FORTINET
Google Cloud
Securing Your Google Cloud Environment with Fortinet

Table of Contents

Understanding the Security Challenges of Cloud Adoption 3

Improve Perimeter Protection without Sacrificing Agility 4

Close the Gap Between Web Apps and API Security 6

Observe Endpoint Behavior for Whole-Environment Protection 8

Weave Security Across Your Organization with Fortinet Security Fabric for Google Cloud 10

Modernize Enterprise Security with Fortinet for Google Cloud 12

Understanding the Security Challenges of Cloud Adoption

For businesses, moving to the cloud comes with a long list of advantages, from the ability to generate new revenue streams to accelerated time to market. But it also presents some unique security considerations. For one, as an organization grows, so does its attack surface.

Organizations are struggling to secure their cloud environments as new threats emerge faster than ever. In the Fortinet 2024 Cloud Security Report, 96 percent of organizations report being moderately or extremely concerned about cloud security.[1] Their challenges include:

- **Multicloud adoption barriers:** More than half of respondents (59 percent) say that security and compliance concerns impede their ability to rapidly adopt multicloud strategies. Technical challenges (52 percent) and resource constraints (49 percent) are creating substantial roadblocks to achieving visibility and policy control within complex multicloud infrastructures.[2]

- **Persisting talent shortages:** Companies still face a critical shortage of cybersecurity expertise. Most respondents (93 percent) are concerned about finding qualified professionals to protect their increasingly complex multicloud environments.[3]

- **Unified cloud security preferences:** More respondents (95 percent) want a single platform to streamline their security across cloud environments and simplify and automate security management. But, they lack the expertise to implement it.[4]

Google Knows the Cloud. Fortinet Knows Security.
Google Cloud powers more than 60 percent of funded GenAI startups, nearly 90 percent of GenAI unicorns, and almost 60 percent of the world's 1,000 largest companies.[5] To help Google Cloud customers bring additional security to their cloud environments, Fortinet built a partnership with Google to deliver seamless, scalable security solutions.

As 2023 and 2024 Google Cloud Technology Partner of the Year award winners and a Google Cloud Premier Partner, Fortinet offers integrated solutions built on an extensive understanding of the Google Cloud environment, addressing the most pressing security challenges of any Google Cloud setup.[6,7] Fortinet's close alignment with Google Cloud—a Fortinet Security Fabric Partner—also helps organizations address their compliance and regulatory needs.

This eBook explains how to secure any variation of a Google Cloud environment with Fortinet products, from securing a move to the cloud to continuous data protection at scale. It also demonstrates the consistent advantages of implementing a deeply integrated suite of products.

Improve Perimeter Protection without Sacrificing Agility

When organizations begin their journey to the cloud, migrating applications and deploying VPNs, ensuring comprehensive security is crucial to both the businesses and the customers they serve. Without a holistic solution that covers all of an organization's assets, customer and partner trust is hard to maintain. Despite knowing this, businesses fear that adding additional layers of security will bottleneck the pace of innovation.

With modern firewalls that natively integrate with Google Cloud—as well as simplify and improve connections across distributed sites, workloads, and applications—organizations can bolster protection while maintaining the speed of operations.

Firewalls as a Foundational Line of Defense

FortiGate Next-Generation Firewall (NGFW) offers multi-layered security for Google Cloud, Anthos, hybrid, and multi-cloud environments. As a result, it can protect organizations from any threats targeting networks across cloud, on-premises, and data center environments.[8] Because FortiGate NGFW comes in a hardware, cloud-driven, and virtual machine versions, organizations can integrate it into any IT infrastructure and benefit from consistent policies, centralized visibility, and management across their entire deployment. This increases security effectiveness while lowering security and network operational complexities. As part of its deep integration with Google Cloud, FortiGate users can enhance perimeter security for Google Kubernetes Engine (GKE) clusters directly, or use Google Cloud SDN connectors for specific workloads based on GKE filters.

High-speed, encrypted network connections paired with identity-based segmentation and micro-segmentation to isolate workloads offer superior protection for an organization's data. FortiGate NGFW enables businesses to scale their environments safely while also supporting a secure work-from-anywhere model that maintains full application control and visibility.

