Checklist: How Fortinet Helps CIOs Keep up with the Rapidly Evolving Threat Landscape

For the CIO, cybersecurity is one of many responsibilities. Yet, inadequate protection literally threatens the success of all of the IT team's other initiatives. CIOs can often feel uncertain where to start when the threat landscape is in constant flux, not to mention increasing in volume, velocity, and sophistication.

6 Ways Fortinet Provides Complete Protection

Fortinet helps CIOs stay a step ahead of emerging threats with an integrated security architecture with consolidated, comprehensive threat intelligence. Integration enables transparent visibility, centralized control, and automation of security processes across the entire infrastructure.

☑ End-to-end, integrated security

The Fortinet Security Fabric integrates a broad portfolio of solutions across the entire security infrastructure to reduce complexity and provide protection against advanced and emerging threats. Full integration enables centralized visibility and control for the whole network.

☑ Open ecosystem

The Fortinet open ecosystem enables Fortinet Fabric-Ready Partners to develop integrations for their tools with the Security Fabric. For other security solutions, Fortinet provides developer scripts and tools—plus a robust representational state transfer application programming interface (REST API)—for customized integration with an organization's unique infrastructure.

☑ Automated security workflows

Deep integration unlocks automation across the spectrum of security processes—including security incident and event management (SIEM), zero-touch deployment, network access control (NAC), and compliance tracking. As a result, manual processes can be eliminated throughout the team so that scarce cybersecurity talent is focused on strategic initiatives.

☑ Threat detection at machine speed

Timely threat intelligence is the key to thwarting attacks—especially when so many threats are zero-day. FortiGuard Labs analyzes millions of files every day using artificial intelligence (AI) and machine learning (ML) techniques, resulting in extremely accurate analysis of new files. As an additional layer of protection, FortiSandbox examines unknown files before they enter the network to determine whether they are malicious.

☑ Comprehensive reporting and analysis

The Fortinet Security Rating Service provides a snapshot of an organization's security posture, generating a score that compares it with peer organizations and industry benchmarks—in a format that can be shared with executive management and the board of directors. Reporting from FortiManager and trends analysis from FortiAnalyzer help streamline compliance reporting and assist with strategic planning.

☑ Proactive risk management

Since intrusions will inevitably occur, CIOs need to take a proactive, risk management-based approach to assess where to expend resources. Fortinet real-time detection and threat response shrinks the window of risk exposure, and its dynamic dashboards show how each vulnerability translates into risk.

Strengthen Protection with a Comprehensive, Integrated Approach

The Fortinet Security Fabric provides comprehensive protection by integrating a broad suite of security tools and leveraging a robust threat-intelligence network that helps them stay ahead of bad actors and the malicious threats they instigate. For more information on the Fortinet Security Fabric, download a copy of the white paper, "Fortinet Security Fabric Powers Digital Transformation: Broad, Integrated, and Automated."

July 17, 2019 12:43 AM

323490-0-0-EN

D:\Fortinet\Checklist\FA\FA - Checklist - CIO Threat Landscape SS\FA - Checklist - CIO Threat Landscape SS