FURTINET

SOLUTION BRIEF

Fortinet Cloud-Based Security Management

Executive Summary

As enterprise networks evolve to meet digital transformation initiatives, they rapidly adopt public cloud computing. This creates an expanded attack surface that necessitates both elevated security and management and analytics. Many organizations retain legacy security management and analytics tools, even though they are ineffective alongside newer security solutions in the cloud. To enable effective cloud-based security management and analytics, these tools must have the same dynamic characteristics as the cloud they are deployed in.

Comprised of three security products—FortiManager, FortiAnalyzer, and FortiSIEM—Fortinet Security Management and Analytics can be deployed in the cloud, whether private or public, enabling organizations to take advantage of the scale, flexibility, and agility of the cloud. This comprehensive solution delivers actionable visibility and centralized controls across the entire network—cloud, on-premises, branch offices, and endpoints.

Top Features:

- Enterprise-grade management
- Advanced compliance reporting
- Risk scoring and assessment
- Automation readiness
- Flexibility, agility, scalability, and lower TCO

Cloud Computing Complicates Security Management

While cloud adoption offers many advantages, including optimized total cost of ownership (TCO), scalability, agility, and fast deployment, it also adds complexity to security management.

In fact, moving to the cloud has caused a security management burden for the majority of companies. Over half (55%) report using more management tools since migrating to the cloud, sometimes needing multiple tools for the same task. In addition, over half (53%) report spending more time on management tasks than ever before.[1] Whether trying to breathe life into legacy management tools, or adding new disparate tools, nonintegrated management tools will cause more grief to already overburdened security teams.

VM-Based Management and Analytics

Together, FortiManager VM, FortiAnalyzer VM, and FortiSIEM VM provide organizations with a cloud-based platform that simplifies management and analytics with transparent visibility and centralized control of both cloud and on-premises assets with one integrated solution.

This combination offers an integrated management and analytics toolset for the network operations center (NOC) and security operations center (SOC), which enables enhanced security operations visibility. Fortinet Security Management and Analytics offers single-pane-of-glass management, best practices compliance, and comprehensive analytics. And while the aforementioned Fortinet VM-based solutions run in the cloud, they also combine to encompass the entire network—from the cloud, to on-premises data centers, to branch offices, to endpoints.

Management and Analytics Use Cases

Following are the three top use cases for Fortinet cloud-based Security Management and Analytics:

Centralized security management and visibility helps consolidate and simplify the management of disaggregated point security products that often reside in their own management silos. This obfuscates visibility across public cloud, private cloud, and on-premises deployments. Operational complexity and security risks are reduced by simplifying and automating device deployment and network monitoring.

Compliance and audit tracking and reporting simplifies regulatory compliance and adherence to security standards. With comprehensive, automated reporting and hundreds of prebuilt compliance reports, the once complicated and burdensome task of regulatory and security compliance can be accomplished quickly and easily.

Rapid response helps enterprises increase operational efficiencies and reduce security risk. With technologies that can see and share threat intelligence in real time, risks can be found and mitigated immediately. Further, by implementing a network-aware SOC, organizations can stay ahead of advanced threats far more easily.

Understanding the Solution Components

Each of the three elements of Fortinet Security Management and Analytics is available for deployment in private and public clouds. Native integration in all the top public cloud platforms, including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, and Oracle Cloud, allows organizations to leverage the inherent scalability and globalization of public cloud infrastructure.

Integration across security disciplines, not merely products, enables a greater level of visibility, control, and operational management. Fortinet Security Management and Analytics combines the capabilities of FortiManager VM, FortiAnalyzer VM, and FortiSIEM VM to coalesce the operational context of the NOC with the security insights of the SOC. NOC context includes appliance status, network performance, and application availability, while SOC insights include breach identification, stopping data exfiltration, and uncovering compromised hosts.

FortiManager VM runs and manages Fortinet next-generation firewalls (NGFWs) on most hypervisors (for private clouds) and software-defined network (SDN) platforms. It provides single-pane-of-glass management for unified, end-to-end protection across the extended enterprise. It also delivers insight into network traffic and offers enterprise-class features for threat containment.

FortiAnalyzer VM not only gives organizations critical insights into threats but also accurately scopes risk across the attack surface. This enables organizations to pinpoint where immediate responses are required. It also offers automated responses to threats for near real-time mitigation.

FortiSIEM VM is a centralized, multivendor security information and event management (SIEM) solution. Integrated within the Fortinet Security Fabric, FortiSIEM VM delivers transparent visibility and automated response and remediation across all security elements in a single, scalable solution. FortiSIEM VM unifies NOC-SOC analytics of all vendor products in the network.

Security Management and Analytics from the Cloud

Security organizations can leverage the global presence of top cloud infrastructure providers by deploying centralized and global security management and analytics systems. Using FortiManager VM, FortiAnalytics VM, and FortiSIEM VM, organizations have an integrated, cloud-based security management and analytics solution. The combined solution includes the same benefits organizations value in cloud computing, such as quick deployment, elasticity, and scalability. It also delivers efficient management and greatly reduced complexity.

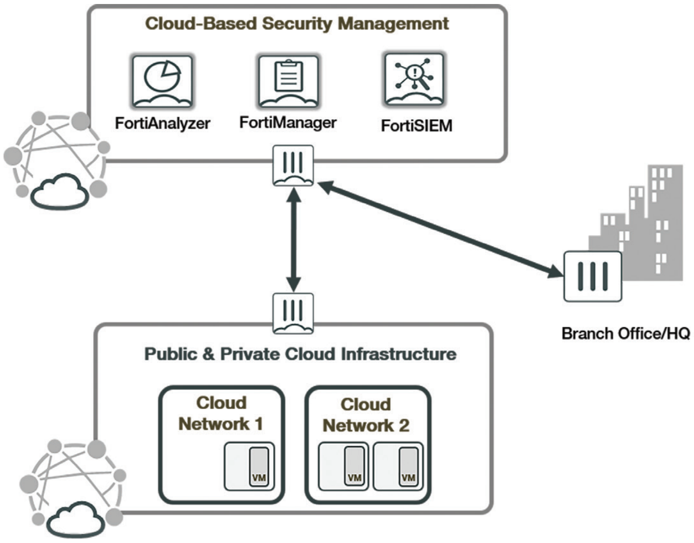

Figure 1: Security and analytics are deployed in the cloud to respond to the demands of managing the entire end-to-end environment.

[1] Security, management and compliance challenges are impacting cloud benefits, Help Net Security, January 11, 2018.

www.fortinet.com

July 24, 2019 8:15 AM

Macintosh HD:Users:ckluck:Downloads:sb-cloud-based-management Folder:c