SOLUTION BRIEF

One Network Firewall Designed to Protect an Expanding Attack Surface: The FortiGate Network Firewall

Executive Summary

The widespread adoption of new digital innovations has transformed enterprise networks, which have become more hybrid while adding breakthrough capabilities to transform the business. But with the rapid proliferation of the mobile workforce, multiple public and private clouds, and Internet-of-Things (IoT) devices, network attack surfaces have dramatically expanded, with more blind spots obscuring visibility into threats.

This makes extended enterprises more difficult to secure, increasing security risks resulting from internally and externally directed attacks. Fortinet FortiGate Network Firewalls (also known as next-generation firewalls [NGFWs]) enable security-driven networking and provide broad, integrated, and automated protection against emerging and sophisticated threats. FortiGate Network Firewalls serve as an integral part of the Fortinet Security Fabric—an end-to-end security architecture that provides automated threat-intelligence sharing for effective security posture, all managed by the Fortinet Fabric Management Center. FortiGate Network Firewalls also leverages artificial intelligence (AI)-powered capabilities to prevent known and unknown attacks.

FortiGate Network Firewalls

- High-performance threat protection
- Validated security effectiveness
- Protection of mission-critical applications
- Continuous risk assessment via security rating and automation
- Integration with the Fortinet Security Fabric
- Enterprise-class security management

Distributed Networks Present a Larger Target for Attack

Driven by the need to build agile IT architecture, consume resources on-demand to meet business velocity, and realize more efficiencies, enterprises are adopting hybrid IT architecture that involves hosting applications and network resources on-premises, in colocation, and across multiple clouds. This includes widespread adoption of cloud environments, geographically distributed offices, and a greater number and variety of endpoint devices. Nearly 80% of organizations report they are introducing digital innovations faster than their ability to secure them against cyberattacks.[1]

Threat actors are well aware of this vulnerability. They pinpoint the weakest points across this ever-expanding network surface. They use sophisticated strategies (e.g., multivector or polymorphic attacks) and automated processes to penetrate defenses and then steal sensitive information or lock down operations in exchange for ransom.

Trying to keep up, network engineering and operations leaders worry about a lack of full visibility into encrypted data as well as control of a network infrastructure that spans applications, data, users, and many network edges. At many organizations, a vast number of disconnected point security products operating in silos across the network only increases complexity. The average enterprise uses 75 different security solutions, many of which only address a single attack vector or compliance requirement.[2] All of this results in an expensive but less effective security posture.

Driving the Evolution in Network Security

To improve security effectiveness, network engineering and operations leaders need greater compatibility across the different security solutions deployed throughout the entire organization. They need security that can share threat intelligence in real time, a constant high level of reliable network performance, open application programming interfaces (APIs) to coordinate and automate responses, and simplified security management using a single-pane-of-glass approach.

Enterprises need to protect the entire expanding attack surface—from IoT to multiple clouds and from users to data. This includes performing secure sockets layer (SSL)/transport layer security (TLS) inspection to detect malware in encrypted flows.

FortiGate Network Firewalls address all of these needs by taking a more collaborative and integrated approach across the entire IT infrastructure.

Fortinet FortiGate Network Firewall

FortiGate Network Firewalls simplify security complexity and provide visibility into applications, users, and networks. They leverage purpose-built security processing units (SPUs) and threat-intelligence services from FortiGuard Labs to deliver top-rated security and high-performance threat protection (e.g., intrusion prevention [IPS], web filtering, anti-malware, application control) for known attacks. Previously unknown attacks are detected and prevented by Fortinet on-premises and using cloud-based advanced threat protection solutions called FortiSandbox.

As part of the broader Fortinet Security Fabric architecture, FortiGate Network Firewalls leverage automated, policy-based responses to accelerate time to resolution. When a FortiGate Network Firewall detects an event, it communicates with the Security Fabric, which determines what information will be shared across the enterprise. For example, when malware is detected in one part of the organization, the Security Fabric shares threat intelligence with the rest of the enterprise IT infrastructure.

