OVERVIEW

FortiGuard Labs
Threat Intelligence and Research at Fortinet
The Need for Threat Intelligence

Digital transformation has unlocked massive potential for organizations. It has also paved the way for a new wave of advanced cybersecurity threats. Cybercriminals are becoming more sophisticated, using tools such as machine learning and AI to take advantage of the expanding attack surface and bypass traditional safeguards. Faced with endless alerts and a flood of data being collected from endpoints, network and IoT devices, cloud environments, and other areas, IT teams are struggling to keep pace, let alone stay ahead of threats.

Security devices today need to be as fast and nimble as the networks they need to protect, and the cybercriminals they need to defend against. Critical to their effectiveness is the need for timely, accurate, and actionable threat intelligence. Constant updates are absolutely essential for security devices to keep pace with the shifting landscape, which means that even the fastest and most adaptable security solutions are only as effective as the threat intelligence infrastructure and researchers that support them. And organizations need skilled support from cybersecurity professionals to help identify security gaps and recover from cyber incidents.

Why FortiGuard Labs

FortiGuard Labs, Fortinet’s global threat intelligence and research team, has brought together some of the brightest and most knowledgeable threat hunters, researchers, analysts, tool developers, and data scientists in the industry, located in research labs around the world. But that’s just the start.

Over the past decade, FortiGuard Labs has also designed, trained, and delivered one of the most advanced artificial intelligence and machine learning platforms in the industry to augment the efforts of the FortiGuard Labs cybersecurity professionals. Combined, their primary mission is to provide Fortinet customers with the industry’s best threat intelligence designed to protect them from malicious cyber-attacks.

What sets the FortiGuard Labs team apart are three key differentiators: their breadth of visibility into the threat landscape, their depth of innovation, and their rapid delivery of actionable threat intelligence to the Fortinet Security Fabric and Fortinet customers.
Visibility into Threats and Across Vectors

You can’t prevent what you can’t see. Threat research teams need broad visibility across the global threat landscape to develop actionable threat intelligence that can protect customers from both active and potential threats. This visibility can answer such critical questions as, What vulnerabilities are being targeted? What threat vectors are being used to launch attacks? Are there zero-day vulnerabilities that could possibly be exploited? What have other threat intelligence organizations seen?

Through the continuous gathering of threat information from the world’s most deployed network security solution, including 5.6M+ sensors deployed worldwide, and an extensive intelligence-sharing partner community, FortiGuard Labs has access to the broadest set of telemetry and threat data resources in the industry.

- **Global visibility across the entire threat spectrum** – Telemetry gathered from Fortinet’s millions of sensors help FortiGuard Labs identify the real-world threats our customers face. These include threats discovered on network, endpoint, and IoT devices, as well as those embedded in emails, applications, and on the web.

- **Zero-Day Vulnerability Research** – FortiGuard Labs has the most successful zero-day detection operation in the industry, having discovered over 850 zero-day vulnerabilities to date, far exceeding any other threat intelligence operation in the industry.

- **Partnerships** – FortiGuard Labs was among the first in the industry to initiate, design, and implement active threat intelligence sharing and collaboration. Today, they receive feeds from over 200 technology, law enforcement, and government organizations for better visibility and analysis.

Innovation

FortiGuard Labs pioneered many of the concepts, processes, and technologies in use today across the threat intelligence industry. Their dedication to innovation has resulted in the creation of the industry’s most advanced AI and ML systems designed to flag threats and automatically create required protections. It has also led to the creation of intelligence-sharing networks, as well as being awarded over 100 patents specifically focused on threat intelligence and research.

