REPORT

Cyberthreat Predictions for 2025

An Annual Perspective from FortiGuard Labs

FORTINET

Table of Contents

Cyberthreat Predictions for 2025: An Annual Perspective from FortiGuard Labs

While threat actors continue to rely on many "classic" tactics that have existed for decades, our threat predictions for the coming year primarily focus on cybercriminals embracing bigger, bolder, and—from their perspectives—better attacks. This year's threat predictions report examines how long-term cyberattack trends evolve, shares emerging threats to watch for in 2025, and more. Here's a look at how we expect the threat landscape to change in the coming year and beyond and how these shifts will impact organizations and their security teams.

The Evolution of Old Favorites

We've discussed numerous attack trends for years, including those we highlighted in our previous threat prediction reports. We note how we expect these fan-favorite cybercrime approaches to evolve in the months and years ahead. In the past 12 months, we've witnessed advanced persistent threat (APT) groups adopting new tactics, techniques, and procedures (TTPs), adversaries using AI to increase the volume and velocity of attacks, and larger-scale, more destructive ransomware deployments, to name a few. Below is a look back at some key 2024 predictions we made and our thoughts on how these longstanding trends will evolve in 2025.

Advanced Persistent Cybercrime Accelerates

It's no secret that APT groups are highly adaptable. For instance, the infamous Stuxnet attack in 2010 marked a turning point in the sophistication of cyber warfare, where state-sponsored APTs demonstrated their ability to disrupt physical infrastructure. Later, APT28 (Fancy Bear), associated with Russian intelligence, exemplified how APT groups could target political entities, such as in the high-profile breach of the Democratic National Committee in 2016. These instances show how APTs constantly change their methods, leverage new vulnerabilities, and stay active despite evolving security defenses. Additionally, we continue to observe that about a third of the APT groups identified by MITRE are active. Based on intelligence from FortiRecon, we saw 38 of the 143 identified APT groups (27%) being active during the second half of 2023, including Lazarus Group, Kimusky, APT28, APT29, Andariel, and OilRig.[1]

Last year, we predicted a trend in which some APT groups would employ even more stealthy, innovative methods to initiate attacks, and this prediction came to fruition. As APT groups continue deepening their collaborations with cybercriminals, it's no surprise that APTs are adopting new TTPs at a record pace. For instance, this summer, we observed the GrimResource technique combined with Remote AppDomain Injection, enabling threat actors to inject malicious code into isolated application domains, making detection significantly harder for traditional endpoint security tools. Groups like APT29 and APT41 also push the envelope with unique payloads tailored to each campaign. APT29, for example, has been deploying advanced memory-resident malware to avoid leaving traces on disk. At the same time, APT41, known for its dual focus on espionage and financial gain, continuously adjusts payloads to bypass detection methods specific to each targeted organization. These adaptive techniques illustrate how APT groups remain agile and innovative, posing an ongoing challenge for cybersecurity defenders worldwide.

Attackers Add New TTPs to Their Toolboxes

For years, threat actors relied on a relatively small collection of TTPs that proved successful, using these frameworks to execute their attacks. In last year's threat predictions report, we anticipated that attackers would continue to expand the TTPs they use to compromise their targets, particularly with the rise of AI and other new technologies to aid their efforts. As predicted, we witnessed the TTP playing field expand, with attackers continuously pushing new procedural-level implementation of techniques and creating new ones.

We're also observing attackers quickly deploying new ways to counter the safeguards many organizations have implemented for specific techniques. To counter the constantly evolving methods used by threat actors to bypass standard defenses, security professionals should:

Embrace proactive threat hunting

Rather than waiting for alerts, defenders should conduct proactive threat hunting to identify signs of potential compromise that automated systems may miss. This approach involves leveraging advanced data analytics, behavioral analysis, and hypothesis testing.

Layer their security posture

Implement a defense-in-depth strategy that layers multiple security mechanisms (such as network monitoring, endpoint security, and anomaly detection) so that if one defense is bypassed, others can act as a safety net. Ideally, these solutions should be integrated into a single platform to share layered checks between security and networking systems seamlessly.

Adopt zero-trust principles

Continuously verify users' and devices' identity and trust level, even within the network perimeter. Zero-trust models minimize the damage attackers can inflict if they gain access to the network.