FortiGate NGFW Highlights

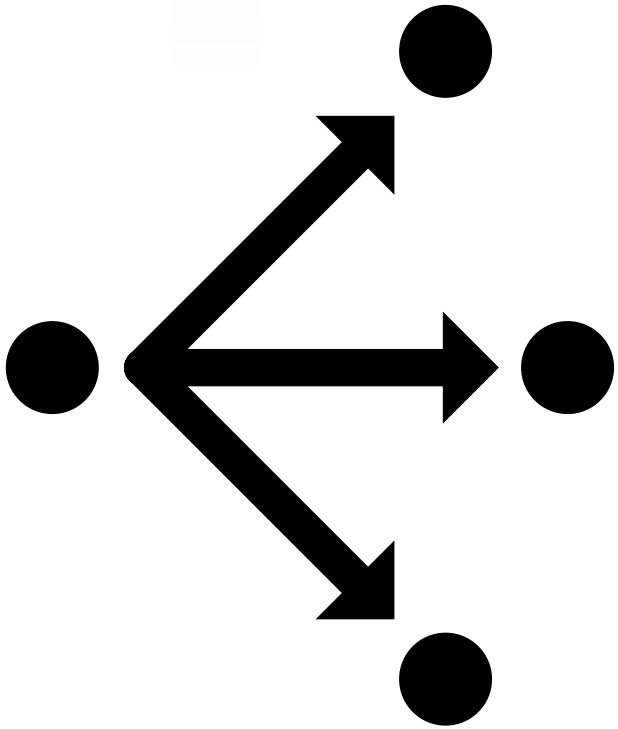
- Defends against advanced attacks, known and unknown, including zero-day
- Mitigates server vulnerability risk and facilitates compliance
- Enables configuration of high-availability environments for automatic failover
- Includes an intrusion protection system (IPS) component that addresses both malware and underlying vulnerabilities

Firewalls as a Foundational Line of Defense

The unique structure of FortiGate NGFW maximizes performance on Google Cloud. From the start of an organization's cloud journey at the Google Cloud landing zone, FortiGate NGFW streamlines the on-ramps orchestration for workloads and applications using SD-WAN integration with Google Cloud's Network Connectivity Center.

When a user has multiple options for connecting to the cloud—from broadband to 5G—Fortinet's SD-WAN solution automatically prioritizes the best route, taking into consideration both the apps to which the user wants to connect and Service Level Agreements (SLAs). This ensures smart routing and optimal performance across an organization.

Fortinet simplifies connectivity across Google Cloud's backbone by integrating with Google Cloud Network Connectivity Center, providing cloud on-ramp orchestration across all on-premises to cloud deployments.



Close the Gap Between Web Apps and API Security

Following the initial shift to the cloud, organizations typically expand their migration and adoption of web applications. Today, organizations heavily rely on their cloud applications to use APIs. Nearly half (44 percent) say that most of their applications use APIs, and over one-third (36 percent) say that all of their applications do.[9] Running web apps in the cloud significantly reduces hardware and software costs. However, the APIs that connect them to one another can open the door to cyberthreats that damage customer trust and disrupt operations. Most organizations (92 percent) reported having one security incident related to insecure APIs in the last 12 months. Over half (57 percent) said they experienced multiple incidents.[10] API calls constituted 71 percent of internet traffic in 2023, with a typical enterprise site averaging 1.5 billion API calls.[11] Cybercriminals increasingly use APIs as a common attack vector because APIs offer a direct route to access sensitive data.

A fundamental challenge for growing organizations is not only the increasing number of web applications they need, but also the volume of API calls those apps need to answer. To a malicious actor, this growth is simply a broader opportunity to infiltrate an organization's infrastructure. Typically, organizations believe that complex security measures slow app deployment. But, security solutions that are built for cloud environments—and leverage advanced technology like machine learning—can facilitate business growth while providing top-tier security.

