SOLUTION BRIEF

FortiNAC Supports Compliance with the NIST Cybersecurity Framework

Executive Overview

The National Institute of Standards and Technology (NIST) is working to standardize cybersecurity guidance so that security professionals across industries and verticals can speak the same language. NIST created its Cybersecurity Framework (CSF) to aid critical infrastructure organizations with their specific cybersecurity challenges. A third-generation network access control (NAC) solution—such as the Fortinet FortiNAC—helps ensure that only devices meeting set policies and regulatory compliance standards (including NIST CSF) can connect to the network, while concurrently providing visibility, control, and automated responses.

FortiNAC delivers:

- Comprehensive device visibility, including pre-connect and post-connect monitoring
- Granular network access controls to enforce minimum security requirements
- Automated threat responses to quarantine suspicious endpoints/users

Understanding the NIST Cybersecurity Framework

Taking enterprise network security to the next level requires strategic planning as well as a holistic understanding of an organization's unique risk profile, business challenges, and the security life cycle. The current state of cybersecurity guidance can sometimes seem disjointed and composed of countless standards endorsed by different agencies, governments, and private sector groups—and not all of which overlap in their advice. They may have the best intent to steer organizations beyond a "checkbox security" mentality, but conflicting sets of guidelines and requirements add confusion to an already complex ecosystem.

The NIST CSF was designed to eliminate these problems by establishing an industry-standard approach to cybersecurity for government organizations and critical infrastructure. Since a U.S. government executive order made compliance with the NIST CSF a requirement for all federal agencies in 2017, it is now being widely adopted by businesses as a yardstick against which companies measure their cyber-security practices relative to the threats they face.[1]

The NIST CSF provides a comprehensive inventory of every major step in the security life cycle using industry-agnostic language. It divides the key components of the security life cycle and its corresponding requirements into five core functions (Figure 1).

As part of the integrated Fortinet Security Fabric architecture, **FortiNAC** prepares organizations to comply with all five directives of the NIST CSF. It offers a flexible, third-generation NAC solution that can adapt to the unique needs of any network environment.

Identify: FortiNAC Enables Networkwide Visibility

Endpoint devices will remain a target for cyber criminals as long as they offer an easy, exploitable pathway to valuable data. With potentially thousands of endpoint devices on any given network, locating and securing a compromised device requires the ability to identify "who, what, when, and where" in an instant.

FortiNAC provides the deepest level of network endpoint visibility. It continuously profiles every endpoint on the network, and provides contextual awareness about the device, user, and applications. This includes Internet-of-Things (IoT) devices, which is currently an area of special interest for NIST researchers developing guideline updates.[2] It also discovers all infrastructure devices to detect and prevent risky network changes. In addition, FortiNAC automates guest management—tracking and monitoring all activity—which reduces the workload on IT staff.

Identify	Protect	Detect	Respond	Recover
• Asset management • Risk assessment • Inventory of devices, systems, platforms, and applications • Provide network-aware context to prioritize endpoint criticality • Identify and document asset vulnerabilities • Determine risk by measuring potential vulnerabilities, threats, and impacts • Identify and prioritize risk responses	• Access control • Data security • Information protection • Processes and procedures • Protective technology • Manage access of identities and credentials • Protect network integrity • Manage and protect physical access to assets • Manage remote access to assets • Manage access permissions • Manage assets throughout any removal, transfer, or disposition process • Verify software, firmware, and information integrity • Keep development and testing separated	• Anomalies and events • Security continuous monitoring • Detection processes • Triage critical nature of network alerts • Monitor network for potential events • Aggregate and correlate event data • Analyze detected events • Determine impact of events • Establish incident alert thresholds • Monitor physical environment for cybersecurity events • Monitor for unauthorized personnel, connections, devices, and software • Perform vulnerability scans • Test detection processes • Communicate event detection • Continuously improve detection	• Analysis • Mitigation • Improvements • Investigate notifications from detection systems • Understand incident impacts • Contain incidents • Perform forensics • Categorize incidents within response plan parameters • Mitigate or document newly identified vulnerabilities • Incorporate lessons learned into response plans • Update response strategies	• Recovery planning • Improvements • Communications • Providing valuable data points for post-mortems, future response plans, and communications to stakeholders • Executing a recovery plan • Incorporating lessons learned into recovery plan

Figure 1: The NIST CSF consists of five core elements.