Integrate threat intelligence

Use up-to-date threat intelligence to stay informed about emerging TTPs and keep playbooks current. This helps defenders anticipate new tactics and adapt existing safeguards accordingly.

Conduct routine red team exercises

Regular red and blue team simulations can reveal weaknesses in an organization's defenses and provide actionable insights into potential bypass strategies attackers might use.

This adaptive, multi-layered approach, underpinned by continuous learning and the adoption of emerging security technologies, helps organizations stay resilient as the threat landscape evolves.

Artificial Intelligence Offers an "Easy" Button for Cybercriminals

Cybercriminals continue to weaponize AI and use it for nefarious purposes. Malicious actors are increasingly harnessing AI to increase the volume and velocity of attacks they deploy. From gathering data more efficiently to using large language models (LLMs) to craft phishing communications that are more realistic than ever, experienced and novice threat actors are relying on AI as an "easy" button to streamline their efforts.

Last year, we predicted attackers would leverage AI in various ways, from conducting generative profiling to powering up password spraying. Here are some examples of how attackers are utilizing AI in their operations:

Automated Phishing Campaigns

- **Example:** Attackers use LLMs to create highly convincing phishing emails with perfect grammar and context-aware personalization. These AI-generated emails can mimic the writing style of known contacts, making them difficult to distinguish from legitimate communications.
- **Impact:** This tactic increases the success rate of spear phishing campaigns, enabling attackers to bypass typical red flags that alert users to fraudulent emails.

Generative Profiling for Social Engineering

- **Example:** LLMs help attackers build detailed social engineering profiles by analyzing social media posts, public data, and other online content. By synthesizing this data, attackers can tailor their communications to match the victim's interests, work relationships, and even recent activities.
- **Impact:** The precision of these AI-enhanced profiles increases the likelihood that targets will trust and engage with malicious actors, leading to higher rates of credential theft or unauthorized data access.

AI-Powered Password Spraying

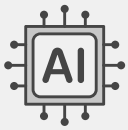
- **Example:** AI can be used to analyze patterns in commonly used passwords and guess variations more efficiently. LLMs trained on large datasets of leaked credentials can generate realistic password lists that are more tailored to the user base of a targeted organization.
- **Impact:** These AI-refined password attacks bypass traditional rate-limiting and lockout mechanisms by spreading attempts across multiple accounts and fine-tuning the approach to minimize detection.

Deepfake-Assisted Voice Phishing (Vishing)

- **Example:** Attackers have employed deep learning models to create synthetic voices that mimic specific individuals' tone and speech patterns. For instance, threat actors may impersonate a company executive to convince an employee to perform unauthorized financial transactions or share sensitive information.
- **Impact:** Deepfake voice technology's realism makes it difficult for employees to recognize fraudulent requests, which can cause significant financial and reputation damage.

Enhanced Malware Creation

- **Example:** LLMs can help generate polymorphic malware that changes its code structure to evade signature-based detection. Attackers can also use these models to write new code snippets or refine existing malware to be more efficient and less detectable.
- **Impact:** This accelerates the development of advanced malware variants and reduces the technical barrier for less skilled attackers, increasing the overall volume of malware in circulation.



AI-Generated Misinformation Campaigns

- **Example:** Threat actors leverage LLMs to create and disseminate misinformation at scale. This includes generating fake news articles, social media posts, and comments to sway public opinion or create panic during critical events like elections and health crises.
- **Impact:** Misinformation campaigns can damage reputations, erode trust in institutions, and create social unrest. The ability to automate content creation allows attackers to flood information channels, overwhelming fact-checkers and response teams.

As adversaries become more comfortable using AI to enhance their efforts, we expect to see adoption accelerate. Cybercrime groups will use AI to aid in even more activities, such as identifying new vulnerabilities in software code that they can exploit.

Adversaries Level Up Their Ransomware Attacks

Ransomware continues to be a severe threat to most organizations. Given the growing competition among threat actors in this space, we predicted in 2023 that cybercriminals would become more aggressive and expand their target lists and playbooks. We also anticipated adversaries looking for larger payouts, focusing on high-value targets.

As expected, this past year saw a significant increase in aggressive attacks. Attackers disrupted critical industries and operations and utilized destructive tools to cause permanent damage to victims.

Here's an overview of several key ransomware events from this past year that illustrate these developments:

Healthcare industry attacks

Cybercriminals continue to target healthcare providers, and several major attacks have disrupted hospital operations and compromised patient safety. Such attacks highlight the industry's vulnerability to ransomware, where downtime can have life-threatening consequences.