Secure Your Google Cloud Connectivity with Advanced Capabilities

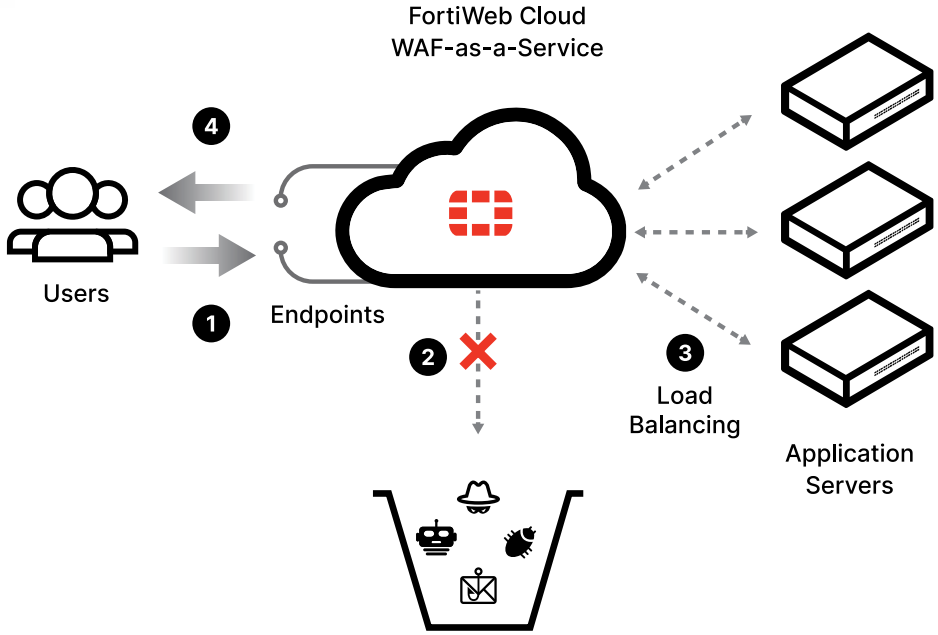
FortiWeb Cloud, a SaaS-based web application firewall (WAF)-as-a-service, secures the web application and API attack surfaces for apps hosted on Google Cloud.[12] This attack surface includes the APIs that many modern web applications rely on. Those APIs may be used to support mobile applications, enable dynamic web applications accessed via a web browser, or even for server-to-server communication. Properly securing this critical attack surface enables organizations to deploy applications to support their essential line-of-business functions.

Most active deployed applications are frequently updated, and organizations relying on more basic protections must manually adjust their security solutions with each update, which can delay the production deployment of your latest code.

FortiWeb Cloud helps your latest code move into production faster by eliminating the need to deploy and manage multiple single-tenant WAF, VM, or container instances, and by leveraging AI/ML to automatically model normal application usage and detect potentially malicious anomalies. This use of AI/ML both improves detection and reduces the false positives that drive administrative overhead. With FortiWeb Cloud, businesses enjoy a consistent security posture for their line of business apps—and customer interactions—with less management and faster value realization.

FortiWeb Cloud Highlights

- Detects and protects against known and unknown vulnerabilities using AI and ML to learn and recognize usual versus unusual behavior
- Leverages ML algorithms for API security to automatically discover endpoints, as well as analyze, and catalog APIs and their schema
- Employs AI to block a range of malicious bot activity using tactics such as bot deception and ML-based mitigation
- Deploys in the same region as an organization's application for low-latency, easier compliance, and lower data transfer rates
- Includes built-in setup for rapid implementation
- Eliminates hardware costs and software maintenance, with capacity planning fully managed by Fortinet



