DELL Technologies

Dell SafeGuard and Response

VMware Carbon Black Cloud Host-Based Firewall

Key Capabilities

- Simplified policy management
  - Single console for endpoint security policy management
  - Consolidated visibility into the protection policies applied to devices
  - Increase efficiency of endpoint security operations
- Rules-based enforcement
  - Block, allow or alert on the network behavior of applications
  - Group rules into policies that are tied to other prevention policies
- Enhanced security for remote devices
  - Maintain visibility and control over devices outside of the corporate firewall
  - Streamline security for remote workers' devices

Key Features and Benefits

- Reduce the resources required to run and maintain host-based firewall
- Manage firewall rules in groups using existing prevention policy workflows
- Streamline operations by leveraging a single platform for multiple security use cases

Enhance network visibility and control for endpoints and workloads

Security analysts require visibility into and control over endpoint network traffic to ensure they have the ability to detect and respond to attacks before they spread to other devices in the network. With remote work increasing due to the COVID-19 pandemic, security teams have an increased need for visibility and control over employees' network activity when they're working outside of the corporate network.

VMware Carbon Black Cloud Host-based Firewall enables security teams to further consolidate their security stack by integrating firewall management capabilities directly into their endpoint and workload protection platform[1]. By including Host-based Firewall capabilities in the Carbon Black Cloud platform, SOCs can leverage a single platform for more use cases, increasing their overall efficiency and reducing the resources needed to run their SOC[2].

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

vmware Carbon Black

DELL Technologies

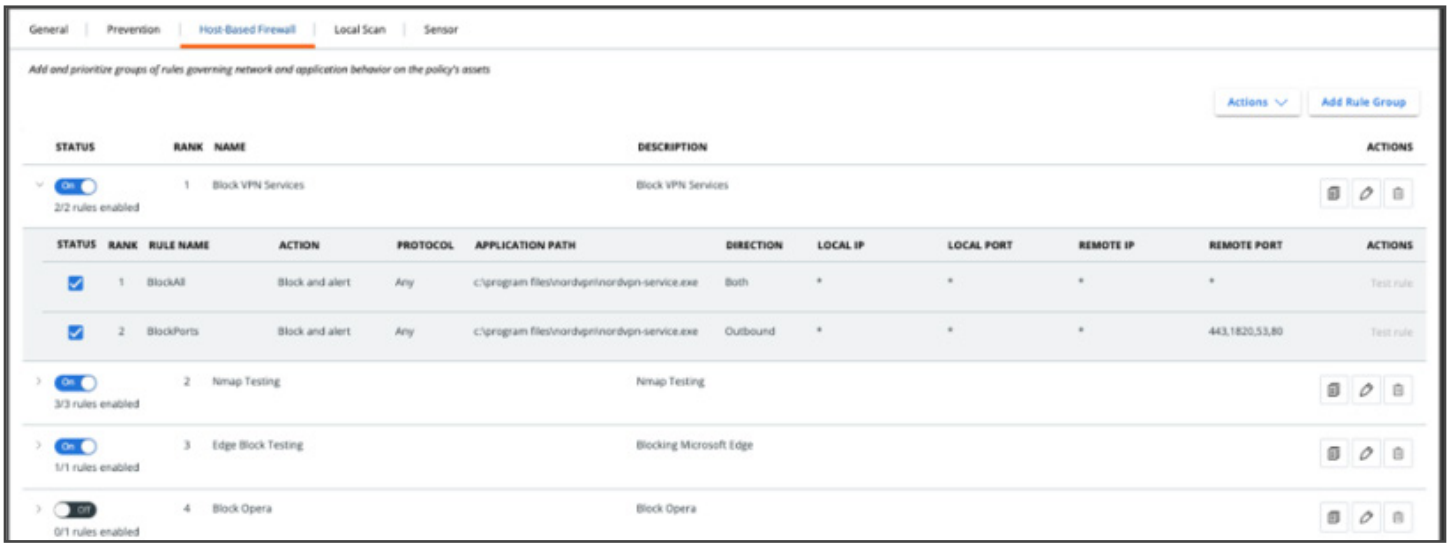

Figure 1: Firewall rules can be grouped and managed within the Carbon Black Cloud policy settings interface.

Reduce the noise with integrated prevention policies and firewall rules

By providing Host-based firewall policy management capabilities within the Carbon Black Cloud console, security teams can simplify their policy management and ensure protection policies aren't causing unnecessary noise or false positives. With grouped rules, devices can be placed into policies based on several factors and have automated response actions enabled for certain behaviors or devices.

Automate response actions to network application behavior

Create policies and rules with response actions attached to ensure malicious behavior is blocked or alerted on for security teams to review. This bi-directional capability allows analysts to spend more time focusing on hunting for threats in their environment and less time tuning prevention policies to manage their alerts.

[1] *Not available as a stand-alone offer. Host Based Firewall requires a minimum of VMware Carbon Black Standard for purchase, so it is available alongside any endpoint bundle (Standard, Advanced, Enterprise) or Workload Advanced or Enterprise.*

[2] *Available for Windows only currently.*

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

vmware Carbon Black