FORTINAC AND THE FORTINET SECURITY FABRIC

EXECUTIVE SUMMARY

Outdated endpoint access security solutions leave mobile and Internet of Things (IoT) devices vulnerable to targeted attacks that can put the entire network at risk. To protect valuable data, organizations need next-generation network access control (NAC). As part of the Fortinet Security Fabric, FortiNAC provides comprehensive device visibility, enforces dynamic controls, and orchestrates automated threat responses that reduce containment time from days to seconds. It enables policy-based network segmentation for controlling access to sensitive information.

THE NEED FOR THIRD-GENERATION NAC

Enterprise networks are undergoing dramatic change through the widespread adoption of bring-your-own-device (BYOD) policies, IoT, and multi-cloud technologies. When this is coupled with a highly mobile workforce and geographically dispersed data centers, the security challenges multiply. With endpoint devices remaining a top attack target, organizations must address the outdated access controls that leave their networks exposed to undue risk.

The first generation of NAC solutions authenticated and authorized endpoints (primarily managed PCs) using simple scan-and-block technologies. Second-generation NAC products solved the emerging demand for guest network access—visitors, contractors, and partners.

But securing dynamic and distributed environments now requires security and networking that share intelligence and collaborate to detect and respond to threats. As part of the Fortinet Security Fabric architecture, FortiNAC offers a third-generation NAC solution that leverages the built-in commands of network switches, routers, and access points to establish a live inventory of network connections and enforce control over network access. FortiNAC identifies, validates, and controls every connection before granting access.

COMPREHENSIVE DEVICE AND USER VISIBILITY

As a result of BYOD and IoT proliferation, security teams must now protect countless devices that aren't owned, managed, or updated by corporate IT. FortiNAC addresses this challenge in a couple of different ways. First, it enables detailed profiling of even headless devices using multiple information and behavior sources to accurately identify everything on the network. Comprehensive agentless scanning automatically discovers endpoints, classifies them by type, and determines if the device is corporate-issued or employee-owned. Second, the user is also identified in order to apply additional role-based policies.

HIGHLIGHTS

- Comprehensive network visibility
- Profiles and classifies all devices and users
- Provides policy-based access controls
- Extends dynamic segmentation to third-party devices
- Orchestrates automated threat responses
- Contains potential threats in seconds
- Simplifies guest access and onboarding
- Low TCO—maximizes existing security investments

DYNAMIC NETWORK CONTROL

Once devices and users are identified, FortiNAC assigns the appropriate level of access while restricting use of non-related content. This dynamic, role-based system logically creates detailed network segments by grouping applications and like data together to limit access to specific groups of users. In this manner, if a device is compromised, its ability to travel in the network and attack other assets will be limited. Security Fabric integration allows FortiNAC to implement segmentation policies and change configurations on switches and wireless products, including solutions from more than 70 different vendors.

FortiNAC also streamlines the secure registration process of guest users while keeping them safely away from any parts of the network containing sensitive data. When appropriate, users can self-register their own devices (laptops, tablets, or smartphones), shifting the workload away from IT staff.

AUTOMATED RESPONSIVENESS

Automation is the “holy grail” of an integrated security architecture. Policy-based automated security actions help Security Fabric solutions share real-time intelligence to contain potential threats before they can spread. FortiNAC offers a broad and customizable set of automation policies that can instantly trigger containment settings in other Security Fabric elements such as FortiGate, FortiSwitch, or FortiAP when a targeted behavior is observed. This extends to all Fabric-integrated products, including third-party solutions.

Potential threats are contained by isolating suspect users and vulnerable devices, or by enforcing a range of responsive actions. This in turn reduces containment times from days to seconds—while helping to maintain compliance with increasingly strict standards, regulations, and privacy laws.

HOW IT WORKS

As an integrated Security Fabric solution, FortiNAC helps to provide additional layers of protection against device-borne threats. For example, if a customer is using FortiSIEM, FortiNAC provides complete visibility and policy-based control for network, mobile, and IoT devices, while FortiSIEM provides the security intelligence.

FortiNAC offers complete visibility into all of these devices, gathers the alerts, and provides the contextual information—the who, what, where, and when for the events. This increases the fidelity of the alerts and enables accurate triage.

FortiNAC sends the event to FortiSIEM to ingest the alert, then FortiSIEM directs FortiNAC to restrict or quarantine the device if necessary. FortiSIEM and FortiNAC communicate back and forth to compile all relevant information and deliver it to a security analyst.

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

August 31, 2018 12:32 PM

Macintosh HD:Users:bhoulihan:Documents:_Projects:Solution Brief:Solution Brief - FortiNAC:sb-fortiNAC:sb-fortiNAC