In March 2024, a U.S. health insurance billing firm fell victim to a ransomware attack by the notorious BlackCat/AlphV group, reportedly paying a $22 million ransom to restore services and prevent further disruption. The attack, which impacted as much as a third of Americans, resulted in disrupted payments to doctors and healthcare facilities, alongside difficulties in billing for and filling prescriptions.[2]

Utilities and energy sector disruptions

Utility providers, especially in the energy sector, have been growing targets for ransomware groups seeking to create widespread disruption and secure high payouts. Ransomware attacks have also targeted water management facilities, disrupting water purification and distribution services. One recent incident caused local authorities to issue boil-water notices for affected communities, underscoring the vulnerabilities within the utilities sector. In this case, attackers did not just encrypt data but threatened to alter water quality parameters, raising public safety concerns and illustrating the threat sector's move towards more aggressive, potentially harmful tactics.

Manufacturing sector targeted for maximum disruption

The manufacturing industry has also seen a rise in ransomware attacks, with attackers targeting OT systems to halt production lines, leading to substantial financial losses. The BlackSuit ransomware attack on one automotive software supplier caused production halts across multiple car manufacturers in North America. This resulted in delays in vehicle manufacturing, affected supply chains, and created widespread ripple effects across the industry.[3]

Financial institutions facing new ransomware playbooks

According to the Financial Services Information Sharing and Analysis Center, in 2024, roughly 65% of financial organizations reported dealing with ransomware-related issues.[4] As attackers increasingly leverage tactics beyond encryption, financial institutions are prime targets. Recent attacks highlight the evolution towards extortion-focused methods in the financial sector, such as threatening to expose the financial records of prominent banking customers. Data sensitivity and reputation make institutions more likely to pay up.

The rise of Ransomware-as-a-Service (RaaS)

The RaaS model, while not new, has enabled a broader set of cybercriminals to launch sophisticated attacks without deep technical skills and has opened up a fresh revenue stream for affiliates. For example, the Black Basta ransomware group has been a prominent player in 2024. It leverages the RaaS model to launch multiple high-impact attacks across sectors. In one instance, a government contractor in the defense industry was targeted, exposing sensitive contract information. Black Basta RaaS affiliates have increased attacks on critical infrastructure, illustrating how this model has widened access to ransomware capabilities and emboldened less-experienced attackers.

Wipers Widen Their Reach

As predicted, this past year also saw an increase in ransomware variants adopting destructive techniques, particularly data-wiping methods, instead of traditional encryption. This trend, intended to maximize disruption and inflict permanent data loss, has been increasingly noted in recent ransomware attacks.

One such trend is integrating "wiper" malware into ransomware payloads, which we've discussed in previous reports. This approach is not new, but in 2024, it became a more prominent part of ransomware strategies aimed at raising the stakes for victims by threatening irreversible data destruction if demands aren't fulfilled. FortiGuard Labs reported that these destructive techniques can devastate organizations, especially in critical infrastructure sectors, where downtime and data loss can have severe societal impacts.

Another example involves threat actors targeting operational technology (OT) and critical systems within industries that rely on data continuity, such as healthcare and manufacturing. Attackers aim to coerce ransom payments and permanently damage systems by integrating disk-wiping capabilities, increasing the urgency of robust incident response and backup strategies. These shifts reflect the growing complexity and aggression in ransomware playbooks, where threat actors are moving beyond traditional encryption to include wiper functionality, amplifying their leverage and making recovery without backups nearly impossible.

These and similar incidents demonstrate how ransomware attacks in 2024 have continued to intensify in impact and strategic focus. Cybercriminals are increasingly targeting sectors where operational disruption can lead to maximum societal and financial consequences, aligning with our predictions of attackers using more destructive playbooks and choosing a broader range of high-stakes targets.

Prominent Events Pave the Way for Cybercrime

In 2024, we expected attackers to take advantage of more tailored, event-driven opportunities, such as the Paris Games and the U.S. elections. While prominent events and geopolitical happenings have always been attractive targets for cybercriminals, threat actors now have new tools to support their efforts.