A Note on Apigee

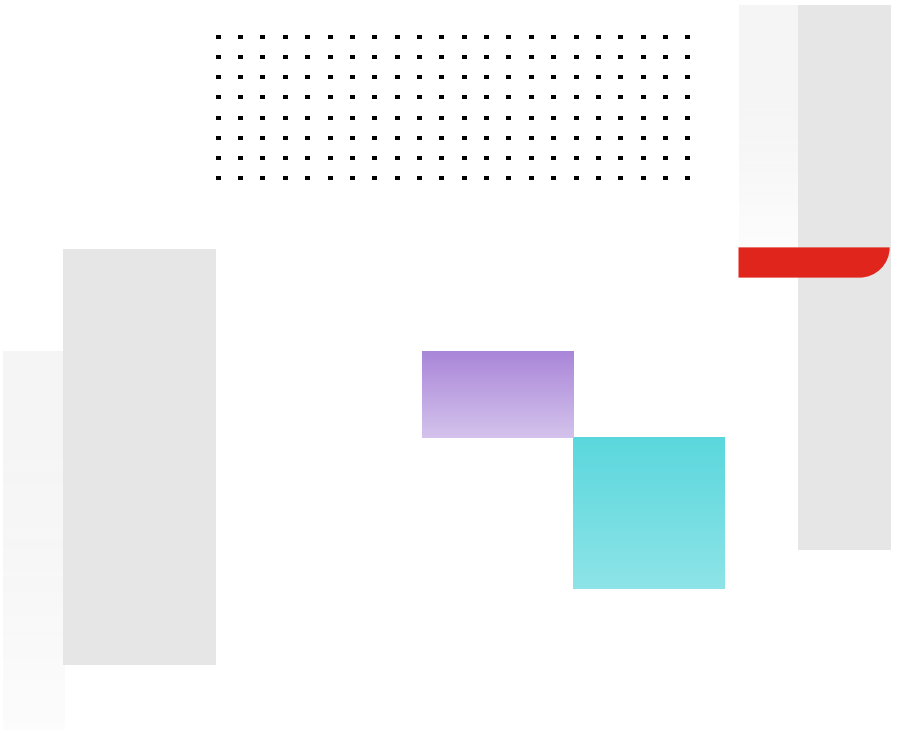
Apigee is Google's market-leading API management platform that organizations use for an app's entire lifecycle. Some of the most data-sensitive industries, such as telecommunications, rely on Apigee to create and configure their API-based operations. Apigee frontends service with a proxy layer that abstracts backend service APIs to provide simplified management of APIs such as analytics, rate limiting, and quotas, along with some security benefits like identity management. However, Apigee does not include any WAF or WAF-like capabilities. As a result, it is important for organizations to deploy a WAF like FortiWeb Cloud alongside Apigee.

Observe Endpoint Behavior for Whole-Environment Protection

Once an organization has shifted to the cloud, migrated apps, implemented an NGFW, and secured APIs, it needs to focus on the security of its endpoints—the destination for almost all attacks. Especially as organizations scale or expand the number of remote workers, true endpoint security can be a challenging feat. Ransomware remains at peak levels as attacks occur more frequently and new variants emerge. Despite 78 percent of organizations feeling prepared for ransomware attacks, 50 percent were still attacked.[13] Maturing Ransomware-as-a-Service operations also enable bad actors to introduce more sophisticated and aggressive variants.

IT teams must have visibility into all the different devices people use to access and transmit data, vet applications, and restrict their communication when vulnerable, as well as constantly monitor system behavior for indications of attack. Without efficient endpoint security, businesses leave the door open for destructive lateral ransomware attacks and other impacts such as data loss. In order to take advantage of the advanced features of an endpoint security solution one has to prepare for extensive setup and management, which is why most offerings require a set up service and offer a managed detection and response (MDR) offering for after set up.

To achieve endpoint security that can contribute to the entire ecosystem, organizations need a solution that can integrate with other security tools to provide a complete picture of their environments and devices, known as endpoint detection and response (EDR). But not all EDR solutions are created equal, and it's important to know what to look for to distinguish claims from ability. Some act as filters that require knowledge of an attack to stop it, creating an opportunity for threats to jump from network to network, and others prioritize detection over response when both are crucial. Others generate more alerts than are necessary and lack automation, forcing security teams to manually triage reported policy violations.



Fast Detection Meets a Multi-Faceted Response

FortiEDR lives on the kernel level of the devices themselves.[14] It can identify what other solutions may not see, including the behavior of unknown or zero-day attacks, even if they're offline. As a result, it offers robust detection of high-value, at-risk activity without burdening security teams.

Deployable directly from Google Cloud Marketplace, FortiEDR uses automation and AI/ML to learn behaviors across endpoints, then investigate and detect policy violations, making it a scalable solution that helps meet regulatory standards. A robust "response" aspect of FortiEDR is not just its ability to quickly react to threats—for example, stopping a malicious file download in its tracks—but to recover, rolling back decisions caused by malware for clean logs.