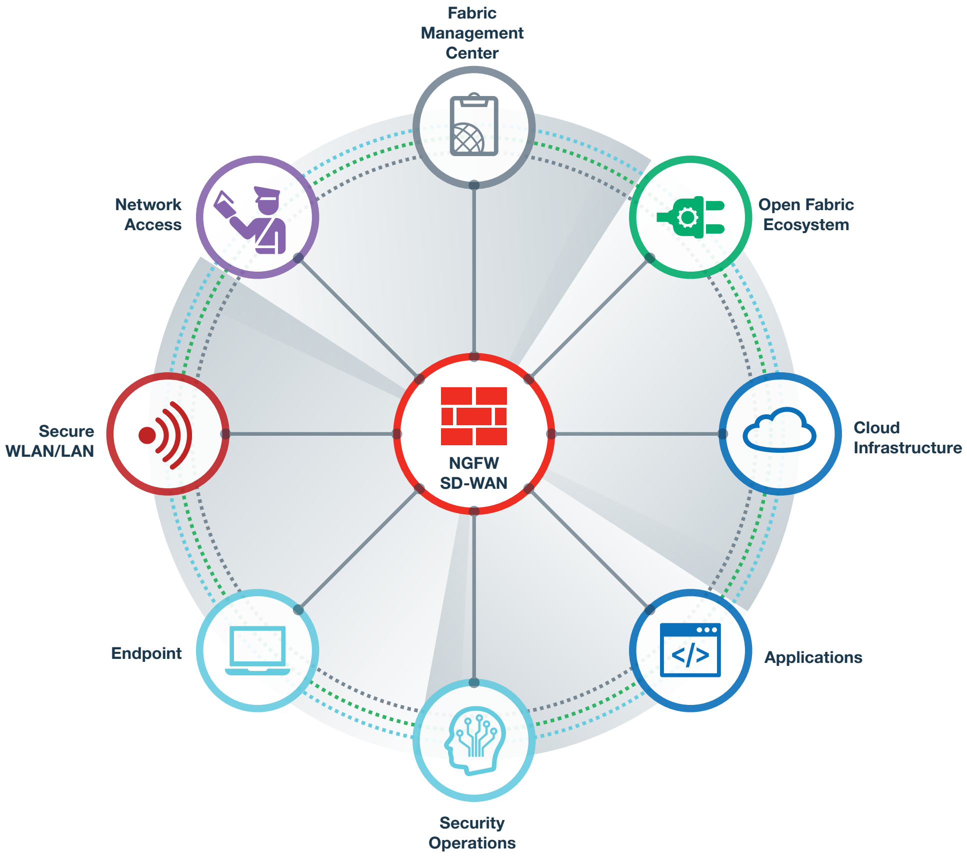


Figure 1: The Fortinet Security Fabric Architecture.

In another instance, when a policy is created for one security solution, the Security Fabric can contextually apply that same policy across other security solutions in the architecture for consistent and coordinated control. For example, when a malicious IP or URL, such as a command-and-control communication, is detected by the FortiEDR endpoint detection and response (EDR) tool running on a user endpoint, the communication is not only blocked at the discovered endpoint but also shared via the Security Fabric to the FortiGate Network Firewall, where the malicious URL is automatically blocked without user intervention for all other users.

FortiGate Network Firewalls enable full visibility into the entire attack surface including all network segments and encrypted network flows. Having full visibility is the key to detect unsanctioned applications and hidden threats, and manage external risks. FortiGate Network Firewalls allow deployment flexibility that can be tailored to the specific security needs of an enterprise that requires either running one or more security features like SSL/TLS inspection (including the latest TLS 1.3 standard), IPS, and antivirus individually or concurrently with minimal performance degradation as verified by third-party entities like NSS Labs.

FortiGate Network Firewalls can also manage internal risks by segmenting, detecting, isolating, and preventing lateral propagation of threats. FortiGate Network Firewalls can also adapt to any type of segmentation including microsegmentation and macrosegmentation and provide advanced Layer 7 security to enable defense in depth.

FortiGate Network Firewalls can also implement privileged access by leveraging identity and access management solutions like FortiAuthenticator and achieve adaptive trust by integrating with EDR systems like FortiEDR.

FortiGate Network Firewalls can also help manage application risks through virtual patching and protecting against vulnerabilities exploits using the high-performance Fortinet Intrusion Prevention System.

Industry-leading Security Effectiveness

Extensive knowledge of the threat landscape combined with the ability to respond quickly at multiple levels is the foundation for providing effective network security. This is why FortiGuard Labs—credited with an unprecedented 885 zero-day threat and vulnerability discoveries[3]—and FortiGuard subscriptions are crucial enablers of Fortinet world-class FortiGate Network Firewall capabilities.