Adversaries certainly capitalized on the global interest in the Paris Games. The FortiGuard Labs team observed a significant increase in resources being gathered across the dark web for the Paris Games, especially those targeting French-speaking users, French government agencies and businesses, and French infrastructure providers. Beginning in the second half of 2023, we saw a surge in darknet activity targeting France. This 80% to 90% increase remained consistent across 2H 2023 and 1H 2024.[5]

Similarly, we witnessed a variety of threats associated with the U.S. elections. In our dark web analysis, we witnessed threat actors selling affordable phishing kits to target voters and donors by impersonating the presidential candidates and their campaigns. Malicious domain registrations also increased, with adversaries creating websites containing election-related content.[6] These types of attacks underscore the need for organizations and citizens alike to remain vigilant, particularly during heightened moments that lead to increased threat actor activity.

Emerging Attack Trends to Watch for in 2025 and Beyond

Cybercriminals will continue to rely on tried-and-true tactics that have enabled them to achieve their goals year after year. As the cybercrime industry evolves, distinct attack trends will emerge in 2025 and beyond. Here are several anticipated developments that will keep security teams on their toes.

More Attack Chain Expertise Emerges

In recent years, cybercriminals have been spending more time "left of boom" on the reconnaissance and weaponization phases of the cyber kill chain. As a result, threat actors can carry out targeted attacks quickly and more precisely. This focus on pre-attack activity among adversaries combined with an increase in new vulnerabilities paved the way for the introduction of the Cybercrime-as-a-Service (CaaS) market, which is the practice of experienced cybercriminals selling tools and knowledge on the dark web to help others execute cybercrimes.

In the past, we've observed many CaaS providers serving as jacks of all trades, offering buyers everything needed to execute an attack, from phishing kits to payloads. However, we previously predicted that CaaS groups would embrace specialization, with many groups focusing on providing offerings that focus on only one segment of the attack chain. We're seeing separate initial access brokers and infrastructure providers emerge, with each group offering specific intelligence needed to execute one stage of an attack and then passing the buyer to the next expert.

We expect to see this supply chain of providers expand. For example, Reconnaissance-as-a-Service brokers will likely emerge as groups hone their expertise in various aspects of an attack and seek to capitalize on specific stages of the kill chain.

It's Cloud(y) with a Chance of Cyberattacks

Edge devices like OT systems remain popular attack targets, particularly as 5G direct-to-device connectivity expands. More devices combined with enhanced connectivity offer adversaries a broader attack surface that provides new opportunities for compromise. While these targets will continue to capture the attention of threat actors, defenders should pay close attention to another part of the attack surface over the next few years: their cloud environments. Although the cloud isn't new, it's increasingly piquing the interest of cybercriminals. We're observing cloud applications coming under attack more frequently, and this is a trend we expect will grow in the future.

According to the Fortinet 2024 Cloud Security Report, 78% of enterprises use hybrid or multi-cloud strategies.[7] Given that most organizations rely on multiple cloud providers, it's not surprising that attackers are leveraging more cloud-specific vulnerabilities, resulting in several high-profile cyber incidents. While fundamental safeguards like multi-factor authentication can help prevent unauthorized access to data in cloud application environments, cybersecurity measures like these are sometimes overlooked as organizations rush to embrace digital evolution.

Beyond implementing security measures to protect cloud environments, this growth in cloud adoption presents broader opportunities for cybersecurity defenders. One example is the development of frameworks for describing, mitigating, and preventing cloud-focused breaches, like the insights developed and made available through MITRE ATT&CK. Additionally, initiatives like the Cloud Security Alliance provide best practices and controls tailored for cloud environments, helping organizations address specific threats through shared knowledge and security standards. Enhancing cloud visibility, enforcing least-privilege access, and employing continuous monitoring solutions are essential for building resilience. The cybersecurity community can also focus on establishing and adopting more comprehensive cloud incident response playbooks and increasing threat intelligence sharing specific to cloud vulnerabilities, ensuring a collective defense against cloud-focused attacks.

Unsurprisingly, threat actors also view the cloud as an area for growth. Cloud environments present another opportunity for cybercrime groups to niche down. We could see an increase in cybercrime groups selling cloud-specific information on the dark web, with some adversaries becoming go-to brokers for this part of the attack chain.

Add to Cart: Automated Hacking Tools for Sale on the Dark Web

The CaaS market has rapidly expanded over the past several years. Today, many attack vectors and associated codes, such as phishing kits, RaaS, DDoS-as-a-Service, and more, are available through this market.

