SOLUTION BRIEF

Critical Security Controls to Enhance Your Campus FortiGate

Executive Summary

Protecting campus networks can be complex. Unlike branch offices, data centers, and remote sites, campus locations host multiple on-site departments that rely on the internet and both cloud-based and on-premises applications for business-critical operations. Campus networks are also more complex because they often include a dynamic guest presence and operational technology (OT) and Internet-of-Things (IoT) technologies that require secure, always-on connectivity. And campuses spanning several industries often carry various compliance requirements that must be tracked, monitored, and reported on. Such factors make defending the campus network challenging, especially as each device, user, and transaction provides ways for malicious attackers to gain entry into the wide area network.

FortiGate Next-Generation Firewalls (NGFWs), as part of a hybrid mesh firewall architecture, protect dynamic campus networks using powerful AI-powered security services that provide deep visibility into all users, devices, and applications. Every FortiGate NGFW also contains a proprietary SPU, a dedicated ASIC designed to offload resource-intensive security and networking functions from the main CPU to deliver critical functions without impacting network performance. That means your FortiGate will deliver the industry's highest ROI and best stakeholder experience while keeping the network secure.

Fortinet provides a variety of services designed for every use case. Here are the top five FortiGuard Security Services designed for campus networks to ensure your business operates safely and without disruption.

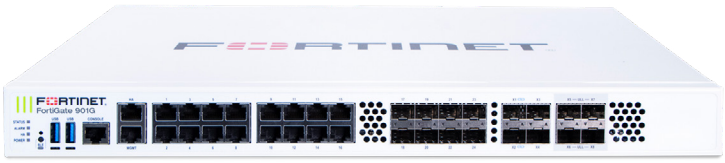

Figure 1: FortiGate 901G

Essential Services Provide Enhanced Security for Campus Deployments

FortiGuard Labs provides a variety of services to enhance the ability of FortiGate NGFWs to identify and protect against active threats, as well as enhance the ability of IT teams to more effectively manage and secure their overall network.

According to Gartner, security is the top spending priority for enterprise customers, expected to exceed $1.1 trillion from 2022 through 2026. By 2026, over 85% of organizations worldwide will need to be compliant with modern data protection requirements.[1]

The following services provide enhanced security for FortiGate NGFWs deployed in campus environments:

URL and DNS filtering

Regardless of their industry or sector, people working in campus environments require access to the internet to do their jobs. But that access introduces risks that must be addressed. According to the 2023 Verizon Data Breach Investigations Report, 64% of ransomware attacks involved malicious URLs, with the majority of these attacks initiated by social engineering.[2] And new developments in AI, such as ChatGPT, are making social engineering simpler and more effective. "A single scammer, from their laptop anywhere in the world, can now run hundreds or thousands of scams in parallel, night and day, with marks all over the world, in every language under the sun."[3]

The URL and DNS filtering services from FortiGuard Labs ensure that hyperlinks sent across the campus network are genuine and won't lead to ransomware or a malicious website.

Antivirus and inline sandbox

Email attachments are among the most common ways users share files, with more than 262.6 billion email attachments being sent in 2022.[4] File attachments are also one of the most common collaboration methods in campus networks. They are also a popular attack vector for spreading malware, such as ransomware.

Antivirus protection is essential for properly defending campus network users from malicious file attachments. But an antivirus solution must be able to identify malicious files and new threats, such as polymorphic malware that changes from benign to malicious over a set of actions or period of time. Built-in antivirus and the FortiGuard Labs antivirus service keep your FortiGate NGFW constantly updated against the latest threat landscape.

Inline sandbox is another essential campus network security service due to the volume of data being shared across departments. A high-performance inline sandbox service utilizes machine learning technology to identify and isolate advanced threats in real time. It inspects network traffic, files, and URLs for malicious activity, including zero-day threats, and uses sandboxing technology to analyze suspicious files in a secure virtual environment.