Innovation also enables FortiGuard Labs to quickly adapt its operations to new threats and threat vectors in order to address new issues. Here are just a few recent examples:

- **AI Enables Threat Intelligence at Machine Speed** – Developed organically over the last decade, FortiGuard Labs’ state-of-the-art Artificial Neural Network is comprised of billions of interconnected nodes that actively gather, process, and correlate data feeds from a wide variety of sources. By simultaneously processing tens of billions of data points, this advanced AI system can do the work of an entire team of data analysts in seconds. It correlates data to uncover emerging threats and map threat patterns. These are shared with research teams while dynamically delivering actionable threat intelligence to millions of Fortinet customers—all in a fraction of the time required by traditional systems.

- **Fortinet Distribution Network (FDN)** – FortiGuard Labs’ bi-directional network collects telemetry threat data from Fortinet devices (5.6M+ devices deployed globally) for analysis of the real-world threats Fortinet customers face. FDN was also designed to efficiently distribute actionable security protection updates to the Fortinet Security Fabric components deployed in customer networks around the world several times each day.

- **Federated Machine Learning** – The next generation AI developed by FortiGuard Labs has improved machine learning processes and threat pattern recognition. By moving from a centralized analysis server to a distributed model, threat patterns can be detected by distributed learning nodes across an environment, enabling a faster local response. This data is then centrally distributed across all learning nodes to improve threat detection efficiency and accuracy across the entire security fabric.
**Actionable Threat Intelligence**

The purpose of any threat intelligence effort is to provide the information necessary to make informed decisions and take appropriate action. FortiGuard Labs provides actionable threat intelligence in a number of areas, including:

- **Security Protection Updates** - FortiGuard Labs provides security updates to the entire portfolio of Fortinet Security Fabric products, with the latest threat identification and protection information being updated multiple times a day. (See box 1, below)

- **Proactive Threat Research** – FortiGuard Labs publishes multiple research vehicles to help organizations proactively understand the threats they face and better prepare their defenses. This includes threat research blogs, threat intelligence briefs, and security alerts. (See box 2, below)

- **Threat Intelligence Services** – Organizations that are looking for specialized consulting help can take advantage of a variety of subscriptions, including penetration testing, malware analysis, phishing issues, and incident response services. (See box 3, below)

**FortiGuard Labs and the Fortinet Security Fabric**

Fortinet’s market-leading defense strategy starts with the Fortinet Security Fabric. It is designed to address the dynamic security challenges faced by those organizations adopting digital innovation initiatives – including today’s expanded digital attack surface, advanced threats, and increased infrastructure complexity – combined with growing performance and scalability requirements.

FortiGuard Labs provides the threat intelligence foundation for all Fortinet Security Fabric components, keeping them up-to-date with the latest threat identification and protection information available.

---

**Information Sharing Leadership**

- Co-founded the Cyber Threat Alliance (CTA) in 2014
- Member of the computer incident response organization FIRST since 2012.
- Contributor to the development of STIX/TAXII protocols, as well as the MISP platform.
- Receives and processes over 200 individual sources of threat intelligence from partners
FortiGuard Labs Threat Research

FortiGuard Labs researchers, located at eight research labs around the world, produce more than 609,000 hours of research annually. The resulting threat research publications are designed to help customers and subscribers better understand and take action against the threats that affect them:

- **Threat Playbooks** – Threat playbooks have become an essential weapon in the arsenal of today’s cybersecurity professionals. Threat actors often follow specific protocols and practices to manage all the moving parts of an attack or malware development. FortiGuard’s playbooks capture these attack patterns – including the complete collection of tools, techniques, and procedures these adversaries use to achieve their goals – to enable organizations to create effective defensive strategies.

- **Threat Intelligence Briefs** – FortiGuard Labs threat researchers, supported by automated systems, monitor malicious activity occurring across the internet every day. Their observations are chronicled in the weekly FortiGuard Threat Intelligence Brief, providing organizations with an actionable snapshot of the current threat landscape across application vulnerabilities, malware and botnets, and malicious web activity.

- **Threat Signals** – FortiGuard Labs’ Threat Signals reports are an early warning system for out-of-policy activity before it becomes an incident. These Threat Signals reports provide concise technical details about emerging cybersecurity issues, combined with insightful analysis and mitigation recommendations.

