INTEGRATED NETWORK ACCESS CONTROLS THAT MAXIMIZE SECURITY INVESTMENTS

EXECUTIVE SUMMARY

Digital transformation (DX) trends—including mobility, the Internet of Things (IoT), and cloud technologies—have helped enterprises reap significant productivity gains. But at the same time, they also bring extraordinary challenges for security architects when it comes to protecting the network from outside attack. It is imperative for organizations to define and implement a comprehensive security architecture that provides end-to-end network visibility, dynamic access control, and automated threat responses. FortiNAC offers an ideal network access control (NAC) solution without requiring a forklift upgrade of computing and network infrastructure. Its compatibility with a wide range of third-party security solutions helps enterprises secure sensitive data while maximizing the value of their existing infrastructure investments.

FORTINAC INTEGRATION EXTENDS VISIBILITY AND AUTOMATION

FortiNAC offers a policy-based security automation and orchestration solution that enables the discovery of every endpoint and network device, provides contextual awareness for implementing dynamic segmentation controls, and delivers the ability to instantly contain a potential cyber breach through automated threat responses. By automating the complex threat-triage process and rapidly responding to security alerts, FortiNAC helps prevent unauthorized access to corporate assets and intellectual property. It also reduces the impact, time, and cost of cyber-threat containment.

To make NAC cost-effective, FortiNAC integrates with leading third-party technologies across the enterprise. This security platform is based on open standards and provides a representational state transfer (REST)-based application programming interface (API), enabling bidirectional communication to and from FortiNAC to extend visibility, control, and responsiveness. This extends the reach of the Fortinet Security Fabric that leverages its connection to FortiNAC to manage and control policy updates to those security elements connected to FortiNAC. This also includes threat intelligence sharing and management. This is particularly important since many of those FortiNAC-connected elements are at the very edge of the enterprise network where vulnerable mobile and IoT devices reside.

BENEFITS OF FORTINAC

FortiNAC offers tangible benefits in four key areas:

1. Lower Total Cost of Ownership. FortiNAC integrates seamlessly with existing networking infrastructure, directory services, and security solutions to maximize an organization's existing investments while delivering complementary defensive functionalities. FortiNAC provides extensive support across 150+ vendors of switches, wireless, firewall, authentication, and client devices. This eliminates the need to replace or upgrade existing, functional gear that isn't supported by the NAC solution.

KEY SOLUTION FEATURES

- Comprehensive network visibility—all devices and users
- Enables dynamic segmentation controls
- Restricts access to sensitive data and IP
- Orchestrates automated threat responses
- Reduces containment from days to seconds
- Supports increasingly strict compliance requirements

2. Rapid Deployment and Scalability. The bidirectional REST-based API and syslog templates in the Security Fabric correlate various log fields from third-party solutions, making it extremely easy to deploy FortiNAC. In addition, inbound and outbound messages can be mapped to simple network management protocol (SNMP) traps. Compatibility with command line interface (CLI) of third-party network devices makes it easy to take advantage of native functionality of the networking device.

3. Accelerated BYOD and IoT Endpoint Adoption. Integration with wired and wireless infrastructure and enterprise mobility management (EMM) solutions allows FortiNAC to provide end-to-end network visibility with pre-connect risk assessment of endpoint devices. This helps address each customer's specific bring-your-own-device and IoT security challenges while accelerating device validation and onboarding.

4. Reduced Containment Time. Integration of FortiNAC with the Security Fabric's firewall, threat detection, and security information and event management (SIEM) solutions enhances the fidelity of security alerts. By correlating users, applications, and network connections to a compromised endpoint, FortiNAC delivers to security analysts alerts with relevant contextual data. Security alerts are triaged automatically and prioritized for one or more containment actions based on the severity and business impact of the incident.

Containment actions for compromised endpoints are then relayed to networking infrastructure devices. Responses can include termination of the connection, placing restrictions on network access, isolation into quarantine VLAN, and a range of notification actions.

A FLEXIBLE AND SCALABLE PLATFORM FOR CONTROLLING DEVICE ACCESS

FortiNAC offers a security automation and orchestration platform that can be deployed as a hardware appliance, a virtual appliance, or a cloud service—offering security architects a flexible, third-generation NAC solution that can adapt to the unique needs of any network environment. Designed with scalability in mind, FortiNAC also helps lower total cost of ownership (TCO) by not requiring a server in every deployment location. It leverages existing directory, networking, and security infrastructures to protect existing investments and minimize disruption.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapore 038988
Tel: +65-6395-7899
Fax: +65-6295-0015

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

247116-0-A-EN August 31, 2018 1:31 PM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:SB-FortiNAC-Integrated-Network-Access:sb-fortinac-integrated-network-access