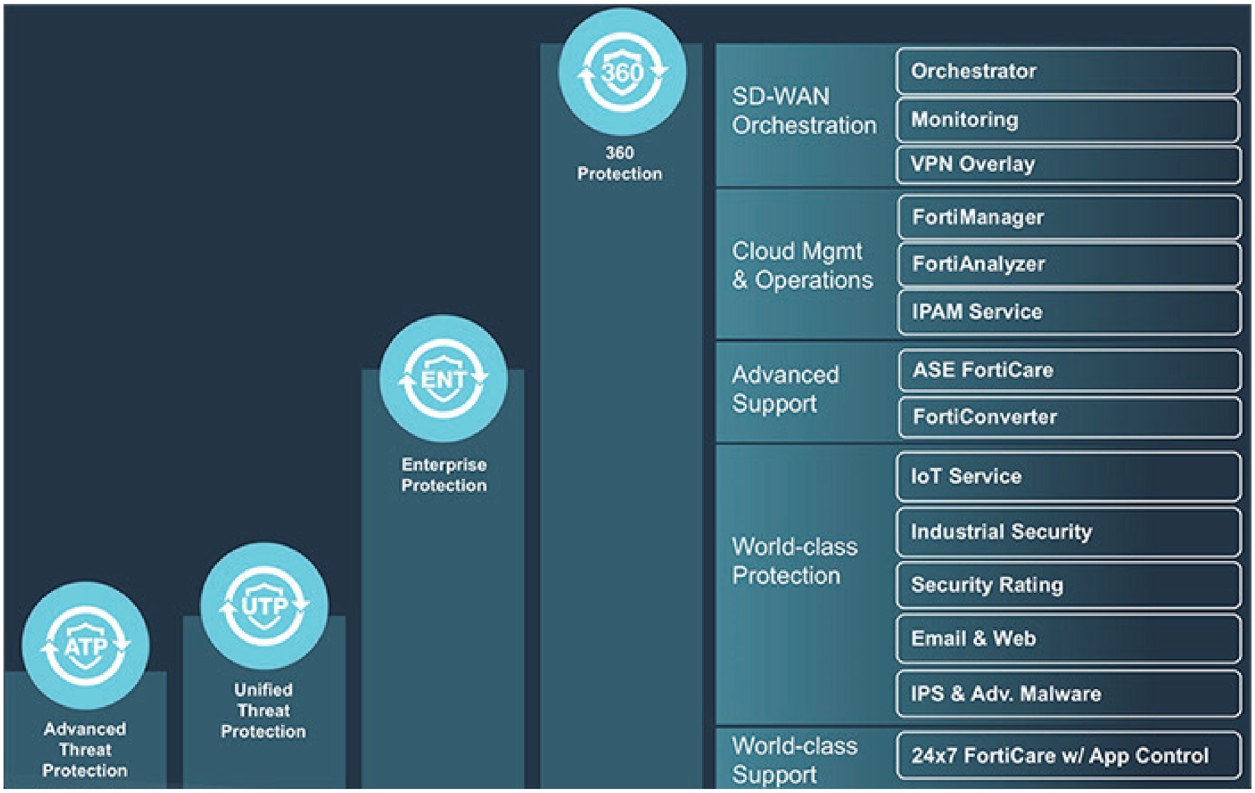


Figure 2: FortiGuard Labs 360 Degrees of Threat Intelligence.

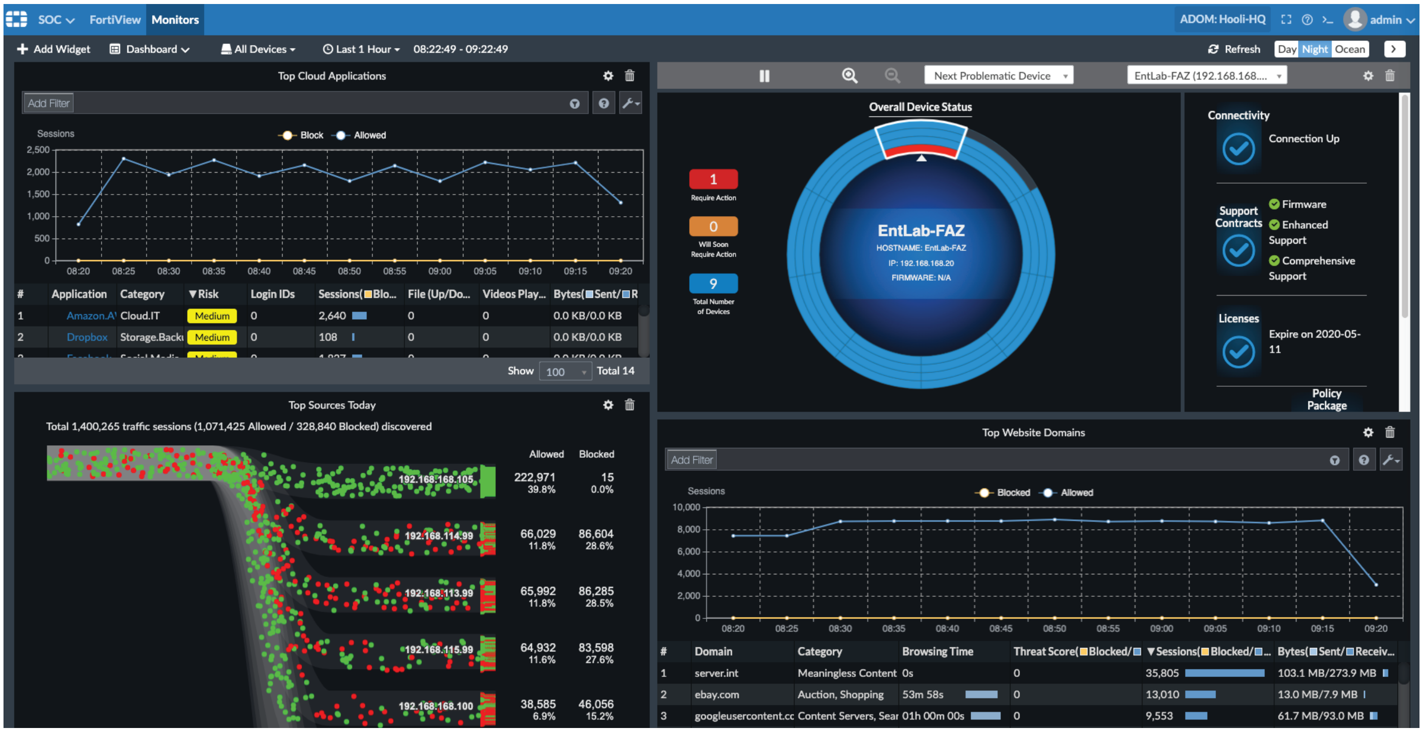
The FortiGuard Labs global threat research team works closely with Fortinet product developers to deliver dynamic security intelligence services. Security updates are instantaneous—automatically and independently validated by third-party research labs. This ensures that the threat intelligence is not only highly accurate but also effective.

