

# Security Manager + VMware NSX

## Increasing security, productivity and agility of virtualized networks with intelligent security management

**THE CHALLENGE:** Your network is more intelligent. Shouldn't the way you manage it be, too?

For years, organizations have invested in hiring more staff and acquiring new defense technology in order to protect against security threats. And yet, network data breaches are at an all-time high. Virtualized environments and microsegmentation are becoming more popular as organizations take advantage of cloud technologies. The adoption of this technology, however, adds to the complexity of our security infrastructures and processes, which increases the level of difficulty for device management.

### THE SOLUTION: Intelligent Security Management from FireMon

FireMon's Intelligent Security Management platform enables users with NSX Networks devices to work smarter, applying intelligence to the entire security program – from planning configurations and monitoring effectiveness to making secure access changes and assessing them for compliance. We provide organizations with the tools necessary to see through the complexity and become more proactive and agile with their security.

#### SINGLE-PANE, CONTINUOUS MONITORING

We take a top-down approach to security management, providing you with a holistic, enterprise-level view of the firewalls you have under management.

- **A Robust Rule Display** provides a rule-specific dashboard as well as compliance, documentation, change and usage information within the rule list page. This extra information gives you the ability to see the full security posture of each rule at a quick glance.
- **Real-Time Configuration Monitoring** ensures easy tracking, reporting and compliance of NSX virtual firewall, router and switch policy changes. **Configuration Monitoring** is supported from the ESXi/NSX management system.
- **Policy Search/Query** helps you find any device, rule, user, application or object across the enterprise using natural-language search, filters or our Security Intelligence Query Language (SIQL).

## NEXT-GEN POLICY ANALYSIS

Next-generation firewalls have an additional layer of data that can be useful when analyzing configurations for effectiveness. FireMon provides a number of analysis tools that read data down to the application, object user level to help optimize your firewall policies.

- **Traffic Flow Analysis** allows you to see exactly which object applications are using a rule or flowing in or out of a zone as well as view Network Access Translation analysis results. This is especially important for firewall migration policy integrity.
- **Access Usage Analysis** tracks usage over a long period of time, including users and applications, to help you identify and remove unnecessary access.
- **Granular Change Report** identifies who is making changes in real time.

## COMPLIANCE ASSESSMENTS & DOCUMENTATION

FireMon gives you the capability to perform automated, continuous and real-time assessments of the entire network security infrastructure according to customer-defined requirements or industry regulations and best practices.

- **Real-time Compliance Monitoring** tracks firewall compliance with user-defined standards or regulatory requirements, such as PCI DSS, every time a change occurs.
- All firewall changes are **automatically documented** for easy reference when preparing for compliance audits.

# Who is FireMon?

FireMon is the No.1 provider of Intelligent Security Management solutions worldwide, combining advanced benchmarking, simulation, and analysis to deliver next generation security intelligence. Since creating the first-ever network security management solution more than 15 years ago, FireMon solutions have continued to deliver visibility into and control over complex network security infrastructure, policies, and risk to over 1,500 customers around the world.

Using the FireMon Intelligent Security Management platform, today's leading enterprise organizations, government agencies, and managed security providers have dramatically improved effectiveness of network defenses, accelerating business agility and optimizing return on investment.

## FIREMON CUSTOMERS USE INTELLIGENT SECURITY MANAGEMENT TO:

- Manage multi-vendor environments
- Clean up and audit firewall policies
- Assess & report on policy compliance
- Intelligently automate policy changes
- Migrate or upgrade firewalls
- Manage vulnerability & risk
- Triage security alerts
- Proactively search for threats