FortiSIEM TALKING POINTS

Overview

- 3rd Generation (Next-Gen) SIEM platform
- Cross correlated NOC & SOC Analytics
- Pre-built compliance reports, out-of-the-box, for PCI-DSS, HIPAA, FERPA, SOX, ISO27001, COBIT, GPG13, ITIL, Sans Critical Controls
- Self learning, real-time network infrastructure and device discovery
- Single pane of glass, web based GUI for monitoring and managing Security, Performance and Compliance requirements.
- Role-based access controls
- Large enterprise, MSP and MSSP ready with Multi-Tenant architecture.
- Highly scalable, virtualized architecture able to collect, parse, normalize, index and store hundreds of thousands of events per second (EPS)
- API's supporting simple integration with external technology solutions
- Able to be deployed at the Customer site, Data Center and Cloud
- Greatly enhances visibility into the security fabric

Key Customer Challenges

- Rapid detection and remediation of real and potential threats to Network Performance, Security and Compliance standards.
- Lack of skilled personnel and integrated systems to support current and future threat landscapes.
- Managing the requirements associated with regulatory compliance standards.
- Unknown risks from the Internet of Things (IoT)
- Agility and ability to securely exploit new technology in support of organizational strategies
- Keeping pace with changes in the regulatory environment.
- Protecting the organization's brand, reputation and customer relationships.
- NOC and SOC have disparate and dis-integrated tools and methodologies in managing threats

FortiSIEM Features

- Virtual Appliance supports rapid deployment and ease of scale.
- Pre-built reports for PCI-DSS, HIPAA, FERPA, SOX, ISO27001, COBIT, GPG13, ITIL, Sans Critical Controls
- Self-learning, and real-time infrastructure and device discovery
- System and Application performance Analytics
- Detection of unauthorized devices, applications and configuration changes
- Distributed real-time event correlation
- Performance Monitoring – Systems, Applications, Virtualization, Storage, Active Directory, MS Exchange, Databases, VoIP, Flow
- Cloud ready - supports: Vmware, ESX, Microsoft HyperV, Xen, Amazon Web Services (AWS), AMI, OpenStack, MS Azure
- Large scale threat feed integration
- Rich, customizable dashboards
- Simple and flexible administration
- Integration with IT ticketing tools – ServiceNow, ConnectWise, and Remedy

Target Opportunities:

- Any organization that must comply with regulatory standards related to protecting network assets
- Organizations seeking tools for faster detection and remediation of threats and breaches.
- **Verticals**: MSP's, MSSP's, Retail, Financial services, Healthcare, Higher Educational institutions, Governmental agencies

Target Decision Makers:

- CSO, CISO, CIO
- Network Security Managers, Directors, Vice Presidents

FortiSIEM TALKING POINTS

Qualification Questions

- How are you protecting your network from breaches today, and how is that working?
- How are you planning to manage against the threats expected from the proliferation of IoT devices?
- Does your organization need to conform with regulatory compliance standards?
- Does your organization need a simpler way to manage security and compliance?
- Has your organization experienced a network breach, yet?
- What is your number 1 concern related to network security, performance or compliance?

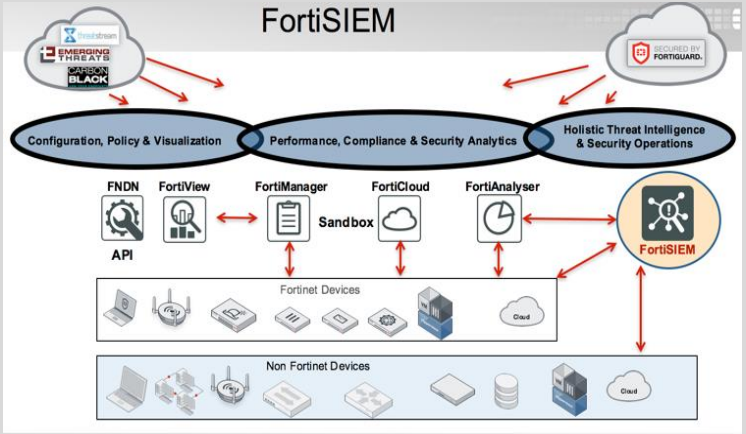
Key Resources

- FortiSIEM Data Sheet
- FortiSIEM ESG Lab report
- FortiSIEM Supported Devices
- FortiSIEM FAQ

FortiSIEM Kill Points

- **Scalable:** FortiSIEM's unique virtualized architecture was purpose built to insure ease of scalability with patented event processing able to collect, parse, normalize, index and store hundreds of thousands of events per second exceeding today's needs, with a foundation to support Future needs from IoT to the cloud.
- **Secure:** FortiSIEM patented analytics enables organizations to more rapidly detect and respond to the threats to their security, performance and compliance.
- **Aware:** Built-in automated infrastructure discovery insures awareness of the devices, systems, hardware, software, running services, applications, storage, users, network configuration, network topology and device relationships are always current.
- **Actionable:** Pre-built and customizable reports for security and compliance along with patented analytics enable organizations to quickly identify root causes of threats for rapid remediation.
- **Open:** FortiSIEM includes support for hundreds of devices, common applications and third party threat feed data, with API's to easily enable others.

Enhancing the Security Fabric



FortiSIEM Architecture