One of the primary reasons Fortinet receives consistently high marks in real-world security effectiveness tests, such as those from NSS Labs, Virus Bulletin, and AV-Comparatives,[4] is the combination of in-house research, information from industry sources, and advanced machine-learning capabilities.

FortiGuard services are available as individual subscriptions or conveniently as part of FortiGuard bundles. Our bundles are designed to help customers readily improve their security posture, reduce cyber risk, simplify operations and management, and address challenges with compliance and policy enforcement. To ensure business continuity, all of our bundles include 24x7 FortiCare support services.

Simplify Operations

The unique single-platform approach of the FortiGate Network Firewall, which includes flexible deployment options, delivers end-to-end protection that is easy to buy, deploy, and manage. Centralized security management and visibility consolidates multiple management consoles into a single pane of glass and unlocks automation-driven management. Specifically, a highly intuitive view of applications, users, devices, threats, cloud service usage, and deep inspection gives network engineering and operations leaders a better sense of what is happening on their network. With this strategic view, they can easily create and manage more granular policies designed to optimize security and network resources.



#	Application	Category	▼Risk	Login IDs	Sessions(■Blo...	File (Up/Do...	Videos Play...	Bytes(■Sent/■R
1	Amazon.A\	Cloud.IT	Medium	0	2,640	0	0	0.0 KB/0.0 KB
2	Dropbox	Storage.Backı	Medium	0	108	0	0	0.0 KB/0.0 KB

EntLab-FAZ
HOSTNAME: EntLab-FAZ
IP: 192.168.168.20
FIRMWARE: N/A

Total 1,400,265 traffic sessions (1,071,425 Allowed / 328,840 Blocked) discovered

	Allowed	Blocked
192.168.168.105	222,971 39.8%	15 0.0%
192.168.114.99	66,029 11.8%	86,604 28.6%
192.168.113.99	65,992 11.8%	86,285 28.5%
192.168.115.99	64,932 11.6%	83,598 27.6%
192.168.168.100	38,585 6.9%	46,056 15.2%

#	Domain	Category	Browsing Time	Threat Score(■Blocked/■	▼Sessions(■Blocked/■...	Bytes(■Sent/■Receiv...
1	server.int	Meaningless Content	0s	0	35,805	103.1 MB/273.9 MB
2	ebay.com	Auction, Shopping	53m 58s	0	13,010	13.0 MB/7.9 MB
3	googleusercontent.cc	Content Servers, Sear	01h 00m 00s	0	9,553	61.7 MB/93.0 MB

Figure 3: FortiManager dashboard view.

One Network Firewall Solution Across the Extended Enterprise

As a foundational part of the Fortinet Security Fabric, FortiGate Network Firewalls deliver protection that keeps pace with the accelerating demands of high-performance enterprise networking. FortiGate Network Firewalls feature a purpose-built security processor technology, which provides extremely high throughput and exceptionally low latency while delivering industry-leading security effectiveness and consolidation.

[1] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, March 6, 2019.

[2] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO Online, March 14, 2016.

[3] "Zero-Day Research | Fixes Available," FortiGuard Labs, accessed July 28, 2020.

[4] "Certifications," Fortinet, accessed July 28, 2020.

www.fortinet.com

July 28, 2020 2:59 PM

Macintosh HD:Users:ckluck:Desktop:Zoom-Pics:Getty:Trucker:Solution Brief_NGFW_Network Leader_Solution Selection Folder:R2:SB-FortiGate-Network-Firewall