Fortinet introduced the industry's first AI-powered inline blocking on a NGFW. This function allows FortiGate NGFWs to hold suspicious files and send them to the inline sandbox for analysis, which provides sub-second verdicts. This is accomplished by leveraging patented FortiGuard AI/ML analysis combined with our global threat intelligence ecosystem. Only files that are certified as clean are allowed into the network. This inline blocking service allows organizations to focus on security without impacting productivity or user experience.

Hardware-accelerated IPS and security rating service

Because so many devices are deployed in campus networks—from endpoint clients to servers and other network infrastructure—unpatched and zero-day vulnerabilities are a major entry point for attacks looking to breach the network and then move laterally in the network.

And while the estimated cost of a data breach is expected to hit $5,000,000,[5] detecting an exploited device can take months, allowing attackers to burrow deep into the network to find and steal critical information. That's why IT must be able to detect and virtually patch device vulnerabilities in campus networks as quickly as possible.

Fortinet offers hardware-accelerated virtual patching via IPS that enables IT teams to protect against device vulnerabilities without impacting campus end-user experiences. The Fortinet Content Process ASIC (CP9) offloads IPS functions from the main CPU, dramatically improving the performance of the firewall device and driving the industry's highest ROI. At the same time, advanced services keep the onboard IPS updated with the latest signatures pulled from our global network of sensors enhanced with our patented AI system that can collect and correlate billions of events to identify emerging threats and identify critical vulnerabilities and configuration weaknesses.

The FortiGuard Security Service also enables IT teams to build a security roadmap and target security maturity level goals using measurable and meaningful feedback. The following services provide actionable configuration recommendations and critical performance and risk indicators. They also help build senior management confidence by demonstrating effective business asset protection and compliance with regulatory requirements.

OT and IoT

Nearly every campus network includes IoT devices that must be managed and secured. However, most IoT devices do not include security or even the ability to be patched or updated. Monitoring, tracking, and protecting these devices requires a systemic approach.

Many campus networks also include industrial facilities that include specialized industrial IoT tools. Defense involves much more than simply protecting end-users connecting their workstations to cloud applications. Industrial environments include operational machines like factory robots, conveyor belts, pumping stations, temperature controls and valves, and other systems that rely on the internet. Outages can cost businesses millions of dollars in lost revenue, so their consistent and secure connectivity is paramount to many IT organizations.

As a result, campus network security must include defenses for OT and IoT devices. The FortiGuard Industrial Security Service and IoT Detection Service complement the FortiGuard IPS Service so your organization can discover, identify, and protect against attacks targeting OT and IoT devices. In addition, FortiGuard services can analyze and deploy new OT and IoT IPS signatures across the network in near real time for a coordinated network response. Multiply this workflow across Fortinet's global customer base, and you have a network effect that accelerates protection for OT and IoT devices.

SOC-as-a-Service

In today's dynamic cybersecurity landscape, properly monitoring firewall logs, alerts, and notifications has become increasingly crucial. The growing sophistication of cyberthreats, combined with the recent rise in consumerized AI, has made it easier for attackers to deploy sophisticated techniques at scale, putting businesses at significant risk. Moreover, the proliferation of internet-connected devices, cloud computing, and IoT has exponentially expanded the attack surface, resulting in a flood of logs, alerts, and notifications generated by firewalls, making it challenging to identify and respond to genuine security incidents.

The FortiGuard SOCaaS (Security Operations Center-as-a-Service) addresses these challenges. With FortiGuard SOCaaS in place, businesses can quickly and affordably establish the necessary monitoring and detection tools without substantial upfront investments in personnel, time, or tools.