Protect and Detect: FortiNAC Enforces Policy-based Controls

Once devices are seen, policies must be applied to enforce the necessary controls that protect organizations from endpoint-based vulnerabilities and associated threat vectors. FortiNAC enables organizations to verify that connecting devices meet compliance requirements—including NIST as well as the Health Insurance Portability and Accountability Act (HIPAA) and the European Union's General Data Protection Regulation (GDPR).

A majority (83%) of organizations report that they are at risk from mobile threats—and two-thirds (67%) say that they are less confident about the mobile asset security than other devices.[3]

FortiNAC also provides contextual awareness for scalable onboarding and dynamic access control. Network access is assigned using automated, predefined profiles—saving a significant amount of time when onboarding potentially thousands of endpoint devices concurrently. For managing BYOD devices, FortiNAC can set and enforce minimum security requirements for things like current operating system version and installed antivirus software. Here, using a pre-connect scan, FortiNAC only grants access for devices that meet requirements and can automatically direct users to a self-remediation page for those that do not qualify. FortiNAC also provides continuous post-connect scanning to look for devices and/or users that act suspiciously or fall out of network compliance.

In addition, FortiNAC gives organizations dynamic, granular control of endpoint access policies and permissions by role or by user to ensure users only receive the necessary amount of access. It creates network segments that keep compromised devices from accessing sensitive data or from causing extended problems across the organization. Automated containment responses across the integrated Fortinet Security Fabric go even further to protect organizations from sophisticated, endpoint-targeted attacks.

Respond and Recover: FortiNAC Automates Threat Responses

Organizations need to be able to instantly triage potential security events, generate actionable alerts, and then enforce endpoint containment to prevent the spread of infection. FortiNAC delivers real-time, automated threat responses that can immediately quarantine any suspicious devices/users (including IoT devices)—reducing containment time from days to seconds.

FortiNAC also features comprehensive history tracking and built-in analytics to accelerate forensic investigation and remediation efforts. It helps streamline analyst reviews by leveraging contextual awareness surrounding an alert to help quickly locate problem devices, diagnose problems, and prioritize security events. This in turn helps to accelerate time to resolution while reducing the burden on staff.

As a compensating control for IoT devices with weak security, FortiNAC monitors for unusual behavior and automatically quarantines suspicious endpoints. For example, if an IoT device starts pinging a DNS server, it will be tracked, an alert will be generated, and the port can be immediately locked down while awaiting analyst review.

Last year, the average cost of a data breach reached $3.92M.[4]

It currently takes an average of 279 days to identify and contain a breach.[5]

Enforcing Standards, Regulations, and Privacy Laws at the Device Level

As an integrated part of the Fortinet Security Fabric, FortiNAC provides comprehensive visibility, control, and automated responsiveness in support of NIST CSF compliance. Beyond these core capabilities, FortiNAC can be deployed as a physical appliance or a virtual appliance. Designed with scalability in mind, FortiNAC also helps lower total cost of ownership (TCO) by not requiring a server in every deployment location. As part of the Fortinet Security Fabric architecture, FortiNAC integrates seamlessly with firewalls and other security solutions to help organizations fortify endpoint defenses.

[1] Jaclyn Jaeger, "Understanding NIST's new Risk Management Framework," Compliance Week, February 8, 2019.

[2] Katerina Megas, "Let's talk about IoT device security," NIST, February 4, 2019.

[3] "Mobile Security Index 2019," Verizon, March 2019.

[4] "2019 Cost of a Data Breach Report," Ponemon Institute and IBM, July 2019.

[5] Ibid.

FORTINET

www.fortinet.com

September 26, 2019 2:20 AM

496175-0-0-EN

D:\Fortinet\Solution Briefs\purple solution briefs\FortiNAC - NIST SS\sb-fortinac-supports-compliance-with-the-nist-cybersecurity-framework-v2.1