Opinnate NSPM

Product Details

1. Definition/Description/Product introduction

Opinnate NSPM is a powerful, user-friendly policy management solution designed to seamlessly integrate with leading firewall vendors. It simplifies the processes of analysis, rule optimization, and automation, enabling organizations to enhance their firewall security with ease and efficiency.

2. Features

Rule Analysis (Shadow, Unused, Permissive, ...)
AD-Aware Shadow Analysis
Rule Checking (network access existence control)
Topology Creation
Rules Export
Risk Acceptance for Risky/Permissive/Conflicting Rules
Passive monitoring for Rule/Object Usage Analysis (Based on last 30-day syslog data to eliminate permissive rules quicker)
Passive monitoring for Custom Usage Analysis (Last 30-day syslog data)
Compliance-based/Custom Reporting
Configuration Change Tracking (filter supported)
Email Alerts
Disabling Shadowed Rules Automatically
Disabling Expired Rules Automatically
Disabling Unused Rules Automatically
Cleaning Disabled Rules Automatically
Singularizing Duplicated Objects Automatically
Decommissioning of Rules for Removed Systems Automatically
Adding New IP-based Rule Automatically
Adding New User-based Rule Automatically
Adding New App-based Rule Automatically
Server Cloning (same or different subnet) Automatically
Adding New Custom Rules Automatically (Using firewall objects)
Updating Existing Rules Automatically
Adding New Rule above/below of a Rule

Copying Rules to Other Firewalls
Rule Reordering
TAG Assignment to Rules
Updating Existing Addresses/Address-Groups Automatically
Adding New Address/Address-Group Automatically
Rule Lifecycle Management (scheduled rules or yearly controls)

3. Highlights compared to competitors

Ease of use/install/integrate
Passive monitoring for rule/object usage and custom usage analysis
No requirement for firewall manager (Fortimanager, Panorama)
Less Disk, CPU, Memory Consumption
Licensing advantages (Cluster firewalls count as 1, standard edition for optimization)
Risk Acceptance
Server Cloning (different subnets)
Rule Lifecycle Management (scheduled rules)
AD-aware Shadow Rule Analysis

4. Customer Benefits/Gains/Advantages/Facilities/etc. (Why the customer needs this product?)

As to Gartner 99% of all firewall breaches are due to firewall misconfigurations. Eliminating this configuration problems is crucial
Almost all regulations, such as PCI and ISO27011, mandate rule analysis actions for firewalls. Opinnate not only facilitates this process but also provides detailed compliance-based reports, simplifying the firewall audit process.
Firewall management is the most labor-intensive activity among all cybersecurity tasks. With automation workflows, routine firewall activities can be fully automated.

5. Which law, standard, regulatory or compliance requirement does it meet? (if any)

NIST, ISO27001, PCI-DSS, HIPAA, SOX, GDPR, SWIFT, NERC CIP, GLBA, SOC2, FISMA, DTO, BRSA

6. Licensing model (All details such as what licensing is based on, what information should be requested from the customer)

Subscripton based depends on the editiom and the number of firewalls.

7. References (Public, Private Sector, Bank, Energy, SMB, etc)

40+ customers including QNB Finans, ING, BKM, Ziraat Katılım, Odeabank, Hepsiburada, Dogus Teknology, Isnet, A&T Bank., ..

8. Potential Customer Profile

All customers having at least one firewall cluster and especially in Finance, Retail, Energy, e-commerce sectors

9. How Does It Work?

Containerized application working on two virtual servers. API integration with firewalls, service desk systems.

10. Deployment Methods and Supported Vendors

On-premises

Check Point, Cisco, Fortinet, Palo Alto, Sophos, Vmware NSX

11. External integrations (SIEM, SOAR, etc.)

SIEM, SOAR, Service Desk integrations possible

12. PoC Process & Requirements

Two virtual servers, ovf files to be given.

Server specs base: 8core/32GB/500GB

13. Common problems and troubleshooting steps (if applicable)

Firewall integration related problems: mostly due to wrong user password or no network access to firewalls.

14. Details of after-sales support and service processes

These are the step by step tasks to be completed for the full utilization of system:

- ✓ The integration of firewalls
- ✓ Collector integration
- ✓ Exchange/AD integrations
- ✓ Environmental settings to be made
- ✓ Corporate security policy creation
- ✓ E-mail alert creation
- ✓ SIEM integration

- ✓ LDAP integration – for user-based rules
- ✓ Service-desk integration – if prefered
- ✓ SOAR integration – if prefered