SOLUTION BRIEF

WWT and Fortinet Network, Edge, Operational, and Distributed Workforce Security Strategies

Best Practice Solutions and Services for SD-WAN, SASE, Endpoints, Teleworkers, and OT

Executive Summary

With today's cybersecurity attack challenges, the security experts at WWT, and Fortinet have partnered to provide best-in-class solutions and services including:

- WWT's Advanced Technology Center (ATC) to facilitate lab tests, proofs of concept (POCs), and integrated solution demonstrations across the Fortinet Security Fabric
- Zero Trust security model expertise and implementation
- Software-defined wide area networking (SD-WAN) solutions and services
- Secure access service edge (SASE) and endpoint security solutions and services
- Remote teleworker and operational technology (OT) security best practices and security expertise

Security Challenges

SD-WAN: Security-driven networking for branch networks with outstanding performance enabled by fast application identification and automated path intelligence.

- Application awareness for improved service levels
- Optimal application experience with accurate detection
- Effective business policies based on application signature
- Continuous application database updates from FortiGuard Labs research

Zero Trust Model: WWT has found that adopting a Zero Trust security model should be consideration in all security plans. The proven framework dictates that trust extends beyond network proximity and Internet-of-Things (IoT) devices. Trust should never be assumed, but instead proven through a set of intentional actions, such as device and user verification. WWT can help your team implement a Zero Trust model using a five-step process:

- **Expand your audience** by securing alignment and executive support within your firm
- **Address asset discovery inventory** by gaining visibility into all IoT devices and endpoints
- **Understand data classification** by ensuring you have a set of data labels and data tags
- **Address user and device access** by implementing the right identity access technologies
- **Address enterprise segmentation risks** by dividing your network into isolated segments

About Fortinet

Fortinet is now the #1 cybersecurity company in the world with 465,000 worldwide customers and more than 30 cybersecurity product lines, including advanced solutions for SASE, SD-WAN, teleworkers, OT, and endpoints. Fortinet secures the largest enterprises and government organizations around the world with intelligent, seamless protection across an expanding attack surface.

About WWT

WWT is a Fortinet Expert Partner that uses a proven and innovative approach to help our customers evaluate, architect, and properly implement Fortinet solutions. WWT's Advanced Technology Center (ATC) offers a unique and robust testing and research lab environment for IT and security teams. The ATC is a software-defined next-generation data center that can help you explore, test, and prove any Fortinet technology. We combine data centers, cloud infrastructures, vendor solutions, and trained experts to help you test, validate, and prove concepts, products, and strategies.

SASE: Ensures security for every edge and solves much of the scalability and infrastructure issues that arise in large, distributed organizations that are highly dependent upon Infrastructure-as-a-Service(IaaS)/Software-as-a-Service (SaaS).

- Combines network and security functions with WAN capabilities for dynamic, secure access
- SASE solutions bring security to the edge and solve infrastructure vulnerability issues
- WWT offers expertise, test labs, and concept testing to determine appropriate SASE solutions
- Industry-leading managed security services backed by multiple security operations centers

Teleworkers: Advanced security controls for remote teleworkers including FortiGate virtual private networks (VPNs), FortiToken identity authentication, FortiAP secure wireless connectivity, and FortiGate next-generation firewalls (NGFWs).

- Defend against escalating cyberattacks on unsecure remote workforces
- Ensure the right hardware processing power to support encrypted tunnels for remote workers
- Create safe connections by combining FortiClient endpoint fabric agents with FortiGate NGFWs

Operational Technologies: WWT and Fortinet operational technology cyberthreat solutions integrate with an automated security architecture to deliver visibility, control, and real-time traffic analysis to proactively neutralize threats.

- Single-vendor, end-to-end, integrated cybersecurity architecture across IT and OT, from protection to detection to response
- Provide visibility on OT risks to identify assets and potential vulnerabilities, provide proactive threat defense, and classify and prioritize risks
- Minimize risk by constantly analyzing traffic for threats and vulnerabilities
- Control access through role-based access and identity management
- Secure both wired and wireless access, including bring-your-own-device (BYOD) devices

Endpoints: WWT experts have found that traditional endpoint detection and response (EDR) solutions often require manual triage and responses that are not fast enough to stay ahead of risks. They also create a large volume of "false positive" alerts that burden analysts and security teams. To properly secure endpoints, WWT recommends the following:

- FortiEDR advanced, real-time, pre- and post-infection threat protection for endpoints
- FortiClient to strengthen endpoint security through integrated visibility, control, and defense
- WWT services to ensure compliance, mitigate risks, and reduce false positive alerts

FORTINET

www.fortinet.com

December 22, 2020 1:59 AM

867866-0-0-EN

D:\Fortinet\Image Graphics\Pam Seeds\867310 - 2020 Q4 WWT Partnership\sb-q4-wwt-partnership-2020-V3-12222020\sb-q4-wwt-partnership-2020-V3-12222020