SOLUTION BRIEF

Fortinet and the Wandera Security Suite

Unified Cloud Security for the Connected Enterprise

Executive Summary

As your employees go mobile, so does your data. To keep your business secure, security needs to extend beyond the perimeter. Complement your Fortinet FortiGate next-generation firewalls (NGFWs) with the Wandera Security Suite to detect threats, prevent data breaches, and even identify and stop attacks before threats reach your business.

Introduction

With significant advances in cloud computing and mobile technologies, data is no longer constrained to the corporate data center. Applications have migrated to the cloud and are built for mobility, empowering people—both employees and contractors—to work and collaborate with ease. Mobile devices and widespread connectivity have allowed workers to stay connected to data and one another, regardless of physical location.

But there is a downside to this hyperconnectivity that introduces significant risk. The physical corporate boundaries that restricted users, data, and applications from connecting are no longer in place to keep cybersecurity risks from coming into the organization. The perimeter has disappeared. With boundaries no longer in place to protect, organizations must now focus their attention on protecting data, wherever it is.

Fortinet and Wandera have partnered to deliver an industry-leading security solution to address these needs. Bringing together Wandera's cloud-delivered security suite with the industry-leading Fortinet FortiGate NGFW platform, organizations are able to empower remote workers with leading threat defense and zero-trust network access solutions, while simultaneously leveraging Fortinet services at the network edge. This joint solution ensures that workers are always protected and that policy enforcement is consistent, both on and off campus.

The Enterprise Perimeter Has Changed

In recent years, corporate data has increasingly shifted to mobile devices, with more than half of internet use occurring on mobile endpoints. Connecting workers to company services and data through mobile devices has completely changed the way employees work, providing speed and flexibility to enable easier access to information. But along with these benefits, organizations are now exposed to new threat vectors attacking users and data outside the traditional security perimeter, including mobile-based malware, phishing attacks, cryptojacking, man-in-the-middle attacks, and sideloaded and malicious apps. Once infected, these devices can return inside the perimeter, exposing critical business systems to attack. With mobile devices forming an increasingly important part of business workflows, organizations need to be able to solve associated cybersecurity challenges. With the majority of successful phishing attacks on mobile taking place outside of email, legacy security solutions that many businesses have deployed are unable to provide the necessary visibility and control as data leaves the perimeter.

Joint Solution Components

- Fortinet FortiGate Next-Generation Firewall
- Fortinet Secure Web Gateway
- Fortinet FortiSIEM
- Wandera Threat Defense App
- Wandera Secure Access Layer
- Wandera Cloud Gateway

Joint Solution Benefits

- Industry-leading protection of company data, both inside and outside the perimeter
- Consistent and always-on protection for workers that includes mobile threat defense and in-network policy enforcement
- Zero-day phishing protection for all mobile apps, including email, SMS, social media messengers, and web browsers
- Acceptable use and compliance policies that are in effect on the campus or in the coffee shop
- Empower mobile workers while staying secure with adaptive access to company applications on-premises and in the cloud
- Gain unparalleled network security protection with the industry-leading FortiGate next-generation firewall platform and the Fortinet Security Fabric

Fabric-Ready

Joint Solution Components

Threat Defense App

Protect against all cyber threats, from device vulnerabilities to malicious or risky apps, with Wandera's leading threat defense solution and advanced threat intelligence, MI:RIAM.

Secure Access Layer

Stop network-based attacks from reaching your mobile endpoints when connected from off-campus locations using Wandera's Secure Access Layer.

Cloud Gateway

Augment your campus-based secure web gateway (SWG) to prevent non-business data use from impacting productivity, causing bill shock and increasing legal liability. Control how, when, and where your data is used with Wandera's Cloud Gateway for mobile devices.

FortiGate Next-Generation Firewall

FortiGate NGFWs enable security-driven networking and consolidate industry-leading security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection. Fortinet NGFWs meet the performance needs of highly scalable, hybrid IT architectures, enabling organizations to reduce complexity and manage security risks.

Fortinet Secure Web Gateway

Fortinet SWG capabilities provide an end-to-end secure web experience with URL filtering, data loss prevention, and advanced malware protection including remote browser isolation to defend users from internet-borne threats, and to help enterprises enforce internet policy compliance.

FortiSIEM

FortiSIEM enables unified data collection and analytics from diverse information sources including logs, performance metrics, SNMP traps, security alerts, and configuration changes. FortiSIEM takes the analytics traditionally monitored in separate silos—SOC and NOC—and brings that data together for a comprehensive view of the security and availability of the business.