But threat actors aren't stopping there. While we're already seeing some reliance on AI to power CaaS offerings, we expect this trend to flourish in the future. We anticipate attackers will use the automated output from LLMs to power CaaS offerings and grow the market, such as taking social media reconnaissance and automating that intelligence into neatly packaged phishing kits. Embracing automation will increase the number of CaaS options available for purchase on the dark web and represents yet another lucrative opportunity for threat actors. We expect the expansion of the CaaS market to drive a general uptick in cyberattacks, as more offerings mean more cybercrime entry points for novice and experienced adversaries alike.

Let's Take This Offline: Playbooks Expand to Include Real-Life Threats

Over the past several years, we've observed cybercriminals upping the ante regarding attacks. Threat actors have moved from taking a "spray and pray" approach to carefully performing reconnaissance and crafting attacks to breach high-value targets and successfully achieve a hefty payout. Their playbooks have also advanced, with attacks becoming more aggressive and destructive. The rise of wiper usage in ransomware attacks is a prime example, as are instances of cybercrime groups moving from simply encrypting an organization's data to executing denial-of-service (DoS) attacks.

These shifts in attacker strategies beg the question of who (or what) cybercriminals will set their sights on next. We predict adversaries will expand their playbooks to combine cyberattacks with physical, real-life threats. For example, cybercriminals could target critical infrastructure, manipulating industrial control systems in power grids to cause outages or disrupt public services, impacting data integrity and physical operations. Another possibility is blending cyberattacks with threats to supply chains, for instance, compromising a company's logistics system to delay shipments and impact inventory or even tampering with GPS systems to cause real-world disruption.

As attackers become bolder, defenders must adapt. This means expanding playbooks to account for blended cyber-physical threats, increasing collaboration with physical security teams, and integrating cross-disciplinary incident response measures to counteract these evolving tactics.

As cybercriminals find new ways to combine online and offline attacks to maximize damage, we anticipate that various types of transnational crime, such as drug trafficking, smuggling people or goods, and more, will also become regular components of more sophisticated playbooks. Cybercriminals and transnational crime organizations will likely collaborate on these sophisticated new playbooks, which will likely be sold (and resold) on the dark web. This collaboration will likely mirror what we've seen with nation-state actors and APT groups.

Automating Anti-Adversary Frameworks to Disrupt Cybercrime

As attackers continually evolve their strategies, the cybersecurity community can do the same in response. Pursuing global collaborations, creating public-private partnerships, and developing frameworks to combat cyberthreats are all vital to enhancing our collective resilience. While an industrywide, coordinated approach to proactively disrupting cybercrime may have seemed like a pipe dream in the past, numerous efforts are underway today that aim to create friction for threat actors and reduce the likelihood of attacks. Some examples include:

- The NATO Industry Cyber Partnership fosters timely information sharing on cyberthreats, allowing participants to enhance their situational awareness as they work to defend their respective organizations.
- INTERPOL Gateway, comprised of cybercrime experts from police, private industry, and academia, is a platform for exchanging cyber information to support law enforcement and offers training to defenders through its Cyber Surge campaigns.
- The Cyber Threat Alliance offers its members a technology platform for sharing advanced threat data.
- The World Economic Forum's Centre for Cybersecurity and Partnership Against Cybercrime (PAC) and its Cybercrime Atlas project, all of which bring together organizations across the public and private sectors that share a common goal of disrupting cybercrime.

The Cybercrime Atlas is a collaborative effort to build an action-oriented, global knowledge base on cybercrime to power the mitigation and disruption of cybercrime at scale. Building on the expertise of the forum's PAC, the initiative is developing a comprehensive picture of the cybercrime landscape that details criminal operations, shared infrastructure, and networks to help law enforcement and government agencies take down cybercriminals and their infrastructure worldwide.

This project is a strong example of a framework that can easily scale across borders and industries. The World Economic Forum's recently published Cybercrime Atlas Impact Report 2024 provides vital insights from the program that can be applied to other similar efforts.[8] The organization also released its collaboration framework, designed to be a "starting point for new anti-cybercrime operational collaborations that can strengthen the defenses of the stakeholders involved."[9]

When we share intelligence regularly among the cybersecurity community, defenders gain knowledge to help them identify and disrupt similar attacks. As more cybersecurity professionals actively participate in collaborations like these, scaling and automating related activities will allow us to take action faster to prevent and mitigate threats collectively.