- **Threat Blogs** – FortiGuard Labs’ threat researchers regularly publish in-depth research on important threat intelligence subjects, such as new malware and variants, zero-day exploits, targeted systems, and critical vulnerabilities being exploited in the wild.

FortiGuard Labs Custom Services

**Threat Intelligence Services**

As organizations mature their security operations, they sometimes require outside consulting services to address specific areas of their security programs. FortiGuard Labs provides a number of threat intelligence services to help organizations identify critical issues and work toward improving their security. These include:

- **FortiPhish – Phishing Simulation Service**

  This cloud-based service evaluates how individuals within an organization respond when tested with different phishing scenarios. Management reporting enables IT teams to evaluate the test results and visualize improvement over time.

---

Security Efficacy

FortiGuard Labs independently validates the effectiveness of the threat intelligence it provides to the individual components of the Fortinet Security Fabric. It does this through sustained year-over-year certifications process and rigorous testing by leading organizations, including:

- NSS Labs
- ICSA Labs
- Common Criteria
- Virus Bulletin
- Virus Bulletin Spam
- Mitre
- Oasis
- NASA

This commitment to testing and validation makes the Fortinet Security Fabric the most certified and proven security solution available in the industry. See how well we’ve done in providing threat intelligence and protection to the individual components of the Fortinet Security Fabric [here](#).
FortiGuard Labs Overview

- **FortiPen – Penetration Testing**
  Technical assessment of the security controls of an organization can identify weaknesses on computer hardware infrastructure and software applications. The FortiGuard Labs team uses commercial automated tools to discover unintended services made publicly available by your network. It also employs real-world attacker methodologies to discover unknown vulnerabilities on a given target.

- **FortiGuard Responder – Incident Response Service**
  This service assists clients with the analysis, response, containment, and remediation of security incidents impacting their organizations. By identifying all impacted resources and analyzing attack and malware methodologies, organizations can not only get back up and running quickly, but also close all threat vectors so they can remain safe.

**Commitment to Global Partnerships**
To amplify their commitment to partnerships, Fortinet also co-founded the Cyber Threat Alliance (CTA). Today, the 28-member CTA organization actively brings threat researchers and security vendors together to share threat information to improve defenses across member organizations and their customers against advanced cyber adversaries.

Fortinet is also a founding member of the WEF Centre for Cybersecurity, holding one of only two permanent seats on this international council. The Centre for Cybersecurity was designed to shape the future of cybersecurity and digital trust around the world, to safeguard innovation, to protect institutions, businesses, and individuals, and to secure our growing reliance on the digital economy.

Today, Fortinet is actively engaged with, and receives threat intelligence feeds from more than 200 partners. These partnerships are key to providing increased visibility to FortiGuard Labs operations and include threat intelligence peers, national CERT/CSIRT teams, government agencies, international law enforcement organizations including NATO and Interpol, and critical partners such as KISA, OASIS and MITRE.

Next Steps
Want to find out more about FortiGuard Labs? Visit our web page here. Sign up for our weekly Threat Intelligence Brief here. And for existing Fortinet customers, make sure to join our “threat intelligence community” here.

---

Project Knightrider
Shortly after joining INTERPOL ICGEG, FortiGuard Labs briefed the Cyber Fusion Center (in Singapore) on threat activity discovered by our threat hunters. INTERPOL then asked for our assistance in further investigating this activity. FortiGuard Labs researchers identified the criminal activity and the perpetrators, leading to the dismantling of an international cybercriminal organization and the arrest of multiple participants, including the ringleader. This crime ring included over 40 co-conspirators based in Nigeria, Malaysia, and South Africa. They were responsible for a wave of online scams that stole more than $60 million over three months from businesses and individuals across the globe, combined with money laundering activities in China, Europe, and the U.S.

---

Copyright © 2020 Fortinet, Inc. All rights reserved. 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. 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.