Joint Solution Integration

Consistent protection, both inside and outside the corporate perimeter

Fortinet provides best-in-class network security through its award-winning **FortiGate** next-generation firewall platform and the integrated **Fortinet Security Fabric** architecture. The **Fortinet Security Fabric** allows security components to share intelligence between devices and systems. This joint solution supports a single console for the security analyst, with security events streaming in real time from Wandera to **FortiSIEM**, allowing the organization to have a comprehensive assessment of its overall security posture. This open architecture of connected defenses allows organizations to scale and adapt their security as business demands change while addressing the full spectrum of cyber threats across an ever-expanding attack surface.

For remote workers, the **Wandera Security Suite** adds on-device and in-network threat defense, providing effective protection against device vulnerabilities, malicious or risky apps, man-in-the-middle attacks, and content security threats like mobile phishing. In addition, Wandera's Threat Event Stream sends all security logs to **FortiSIEM**, enabling centralized threat hunting and security operations.

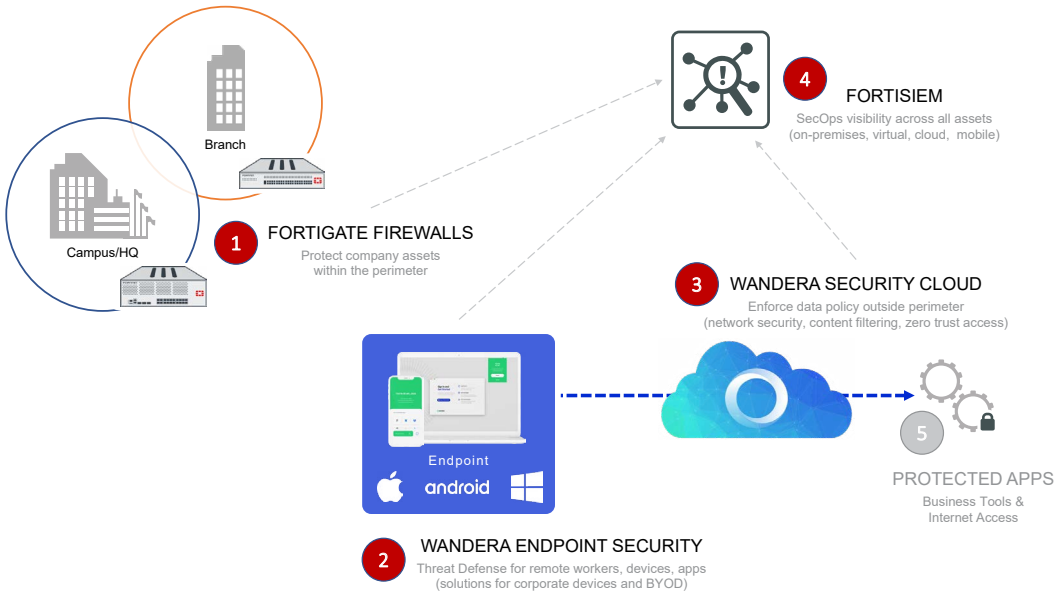

Figure 1: Fortinet-Wandera Integration.

Joint Use Cases

Use case 1: Advanced threat defense and policy for remote workers

Users are now empowered to work outside the protected corporate network with devices such as SIM-enabled Windows 10 laptops, but requiring a virtual private network (VPN) to backhaul traffic to campus can slow down productivity.

Wandera keeps users protected and connected while working away from campus with advanced threat defense across all network connections that may be outside the organization's firewall scope, including cellular and public Wi-Fi.

Use case 2: Application security for managed and unmanaged devices

Many businesses have embraced a modern workplace that allows unmanaged devices, including personal bring your own device (BYOD), to access sensitive company applications. Due to privacy concerns, these devices are not protected by management solutions; this means if a device is compromised, IT is powerless to stop the threat.

The Wandera Security Suite can be deployed to both managed and unmanaged devices, ensuring consistent policy across the entire workforce and providing extended privacy protections for workers. Wandera enables secure access to company applications, while continuously monitoring for risk. A variety of policy actions are available to prevent threats from compromising company data, and integration with FortiSIEM ensures that security operations are alerted at the first sign of a threat.

About Wandera

Wandera, a cloud security company, protects modern enterprises beyond the traditional perimeter. When remote users access applications from their smartphones or laptops, anywhere in the world, Wandera's unified security cloud provides real-time threat protection, content filtering, and zero-trust network access. Wandera regularly shares the latest findings from its industry-leading threat intelligence which applies machine learning across 425M worldwide sensors. Founded in 2012 by a team of cloud security veterans and recognized as a leader by analyst firms including Gartner and IDC, the company is headquartered in San Francisco and London. To learn more, please visit www.wandera.com

November 3, 2020 3:56 AM

820522-0-0-EN

D:\Fortinet\Solution Brief\Grey Solution Brief\Wandera\sb-FA-fortinet-and-the-wandera-security-suite-10272020\sb-FA-fortinet-and-the-wandera-security-suite-10272020