Checklist: How Fortinet Helps CIOs Simplify Security Complexity

CIOs are measured on speed. Things like cloud applications and advanced development operations (DevOps) processes accelerate business cycles and enable radical new capabilities.

But speed without the right cybersecurity protections places businesses at risk. The same digital innovations that turbocharge business productivity can simultaneously create risk that needs to be managed. The full implications of a data breach can include: 1) data theft or ransom, 2) operational downtime, 3) brand degradation, 4) legal expenses, and 5) regulatory fines and penalties.

7 Ways That Fortinet Simplifies Security

Fortinet helps CIOs reduce network security complexity and the costs of continuously adding on more isolated products to cover new threats or risk exposures.

☑ Security integration.

The Fortinet Security Fabric integrates security solutions across the entire security infrastructure to reduce complexity and enable virtual real-time threat responses. It is based on an open ecosystem that incorporates third-party solutions to fortify protection while maximizing existing security investments.

☑ Transparent visibility and control.

Fortinet integrated security follows the attack surface, wherever it goes—from the data center, to the cloud, to the edge of the network. This enables transparent visibility and control across the entire attack surface and each security element via a single-pane-of-glass console.

☑ Threat intelligence at machine speed.

The Security Fabric creates the framework for rapid sharing of information to defend against sophisticated polymorphic threats and multivector attacks. It also supports automated detection, protection, and remediation responses.

☑ Intent-based segmentation.

With critical information now spread across increasingly extended networks, organizations must control access to data based on specific business intent. Intent-based segmentation enables granular access management (who, what, where), continuous trust assessment, and automated threat protection, as well as control for both east-west and north-south network traffic.

☑ Automated workflows.

Integration unlocks automation across the entire kill chain—including security information and events management, zero-touch deployment, and network access controls. Automating security processes enables security staff to extract themselves from daily log reviews and other manual processes and to focus on activities pivotal to the business. It also enables threat detection, prevention, and response in real time.

☑ Risk management.

All vulnerabilities cannot be patched in real time. CIOs need proactive risk management—dynamic dashboards that show how each vulnerability translates into risk. Fortinet does this—along with prevention, detection, and incident response processes that help shrink the window of risk exposure, accelerate time to remediation, and comply with security standards.

☑ Automated compliance tracking and reporting.

Fortinet provides built-in regulatory and security standards controls as well as tracking, reporting, and audit tools that help CIOs take a proactive approach to compliance. Automated reporting includes industry regulations such as the Payment Card Industry Data Security Standard (PCI DSS). It also extends to security standards such as the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS).

Simplify and Strengthen Network Defenses

The Fortinet Security Fabric integrates all of the elements of a security infrastructure while automating security workflows and threat-intelligence sharing. This enables CIOs to tackle complexity and costs head-on.

March 18, 2019 8:10 AM

Checklist-CIO-persona-problem

323490-0-0-EN