively block malicious activity
- Custom IOAs enable you to define unique behaviors to block
- Quarantine captures blocked files and allows access for investigation
- Script-based execution monitoring inspects and blocks malicious Microsoft Office macros
- Sensor tampering protection stops user or process attempts to manipulate or disable the CrowdStrike Falcon® sensor

INTEGRATED THREAT INTELLIGENCE

- Automatically determine the scope and impact of threats found in your environment
- Find out if you are targeted, who is targeting you and how to prepare and get ahead
- Use Falcon Prevent integrated with CrowdStrike Falcon Intelligence to:
  - Fully understand the threats in your environment and what to do about them
  - Access malware research and analysis at your fingertips
  - Easily prioritize responses with threat severity assessment
  - Immediately get recovery steps and resolve incidents with in-depth threat analysis

FULL ATTACK VISIBILITY AT A GLANCE

For unparalleled alert context and visibility, Falcon Prevent:

- Provides details, context and history for every alert
- Unravels an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data
- Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections
- Keeps detection details for 90 days

SIMPLE, FAST AND LIGHTWEIGHT

Purpose-built in the cloud with a single lightweight-agent architecture, Falcon eliminates complexity and simplifies endpoint security operations.

- Falcon operates without constant signature updates, complex integrations or on-premises equipment
- The lightweight agent bears little impact on endpoints, from initial install to day-to-day use — no reboot is required after installation
- Minimal CPU overhead restores system performance and end-user productivity
- Falcon enables the industry's fastest deployment and instant operationalization — without requiring a reboot after installation
- It is automatically kept up to date with cloud-native architecture and SaaS delivery
- Falcon provides broad platform support across an organization's entire estate of endpoints
- Automated IOA remediation streamlines the removal of artifacts that may lead to reinfection

GARTNER is a registered trademark and service mark of Gartner and Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Learn more at **www.crowdstrike.com**

FALCON PREVENT: THE EASIEST AV REPLACEMENT

Better 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/

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today:
https://www.crowdstrike.com/free-trial-guide/