SOLUTION BRIEF

Delivering AI-driven Web Security at Scale

Protect Against Unknown Zero-day Threats in Real Time

Executive Summary

For most organizations, web traffic now comprises an increasing volume of their total traffic. This is the result of more applications moving to the cloud, combined with direct user access to the internet rather than backhauling web traffic through the data center. Additionally, much of this traffic now includes sensitive data. Applications and remote users are also accessing information that was traditionally hidden deep in the data center.

At the same time, web-based attacks continue to proliferate. The web continues to be one of the top attack vectors for delivering today's rapidly evolving, sophisticated attacks, including ransomware, phishing, cryptomalware, command-and-control (C2) backdoors, and more. In addition, web-based attacks have become more versatile, leveraging encryption technologies to evade traditional web security techniques and exploit the fact that most legacy firewalls are unable to keep up with the inspection of encrypted traffic without impacting user experience. Complicating things further, most of the content being consumed today is video, which few firewalls can inspect or secure.

As a result, organizations struggle to enforce acceptable use policies for anything beyond traditional web content. In addition to scalability and performance issues, point security products lack integration with the larger security architecture. This makes it challenging to deliver a consistent and coordinated web security posture across the distributed network, including remote workers, mobile endpoints, and the hybrid multi-cloud. Visibility is fragmented, making the ability to detect and respond to threats increasingly difficult, especially as the speed and efficiency of attacks continues to increase.

To address these challenges, organizations are increasing their reliance on a defense-in-depth security strategy augmented with advanced technologies. According to IBM's 2021 Cost of a Data Breach Report[1], the adoption of artificial intelligence (AI), security analytics, and encryption are now the top three mitigating factors shown to reduce the cost of a breach. Leveraging such tools saves companies more than $1.25 million per breach. An AI-driven approach is especially effective at mitigating the rise in web-based attacks. Among other things, such as rapid detection and response to threats, an AI-based system helps extend a secure web access strategy across the attack kill chain, ensuring a consistent web security posture across the entire attack surface, from endpoints to networks to the cloud.

1. 90% of hacking vectors in breaches use web applications.[2]
2. 35% of attacks involve phishing, making it a leading cause of breaches.[3]
3. 287 days is the average time to detect and contain a data breach in 2021.[4]
4. $4.24 million is the average cost of a data breach in 2021.[5]

Fortinet was recognized as the most innovative solution in Frost Radar: Global Web Security Market 2020.[6]

Key Benefits

- Real-time protection against zero-day unknown threats
- Enforce acceptable use policies and regulatory compliance
- Granular control of web traffic, including advanced video content
- Protects against malicious file downloads and malicious content hosted on websites
- Protects against sophisticated DNS-based threats
- Reduces mean time to detection (MTTD) through deep content analysis
- Protects against web-borne threats in encrypted traffic with deep secure sockets layer (SSL) inspection
- Consistent web security across the network, endpoints, and cloud

The FortiGuard Web Security Service offers a unique combination of market-leading, AI-driven security capabilities designed to enable full spectrum protection against known and unknown zero-day threats at scale. Driven by a defense-in-depth approach, it employs multiple layers of defense to protect targeted systems, including anti-botnet, content disarm and reconstruction (CDR), web application security, Domain Name System (DNS) filtering, and more, enabling a strong web security posture across networks, endpoints, and the cloud.

This web security service can be leveraged in a wide range of deployment options, including Forward Proxy, Explicit Proxy, Transparent Proxy with WCCP/PBR, and inline. And its web security policies support a variety of authentication modes, including RADIUS, SAML, LDAP, NTLM, Kerberos, and FortiToken, to enable policies based on username or user groups.

AI Analysis at Scale: The Race Against Time

For critical security operations, from threat detection to investigation to remediation, speed matters. Because web-based attacks can compromise a device in seconds, one of the most critical metrics to manage is mean time to detection (MTTD). With AI-driven web filtering, the time from visibility to prevention of sophisticated web-borne threats is reduced to near zero. At the heart of this enhanced web filtering technology are AI models trained to identify indications of malicious domains and URLs, while eliminating noise at scale.

AI and analytics systems are only as good as the inputs and training that go into them. Fortinet's web-focused AI behavioral analysis is based on one of the largest and most diverse datasets in the industry, spanning millions of deployments of Fortinet Security Fabric across the globe. As a result, we are able to deliver credible security analysis results based on a unified dataset to rapidly detect and block both known and unknown threats.

Comprehensive training. The FortiGuard Web Security Service is powered by a true AI system designed by Fortinet's team of data scientists. It has undergone all three stages of AI training: supervised, unsupervised, and reinforcement learning

Expansive data. In addition to an advanced training cycle, the datasets used in AI training are just as critical. The FortiGuard Web Security Service AI is trained on one of the largest and most diverse datasets in the industry, with intelligence gathered from millions of endpoints, networks, and cloud environments.

