CROWDSTRIKE

FALCON FIREWALL MANAGEMENT

Simple, centralized firewall management makes it easy to manage and enforce host firewall policies

FIREWALL MANAGEMENT MADE EASY

As more organizations look to adopt host firewall capabilities native to the operating system, they often find effective functionality but are faced with complex, cumbersome management and visibility blind spots that can frustrate administrators and open security gaps.

CrowdStrike® Falcon Firewall Management™ eliminates the complexity associated with native firewalls by making it easy to manage and enforce policies using a simple, centralized approach. An easy-to-understand activity view provides instant visibility allowing you to monitor and troubleshoot critical rules to enhance protection and inform action.

Delivered via the CrowdStrike Falcon® lightweight agent, single management console and cloud-delivered architecture, Falcon Firewall Management immediately enhances protection from network threats with minimal impact on the host — from initial enablement to ongoing day-to-day use.

KEY BENEFITS

Simplifies management of host firewalls native to the operating system

Enhances protection

Delivers instant visibility

Reduces complexity

Speeds troubleshooting

KEY PRODUCT CAPABILITIES

SIMPLE FIREWALL MANAGEMENT

- Easily create, enforce and maintain firewall rules and policies
  - Build new policies based on templates — start with an empty policy, your template or a CrowdStrike template
  - Create a firewall rules group once and reuse it in multiple policies
  - Easily view and rearrange rules to achieve the desired order
  - Quickly propagate changes to the appropriate policies
  - Validate rules to prevent administrators from creating faulty rules
  - Seamlessly add new systems to host groups with desired policy
- Test the entire policy in monitor mode before you deploy to understand what would have been blocked or allowed

REDUCED COMPLEXITY

- Simplifies operations by using the same lightweight Falcon agent, management console and cloud-native architecture
- Deploys and is operational in minutes without requiring reboots, fine-tuning or complex configuration
- Has no additional impact on hosts, from initial installation to ongoing day-to-day use
- Streamlines workflows and increases visibility across endpoint security controls due to the single management console for both endpoint protection and host firewall management

BETTER PROTECTION

- Automatically identify and view specific activities, potential threats and network anomalies
  - At-a-glance activity page provides instant visibility, allowing you to:
    - Monitor and troubleshoot critical rules
    - View matched rules
    - Directly modify firewall policies from the activity page
- Application and location-aware firewall policies enhance security and provide granular control

LOGGING, TROUBLESHOOTING AND COMPLIANCE

- Speed troubleshooting with granular control and visibility
  - Easily enable or disable a specific rule, an entire rules group or a policy
  - Monitor select or newly added rules
- Incorporate network events into investigations
- Audit all firewall rules and policy changes
  - See what changed, who did it and when it happened
- Use role-based access control to ensure that only the appropriate administrators view and manage firewall rules

ELIMINATE THE BURDEN OF MANAGING HOST FIREWALLS

Is operational within minutes via the lightweight Falcon agent

Enables you to create, enforce and maintain firewall rules and policies with ease

Accelerates policy enforcement and expands visibility via a single console

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 2.5 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.