INTEGRATION BRIEF

FireMon + VMware

Ground-to-Cloud Unified Multi-Vendor Security Policy Management

A certain amount of complexity is expected within any security infrastructure. However, even in the best managed environments, it slowly accumulates over time jeopardizing security and reliability. This holds true even with industry leading technologies such as VMware NSX when they need to operate within a multi-vendor hybrid environment. To ensure security and compliance while remaining agile, NSX customers need to comprehensively manage all network policies no matter where they exist to tame the complexity that can lead to costly errors and unplanned outages.

Challenges of Managing Policies Across Hybrid Cloud Environments

As networks become more complex and policy rulesets continue to multiply, it becomes increasingly more difficult to manage compliance, implement rule changes, prevent outages, and address vulnerabilities before they're exploited. Without an integrated way to manage policies across multi-vendor, highly-distributed environments, organizations struggle with time consuming and error prone manual compliance reporting, extended response times to business owners, and lack a clear view of risk across their entire environment.

The FireMon-VMware partnership enables companies to simplify and automate policy management across public cloud, private cloud, and on-premises environments to:

- Increase agility, security, and compliance posture with centralized policy management for the entire network, including VMware NSX security groups, micro-segmentation policies, and virtual 3rd-party firewalls deployed alongside the NSX framework
- Find existing policies that impact security, compliance, and business continuity
- Ensure continuous compliance with real-time violation detection
- Create, test, and deploy consistent policy changes across the entire environment

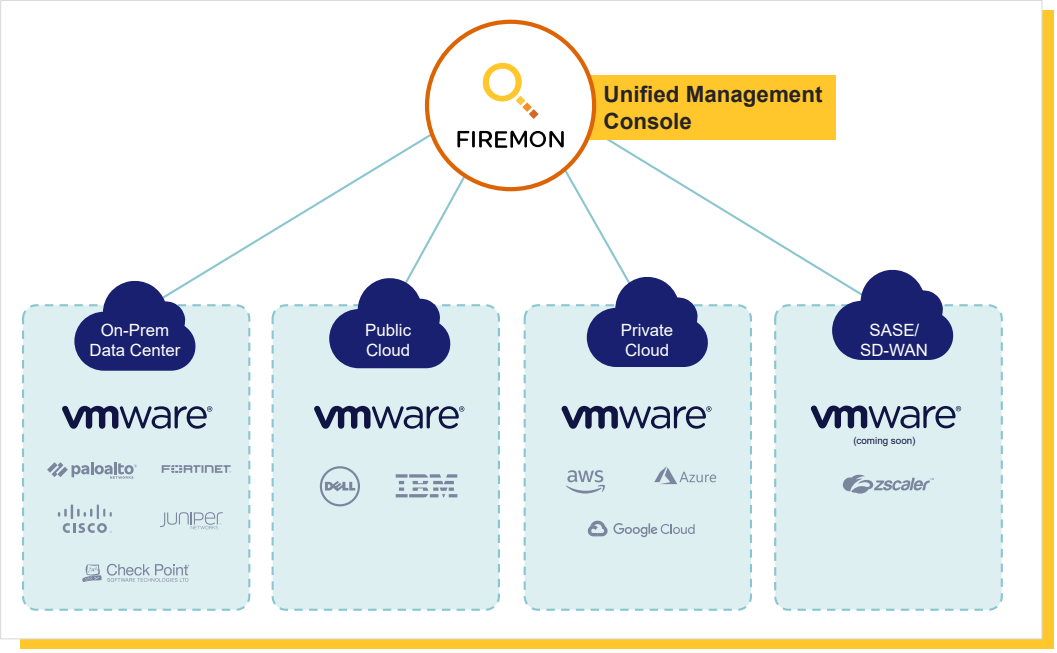
FireMon and VMware: How the Integration Works

VMware NSX powers digital transformation using a software-defined approach to networking that extends across data centers, clouds and application frameworks. VMware NSX-V and NSX-T enable the creation of segmented zones and protection rules that can apply to virtual machines (VMs) or groups of VMs via the NSX distributed firewall or supported 3rd-party virtual firewalls. NSX enhances agility with security and optimization services at the VM level, and automation in supporting application developer and DevOps workflows.

FireMon customers with NSX deployed in their environment get a single management console to manage polices across every firewall and security device on the network, no matter its location or who manufactured it. A simplified normalized source of truth and policy normalization simplifies reporting and reduces policy changes from weeks to minutes.

Figure 1. FireMon-VMware Integration

The integration of FireMon with VMware NSX allows FireMon to collect and aggregate VMware NSX policy information from each NSX security group into the FireMon platform. Once there, customers can visualize their VMware NSX virtual network devices as part of an overall network map in relation to their hybrid network security topology.



Security Policy Management Use Cases

Compliance Highly-customizable reports deliver a one-click overview of compliance throughout the entire environment tailored to precise business needs. Automatic scans identify and remove rules that violate internal and external compliance standards including PCI-DSS, HIPAA, and GDPR. Real-time detection identifies and notifies administrators of existing policy violations and scans for any new violations before changes are deployed.

Change Automation FireMon's centralized rule repository captures and standardizes policies across all vendors to simplify rule management and plan for changes. Rules can be created, tested, and deployed directly to any or all devices on the network using built-in workflows or integration with ITSM providers such as ServiceNow and Remedy. Real-time change detection alerts administrators when a policy is created, updated or removed, so nothing is missed.

Risk Management Custom business policy and best practice reviews identify and mitigate risks before they are exploited. Third-party scanner integrations and risk analysis modeling check for known vulnerabilities and test for policy weaknesses. Automatic guardrails review changes for policy violations before they're deployed.

FIREMON

FireMon is the only agile network security policy platform for firewalls and cloud security groups providing the fastest way to streamline network security policy management, which is one of the biggest impediments to IT and enterprise agility. Since creating the first-ever network security policy management solution, FireMon has delivered command and control over complex network security infrastructures for more than 1,700 customers located in nearly 70 countries around the world. For more information, visit www.firemon.com

vmware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact.

SB0025-EN-20210927-01