Intelligence at scale. An AI system also needs to be regularly updated with current data. FortiGuard Labs ingests and analyzes more than 100 billion events every day to deliver over a billion daily security updates across the Fortinet Security Fabric and extended ecosystem.

Key Capabilities

AI-driven web filtering

FortiGuard's cloud-delivered, AI-driven web filtering service provides comprehensive threat protection to address a wide variety of threats, including ransomware, credential theft, phishing, and other web-borne attacks. It leverages AI-driven behavioral analysis and threat correlation to block unknown malicious URLs almost immediately, with near-zero false negatives.

The web filtering service leverages threat intelligence produced by FortiGuard Labs, based on telemetry gathered from over 10 billion real-world events per day. The FortiGuard Web Filtering service also leverages a database of hundreds of millions of URLs classified into 90+ categories to enhance granular web controls and reporting. And with TLS 1.3 support, this analysis extends to encrypted traffic to meet compliance and acceptable usage requirements. It also offers the ability to add exclusion categories, so websites like finance, banking, healthcare, and similar sites containing sensitive information are not monitored, thereby avoiding compliance and regulation challenges. All web filtering capabilities can be defined based on simple URL, Regular Expression, or even wildcard parameters, and the final action can be set to Exempt, Block, Allow, or Monitor.

SafeSearch

The FortiGuard Web Filtering service also supports SafeSearch across all major search sites, a key requirement for the education sector. This prevents explicit websites and images from appearing in search results. When enabled, it automatically rewrites URL searches to include the code used to enable the SafeSearch feature.

Video filtering

The service has now been expanded to offer the industry's first advanced video filtering service. It provides the same level of granular filtering for YouTube as it does for other web traffic, including granular controls based on channels beyond categories. This ability to apply granular video filtering controls helps organizations achieve stronger regulatory compliance.

DNS filtering

Protect against sophisticated DNS-based threats, including DNS tunneling, C2 server identification, and domain generation algorithms (DGAs). DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, including malicious newly registered domains (NRDs), parked domains, and more.

Content disarm and reconstruction service

With the addition of the content disarm and reconstruction (CDR) service, organizations can reduce MTTD with low-latency content sanitization. A broad range of file types are supported beyond traditional signature-based and reputation-based measures.

IP reputation service

With the addition of the IP reputation service, organizations can proactively block attacks with near real-time threat intelligence. Malicious source IP data is aggregated from global threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources. Its geo IP capability delivers additional protection to this category by providing location information on IP traffic to help manage region-based threats.

Anti-botnet service

The additional anti-botnet service enables organizations to block unauthorized attempts to communicate with compromised remote servers, whether for receiving malicious commands or extracting information. This prevents botnets and other threats from communicating with C2 servers to exfiltrate data or download malware.

Web application firewall (WAF)

FortiWeb, the Fortinet web application firewall, has been optimized to protect your business-critical web applications from attacks that target known and unknown vulnerabilities.

Web security services—Delivery method

Subscription service	Type of Service
AI-driven web filtering	Cloud-based query
Video filtering	Cloud-based query
URL certificate blacklist	Fingerprint-based certificate list
DNS service	Cloud-based hosted service
Content disarm and reconstruct	Feature
Botnet IP and domains	IP, domain list

FortiGuard Web Security Advantage

Consistent security everywhere: Cloud-enabled security detection and response across the attack surface and cycle, with complete protection for web-borne threats and native integration across the Fortinet Security Fabric.

AI analysis at scale: AI-driven detection, analysis, and enforcement for real-time protection against unknown threats, powered by one of the largest and most diverse datasets in the industry. This data spans intelligence gathered from endpoints, networks, and cloud environments and is then analyzed by one of the most experienced security research organizations in the industry, FortiGuard Labs.

Defense-in-depth web protection: Provides full spectrum protection against unknown and newly discovered web-borne threats using its advanced malware protection.

		WEB SECURITY					
		IP rep	Web & video filtering	Botnet DP	Geo IP	DNS	Web application
Network Security	FortiGate	●	●	●	●	●	
	FortiProxy		●			●	
Endpoint Security	FortiClient		●	●	●	●	
Cloud Security	FortiWeb	●		●	●		●
	FortiCASB			●			
	FortiADC	●	●	●		●	●
	FortiMail						
	FortiDDoS	●					
Security Operation	FortiSandbox	●	●			●	●
	FortiAnalyzer						
	FortiSIEM						

[1] "IBM Report: Cost of a Data Breach Hits Record High During Pandemic," IBM, July 28, 2021.

[2] "2021 Data Breach Investigations Report," Verizon, May 2021.

[3] Ibid.

[4] "IBM Report: Cost of a Data Breach Hits Record High During Pandemic," IBM, July 28, 2021.

[5] Ibid.

[6] "FROST RADAR™: Global Web Security Market, 2020," Frost & Sullivan, June 4, 2020.

FORTINET®

www.fortinet.com

August 14, 2021 5:11 AM
1213001-0-0-EN