Winning the Mean-Time-to-Respond Race

In traditional warfare, defenders are assumed to be at a disadvantage. And while historically, there may have been some truth to this in cybersecurity, the prevalence of technologies like machine learning (ML) and AI are quickly changing the game for defenders, putting us all in a better position to win the arms race against attackers.

According to our recent threat landscape report, newly discovered vulnerabilities are being exploited at a record average of 4.76 days after discovery. This is 43% faster than the time to exploitation observed in the previous period.[10] As a result, defenders must move faster than before, but thanks to AI, security teams are enhancing their ability to detect, analyze, and respond to threats in real time.

We predict that more organizations will integrate AI technology into their cybersecurity platforms to process vast amounts of data, rapidly identify patterns and anomalies, and automate routine tasks. More security teams will employ predictive, AI-driven analytics to anticipate potential attack vectors and vulnerabilities, giving defenders a better chance to disrupt the attack chain and significantly outpace cybercriminals.

Enhancing Our Collective Resilience against the Evolving Threat Landscape

Cybercriminals will always find new, more sophisticated ways to infiltrate organizations. Yet the cybersecurity community has numerous opportunities to collaborate to anticipate adversaries' next moves better and meaningfully interrupt their activities.

The value of industrywide efforts and public-private partnerships cannot be overstated, and we anticipate that the number of organizations participating in these collaborations will grow in the coming years. As the saying goes, "There is strength in numbers," which rings true for cybersecurity. Building alliances is one of the most effective yet frequently overlooked actions organizations can take to address the challenges that cybercrime presents. Developing relationships and exchanging information fosters trust, and when public and private institutions have greater trust in one another, more intelligence can be shared to not just keep pace with but, ideally, stay ahead of threats.

While an organization's security team often takes primary responsibility for defending the enterprise's digital assets, every individual has a role in cybersecurity. Malware, phishing, and web attacks account for 80% of all attacks yearly.[11] These frequently used attack types target individual users directly, underscoring the importance of general security awareness. Implementing an ongoing cybersecurity awareness and training program is crucial to managing organizational risk, as employees can serve as a strong line of defense against threat actors when equipped with the proper knowledge.

Outside the walls of our respective organizations, other entities have a responsibility to promote and adhere to robust cybersecurity practices, ranging from governments to the vendors that manufacture the security products we rely on. To enhance cyber resiliency, organizations should procure technology products that are secure by design, as defined by the Cybersecurity and Infrastructure Security Agency (CISA) and U.S. and international partners.[12] "Secure by design" is a foundational approach to product development that ensures security is an integral part of the design and development process, with strong security controls built into the DNA of every product and service. Fortinet is proud to be an early collaborator and signer of the CISA Secure by Design Pledge, which requires that participants commit to taking measurable steps across seven key areas to make their product development processes and the resulting technologies more secure.[13]

As malicious actors advance their efforts, one thing is clear: No single security team or organization can singlehandedly disrupt cybercrime. Collaborations and partnerships that span industries and borders are vital, and we must find new ways to work together to effectively manage risk, outpace our adversaries, and protect society.

About FortiGuard Labs

Founded in 2002, FortiGuard Labs is Fortinet's elite cybersecurity threat intelligence and research organization. A pioneer and security industry innovator, FortiGuard Labs develops and utilizes cutting-edge ML and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence. Its data is collected through telemetry gathered from Fortinet's millions of sensors (6M+ devices deployed globally), giving It visibility into the real-world threats organizations face today.

1 Douglas Jose Pereira dos Santos, Key Findings From the 2H 2023 FortiGuard Labs Threat Report, Fortinet, May 6, 2024.

2 Raphael Satter, Hacker Forum Post Claims UnitedHealth Paid $22 Million Ransom in Bid to Recover Data, Reuters, March 5, 2024.

3 Sam Sabin, BlackSuit Ransomware Linked to Auto Dealers' Outages, Axios, June 24, 2024.

4 FS-ISAC Releases Guide for Financial Institutions on Ransomware Defense, Banking Journal, October 28, 2024.

5 Dark Web Shows Cyber Criminals are Ready for Olympics. Are You?, Fortinet, July 17, 2024.

6 Fortinet FortiGuard Labs Observes Darknet Activity Targeting the 2024 United States Presidential Election, Fortinet, October 15, 2024.

7 Frederick Harris, