FORTINAC: SECURITY AUTOMATION AND ORCHESTRATION PLATFORM

EXECUTIVE SUMMARY

The widespread adoption of cloud, Internet of Things (IoT), and mobile technologies has changed the nature of how enterprises must secure their networks. Outdated security measures are leaving endpoint devices vulnerable to targeted attacks. To protect valuable data, organizations need next-generation network access control (NAC). In this context, FortiNAC provides a policy-based security automation and orchestration platform that enables discovery of every endpoint and network infrastructure device, provides contextual awareness for implementing dynamic network access control, and the ability to contain a cyber breach through automated threat responses.

FORTINAC: TRANSPARENCY, DYNAMIC, AUTOMATED

Cyber criminals continue to choose endpoint devices as a favorite attack point for gaining illicit access to enterprise networks. To address these threats, organizations have been spending 1,156 hours each week on detecting and containing endpoint-borne risks—an average of $3.4 million weekly.[1]

Automating endpoint detection and response solutions is the top priority for IT professionals trying to put actionable controls around their endpoints.[2] Automated responses and workflows enable faster detection and better protection, while reducing the strain on over-burdened and under-resourced security teams.

As an integrated part of the Fortinet Security Fabric, FortiNAC offers a next-generation NAC solution that delivers end-to-end network visibility, dynamic network access control, and automated threat responsiveness. By automating the complex threat triage process and rapidly responding to security alerts, FortiNAC minimizes the risk of unauthorized access to corporate assets and intellectual property while reducing the impact, time, and cost of containing device-borne threats.

VISIBILITY ACROSS THE NETWORK

Fundamental to the security of a constantly changing network is understanding its makeup—you can't protect what you can't see. An effective NAC platform must facilitate access orchestration by first seeing every user, application, and device on the network.

IDENTIFICATION AND CLASSIFICATION OF ENDPOINTS AND USERS

FortiNAC uses agentless scanning to profile each element on the network based on observed characteristics and behavior, as well as noting the need for software updates and patches. FortiNAC automatically discovers and profiles endpoints, classifying devices by type and determining if it is corporate-issued or employee-owned. The user is also identified and the appropriate role-based network access policies are implemented within FortiNAC to protect critical data and sensitive assets.

SIMPLIFYING GUEST ACCESS

FortiNAC streamlines the secure registration process of guest users. When appropriate, users can self-register their own devices—laptops, tablets, or smartphones—shifting the workload away from the IT staff. Or, the simplified task of onboarding guests can also be delegated to designated network administrators.

GRANULAR ACCESS CONTROLS

Beyond the high volume and diversity of devices, corporate networks also host a breadth of different users, groups, and applications. To manage this complexity, a NAC solution must be able to provide dynamic access controls and segmentation.

DYNAMIC NETWORK SEGMENTATION

Once devices and users are identified, FortiNAC assigns devices and users the appropriate level of access while restricting their 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 a specific group of users. In this manner, if a device is compromised, its ability to travel in the network and attack other assets will be limited.

FortiNAC can automatically implement segmentation policies and change configurations on switches and wireless products from more than 70 vendors. This tapping of third-party products extends the reach of the Security Fabric in heterogeneous environments.

CONTINUOUS RISK ASSESSMENT

Ensuring the integrity of a device before it connects to the network minimizes risk and the possible spread of malware. FortiNAC validates a device's configuration as it attempts to join the network. If the configuration is found to be noncompliant, the device can then be relegated to an isolated or limited-access VLAN. Users are then warned that their device must be remediated. Access is granted only after corrective measures have been taken. Even then, FortiNAC performs ongoing deep information scanning to provide continuous evaluation post-connection.

SECURITY AUTOMATION

Policy-based automated security actions are the "holy grail" of an integrated security architecture. They allow the NAC solution to share real-time intelligence across the organization to contain potential threats before they can spread. Automation also reduces the strain on overburdened and under-resourced security teams.

DRAMATICALLY REDUCE TIME TO CONTAINMENT

FortiNAC offers a broad and customizable set of policies that enable errant device or user behavior to instantly set containment in motion across the Security Fabric. Once a compromised or vulnerable endpoint is identified, FortiNAC triggers an automated response. This can include termination of connection, restrictions on network access, quarantine isolation, and/or a range of notification actions. Control features are accessed via a highly customizable, easy-to-use, web-based administrative dashboard. FortiNAC reduces containment time from days to seconds—while maintaining compliance with increasingly strict regulations, standards, and data privacy laws.

ALERT PRIORITIZATION

FortiNAC enhances the fidelity of security alerts by correlating users, applications, and network connections to a compromised endpoint and sharing that intelligence across the Fortinet Security Fabric. The security alerts are triaged automatically and prioritized for one or more containment actions based on the severity and business criticality of the security incident.

ENABLING FLEXIBLE AND SCALABLE NAC DEPLOYMENTS

FortiNAC offers a security automation and orchestration platform with unparalleled visibility, control, and automated responsiveness. Beyond those core capabilities, FortiNAC 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.

[1] "The Cost of Insecure Endpoints," Ponemon Institute, June 2017.
[2] Lee Neely, "Endpoint Protection and Response: A SANS Survey," SANS Institute, June 12, 2018.

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 12:29 PM
246973-0-0-EN
Macintosh HD:Users:bhoulihan:Documents:_Projects:Solution Brief:FortiNAC - Automation and Orchestration:sb-fortiNAC-automation-orchestration:sb-fortiNAC-automation-orchestration