CrowdStrike Products

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 that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. Even the largest organizations can be up and running in minutes with Falcon Prevent.

Certified to replace legacy antivirus products — 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.

Named a leader in the 2019 Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) — In addition to being positioned in the Leaders Quadrant, CrowdStrike is furthest for “completeness of vision,” which includes Gartner criteria such as innovation, marketing and product strategies, vertical industry and geographic strategies, as well as the validity of the business model as a whole.

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)
- Behavior-based indicators of attack (IOAs) prevent sophisticated attacks, including ransomware and fileless and malware-free attacks
- Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities
- Threat intelligence prevention blocks activities known to be malicious
- 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 X™ 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

The cloud-native CrowdStrike Falcon platform and lightweight Falcon agent eliminate complexity and simplify 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
- It works on Day One, deploys in minutes and is immediately operational
- It is automatically kept up to date with cloud-native architecture and SaaS delivery
- Falcon provides broad platform support including Windows, Windows Server, macOS and Linux
- Automated IOA remediation streamlines the removal of artifacts that may lead to reinfection

FALCON PREVENT: THE EASIEST AV REPLACEMENT

Better protection

Fast and easy deployment

Optimal performance

Reduced complexity

ABOUT CROWDSTRIKE

CrowdStrike, 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 5 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.

Start Free Trial
of Next-Gen AV

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

DISCLAIMER: 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. 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.