How do you know it's a comprehensive EDR solution? FortiEDR has been tested by third parties and has consistently demonstrated documented success. In a MITRE ATT&CK evaluation, the company had a 98 percent overall visibility rate and a 95 percent analytic detection rate. It maintained a perfect score in the Linux test. FortiEDR's analytic detention rate in 2023 was 22 percent better than the average of all participating vendors.[15]

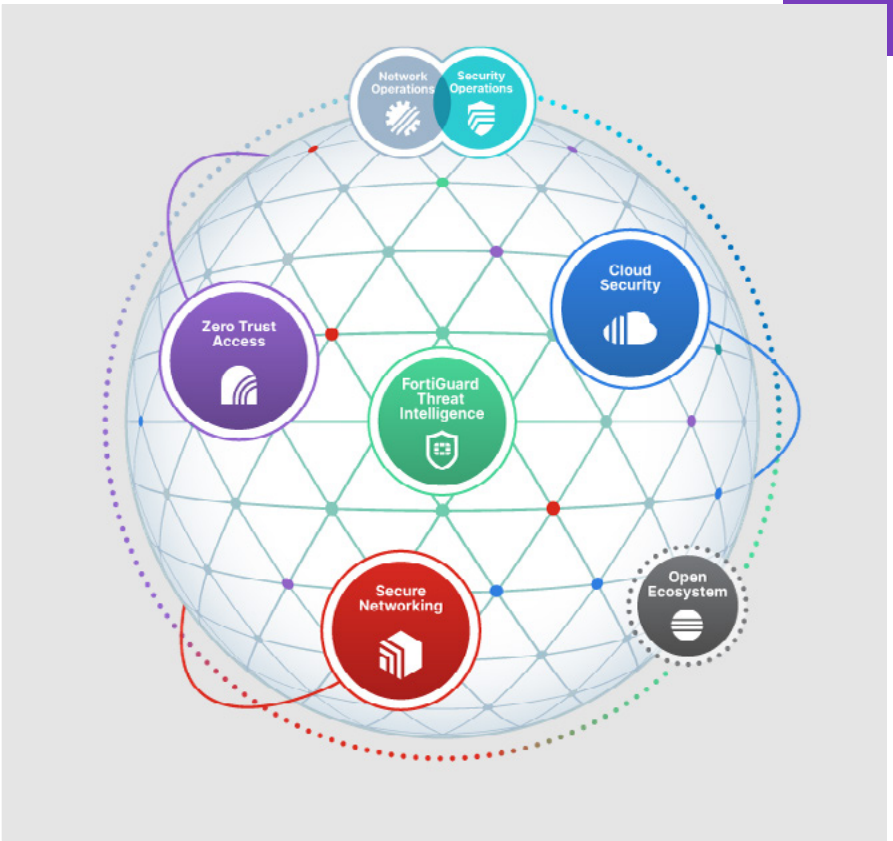
FortiEDR Highlights

- Automated endpoint deployment orchestration for Google Compute Engine
- Real-time workload and endpoint visibility, analysis, protection, and remediation
- Ability to proactively discover devices and detect various breeds of threats, including zero-day, extended to security edge points
- AI/ML helps maintain uptime and deliver a superior user experience
- Pre- and post-infection protection, with memory snapshots for easier analysis and recovery
- Integration with Fortinet products for additional defense capabilities and value
- Integrate FortiEDR with Security Command Center (SCC) to establish an additional data lake for XDR functionality

Weave Security Across Your Organization with Fortinet Security Fabric for Google Cloud

Native integration with an organization's Google Cloud environment is important, but it's equally important that different solutions integrate with each other. This has been the Fortinet philosophy from day one, and the reason all of Fortinet's products are part of the Fortinet Security Fabric.

The Fortinet Security Fabric is a cybersecurity mesh platform that delivers broad, integrated, and automated cybersecurity capabilities, supported by a large, open ecosystem. It empowers organizations to achieve secured digital acceleration outcomes by reducing complexity, streamlining operations, and increasing threat detection and response capabilities. Supported by more than 500 third-party technology partners and growing, the Fortinet Security Fabric gives organizations the flexibility to adopt a wide range of solutions that fit their individual needs now and in the future. Cloud-native integrations with Google Cloud provides encrypted connections, centralized visibility, and policy reinforcement across cloud networks and environments with an intuitive, user-friendly interface.

