

FALCON PREVENT FOR HOME USE

Fast, easy protection for home-based employees

NEXT-GENERATION ANTIVIRUS PROTECTS HOME WORKERS' PERSONAL COMPUTERS

When employees work from home, they may access corporate data and applications from their own personal computer systems. This introduces new risks, as these systems may not have the up-to-date endpoint protection that is needed to keep their home systems secure from cyber threats.

CrowdStrike® Falcon Prevent™ for Home Use allows organizations to provide employees with a simple option for securing their personal devices, so those who must use a home system to access corporate resources can do so safely and productively.

Under the Falcon Prevent for Home Use program, company administrators provide a specially packaged version of the CrowdStrike Falcon® lightweight agent to their employees to install on their home Windows systems.

The agent installs quickly, requires zero configuration by the end user and provides proven next-generation antivirus protection without impacting system performance. The management of remote users is performed via the cloud-native Falcon platform console, and remote users are maintained separately from corporate users for ease of management.

KEY BENEFITS

Ensures easy, cloud-native security for remote workers using personal computers: The CrowdStrike lightweight agent installs in seconds without requiring a reboot, and the cloud-native architecture scales without friction, providing an ideal solution for remote workers.

Provides unified management for corporate-owned and employee-owned devices: Falcon Prevent for Home Use is managed and maintained through the Falcon console, providing a single solution that meets the unique needs of your workforce.

Delivers proven protection: The CrowdStrike Falcon platform is certified by multiple independent third parties to provide the protection needed by enterprises of all types and sizes, with very low performance impact.

FALCON PREVENT FOR HOME USE

KEY CAPABILITIES

STATE-OF-THE-ART PREVENTION

- **Machine learning and artificial intelligence** detect known and unknown malware and ransomware
- **Behavior-based indicators** of attack (IOAs) prevent sophisticated 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

SIMPLE, FAST AND LIGHTWEIGHT

- **The lightweight Falcon agent** has little impact on endpoints — from initial installation to day-to-day use
- **Minimal CPU overhead** ensures high system performance and end-user productivity
- **Falcon for Home Use works alongside existing antivirus solutions** the user may already have installed

EASY TO DEPLOY AND MANAGE

- **Zero-configuration installation:** The lightweight Falcon agent can be quickly installed by the user, requires no interaction and does not require a reboot
- **Automatic updates** ensure that users always have the best protection, without cumbersome manual intervention
- **Central management** via the cloud-native Falcon console requires no on-premises infrastructure or new processes

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 3 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.

Learn more at www.crowdstrike.com

© 2020 CrowdStrike, Inc. All rights reserved.