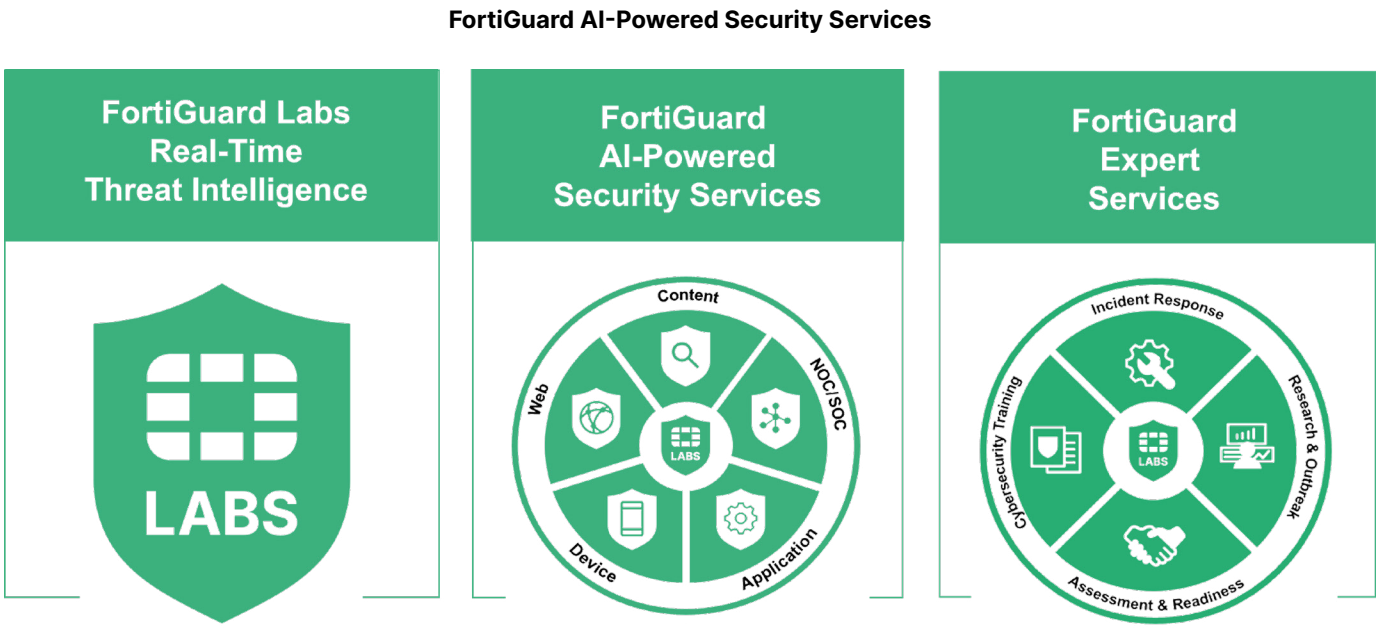

Figure 2: FortiGuard Services deliver essential protections across the distributed enterprise

FortiGate NGFWs Address the Unique Challenges of Today's Campus Networks

Campus networks, regardless of their industry or location, are difficult for IT to defend because of several critical factors, including:

- Rich internet usage, including web links and file attachments from multiple on-site departments
- Dynamic guest access environments
- Robust IoT and OT connectivity

In today's increasingly sophisticated campus environments, it's essential that you have advanced, multilayered protection. FortiGate NGFWs, as part of a larger hybrid mesh firewall architecture, provide critical security controls to protect campus networks from malicious exploits. Contact your Fortinet salesperson and ask about how FortiGate NGFW solutions can improve your campus security while lowering your TCO.

Over the past six months, Fortinet has documented 10,666 new ransomware variants, compared to just 5,400 in the previous six-month period. That's nearly 2x growth in variants in just half a year. [6]

[1] Gartner®, Top 10 Trends in Enterprise Communication Services for 2023, Pablo Arriandiaga, Lisa Unden-Farboud, Gaspar Valdivia, Ajit Patankar, Daniel O'Connell, Gregor Petri, Kameron Chao, Jon Dressel, Megan Fernandez, To Chee Eng, Gartner, March 28, 2023.

[2] Verizon 2023 Data Breach Investigations Report, Verizon, 2023.

[3] Brace Yourself for a Tidal Wave of ChatGPT Email Scams, Wired Magazine, April 4, 2023.

[4] Email Statistics Report, 2022-2026, The Radicati Group, Inc., 2022.

[5] Steve Zurier, Average cost of a data breach expected to hit $5 million in 2023, SC Magazine, December 12, 2022.

[6] The 2023 Global Ransomware Report, Fortinet, April 20, 2023.

FORTINET®

www.fortinet.com

June 26, 2023 9:36 PM
2213555-0-0-EN