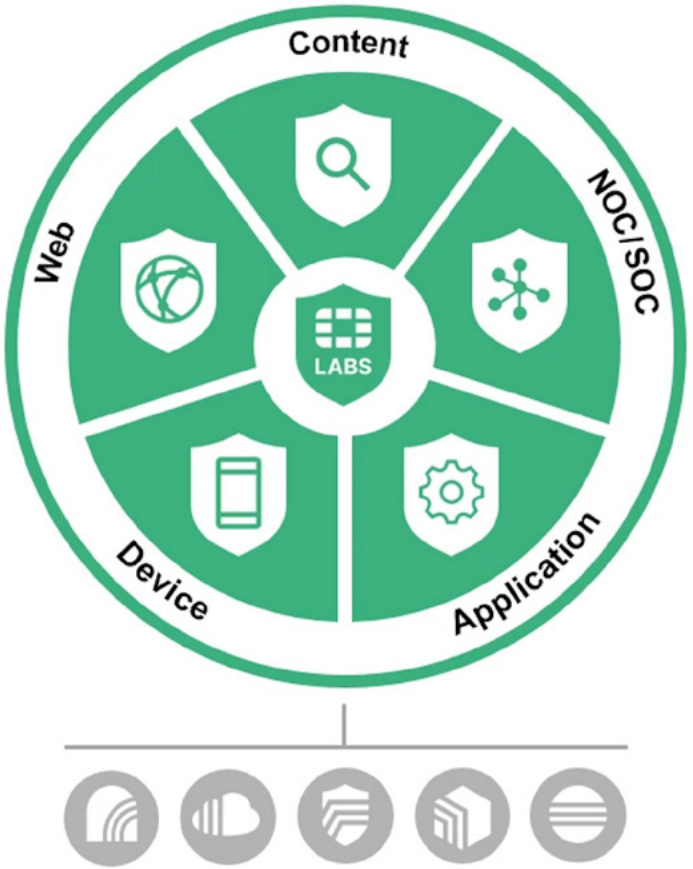


How FortiGuard Labs Keeps Customers Steps Ahead

At the center of Fortinet's Security Fabric is FortiGuard Labs, Fortinet's industry-leading threat intelligence research and response organization. FortiGuard Labs collects and analyzes telemetry on a global level so that organizations can rapidly adjust their security posture. With input from analysts, researchers, and threat hunters examining this aggregated overview of malicious activity across the globe, alongside zero-day threat research conducted by FortiGuard Labs, FortiGuard then pushes intelligence and protection to devices immediately, enabling faster time-to-prevention and response. Since its inception, Fortinet continues to work with global entities such as INTERPOL, FIRST, and MITRE to advance the safety of cloud-based operations.

Fortinet by the Numbers

- **730K+** customers worldwide
- **90+** analyst report inclusions
- **11.8M+** units shipped
- **50+** enterprise security products
- **1,299 patents** globally



Modernize Enterprise Security with Fortinet for Google Cloud

Learn more about how to bring complete, advanced protection to your organization with Fortinet on Google Cloud Marketplace.

All purchases of Fortinet products on Google Cloud Marketplace count toward an organization's spend commitment.

FORTINET | Google Cloud

[1] Frederick Harris, Key Findings from the 2024 Google Cloud Report, Fortinet, April 23, 2024.

[2] Frederick Harris, Key Findings from the 2024 Google Cloud Report, Fortinet, April 23, 2024.

[3] Frederick Harris, Key Findings from the 2024 Google Cloud Report, Fortinet, April 23, 2024.

[4] Frederick Harris, Key Findings from the 2024 Google Cloud Report, Fortinet, April 23, 2024.

[5] Google Cloud customer stories and case studies, Google Cloud, accessed May 17, 2024.

[6] Fortinet Wins Google Cloud Technology Partner of the Year Award for Security – Identity & Endpoint Protection, August 29, 2023.

[7] Fortinet Wins Two Google Cloud Technology Partner of the Year Awards for Security, April 9, 2024.

[8] Protect Your Workloads at Cloud Speed, Fortinet, accessed May 17, 2024.

[9] Linda Tucci, Better API security needed as companies modernize apps, August 25, 2023.

[10] Linda Tucci, Better API security needed as companies modernize apps, August 25, 2023.

[11] The State of API Security in 2024, Imperva, accessed May 17, 2024.

[12] Web Application Firewall, Fortinet, accessed May 17, 2024.

[13] The 2023 Global Ransomware Report, Fortinet, accessed May 17, 2024.

[14] Endpoint Detection and Response, Fortinet, accessed May 17, 2024.

[15] Brook Chelmo, Reveling in the MITRE ATT&CK Evaluations Results, Fortinet, September 20, 2023.

FORTINET

www.fortinet.com

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

May 21, 2024 4:56 PM

123456-0-0-EN