DELL Technologies

Dell SafeGuard and Response

CrowdStrike Falcon® Prevent™ Next-Generation Antivirus (NGAV)

KEY BENEFITS

- Helps prevent 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

AV combines prevention technologies with attack visibility and simplicity

For organizations struggling with the ineffectiveness and complexity of legacy antivirus solutions, CrowdStrike® Falcon Prevent™ delivers 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.

Falcon Prevent has also been validated for PCI, HIPAA, NIST and FFIEC regulatory requirements.

CROWDSTRIKE

Learn more at www.Dell.com/endpoint-security

DELL Technologies

Key product capabilities

Prevention

Falcon Prevent protects endpoints against 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, eliminating complexity and simplifying 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.
- 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.

Contact your dedicated Dell Endpoint Security Specialist today at endpointsecurity@dell.com, for more information about the Dell solutions to help improve your security posture

Learn more at www.Dell.com/endpoint-security

CROWDSTRIKE