CROWDSTRIKE

CrowdStrike Products
Data Sheet

# Falcon Prevent

## Ideal antivirus (AV) replacement combines effective next-gen 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.

**Falcon Prevent is certified to replace legacy antivirus products —** independent testing by 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.

CrowdStrike is **positioned as a Leader in the 2023 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for the Fourth Consecutive Time —** in addition to being positioned in the Leaders quadrant, CrowdStrike is positioned furthest to the right for Completeness of Vision.

### 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

### 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 existing antivirus as you migrate to simplify transiition
- Provides full attack visibility

- 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 Falcon® platform 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® Adversary 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 effective 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

## Falcon Prevent: The Easiest AV Replacement

- Better protection
- Fast and easy deployment
- Optimal performance
- Reduced complexity

## Simple, fast and lightweight

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

- Falcon Prevent operates without constant signature updates, complex integrations or on-premises equipment
- Falcon Prevent 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
- The lightweight Falcon agent deploys in minutes for instant protection, with no complex configuration needed
- Minimal CPU overhead restores system performance and end-user productivity

**Start Free Trial**

**Operating system coverage:** For more information about supported operating system versions, please click here.



# 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/