SOLUTION BRIEF

Fortinet and Jamf Pro Network Security

Broad and Automated Solution for Integrating Network Access Controls with Device Management to Secure the Perimeter and Protect the End-user Experience

Executive Summary

Fortinet and Jamf offer an integration to eliminate the security risks associated with unsecured devices accessing the network by evaluating enrollment and compliance with Jamf Pro policies.

Challenge

Apple has changed the mobility landscape. Users are no longer tethered to a desk, and the device of choice for most users is wireless only. Historically, Wi-Fi access has meant a compromise in either security or user experience. Mobile device management solves part of this by securing the exchange of network credentials, but it also creates an opportunity for enhanced network security.

Jamf and Fortinet have partnered to deliver a conditional network access solution to ensure only trusted devices are granted seamless access to resources on the network, and unknown devices are not. This solution gives peace of mind to organizations scaling up their Apple mobility deployments.

Joint Solution

The integration of Jamf Pro and Fortinet FortiNAC and FortiClient, enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, delivers increased visibility and security for network admins.

Jamf makes products that simplify the process of managing, protecting, and connecting Apple devices at scale. To take the consumer Apple experience that everyone knows and loves, add the security and configurations required to be productive, and then scale that experience to thousands of devices is exactly what Jamf does every day. Connecting devices to the network layer is important, but when Jamf Pro is paired with Fortinet FortiNAC, ongoing security analysis ensures proper security controls are in place before allowing devices full network access.

Jamf is a comprehensive companion to Fortinet solutions. In addition to FortiNAC integration, Jamf Pro can also help administrators deploy FortiClient and associated virtual private network (VPN) and secure sockets layer (SSL) settings to macOS and iOS, closing the loop on data in transit.

Joint Solution Components

- Jamf Pro 10.0+
- Fortinet FortiNAC
- Fortinet FortiClient

Joint Solution Benefits

- Increased contextual awareness provided to FortiNAC and FortiClient for individual device analysis
- Invisible security layer, transparent to users with enrolled and compliant devices

Joint Solution Components

Jamf Pro 10.0+

Jamf automates device deployment, management, and security without impacting the end-user experience or requiring IT to touch the device. Jamf preserves the native and consistent Apple experience that people expect at work, while fulfilling the security and compliance requirements of the enterprise.

Fortinet FortiNAC

The FortiNAC solution protects both wireless and wired networks with a centralized architecture that enables distributed deployments with automated responsiveness. FortiNAC enables three key capabilities to secure IoT devices: network visibility to see every device and user as

they join the network, network control to limit where devices can go on the network, and automated response to speed the reaction time to events from days to seconds. Collectively, these three capabilities provide the tools that network owners need to secure a world that is embracing the Internet of Things (IoT).

Fortinet FortiClient

FortiClient strengthens endpoint security through integrated visibility, control, and proactive defense. With the ability to discover, monitor, and assess endpoint risks, you can ensure endpoint compliance, mitigate risks, and reduce exposure. FortiClient proactively defends against advanced attacks. Its tight integration with the Security Fabric enables policy-based automation to contain threats and control outbreaks. FortiClient is compatible with Fabric-Ready Partners to further strengthen enterprises' security posture.

Joint Solution Integration

Devices connecting to the network are registered in FortiNAC using host data from Jamf. FortiNAC can also gather application data from the Jamf server to assist in FortiNAC policy creation. FortiNAC profiles each element based on observed characteristics and responses, and can call on FortiGuard IoT Services, a cloud-based database for identification lookups.

FortiNAC assesses a device to see if it matches approved profiles, noting the need for software updates to patch vulnerabilities. Once the devices are classified and the users are known, FortiNAC enables detailed segmentation of the network to enable devices and users access to necessary resources while blocking nonrelated access. FortiNAC monitors the network on an ongoing basis, evaluating endpoints to ensure they conform to their profile.

Joint Use Cases

Use Case #1

Corporate-owned devices should be able to connect to the network with minimal user interaction. Jamf can not only deliver secure network credentials but it can also register devices with FortiNAC as they come online.

Use Case #2

Bring your own device (BYOD) can be difficult to deal with when it comes to network access control. Jamf Pro supports enrollment methods that embrace BYOD and integrate with network security tools like FortiNAC.

About Jamf

Jamf, the standard in Apple Enterprise Management, extends the legendary Apple experience people love to businesses, schools, and government organizations through its software and the largest online community of IT admins focused exclusively on Apple in the world, Jamf Nation. To learn more, visit: www.jamf.com.

September 4, 2020 5:07 AM

771406-0-0-EN

D:\Fortinet\Solution Brief\Grey Solution Brief\Jamf\sb-FA-fortinet-and-jamfpro-network-security-942020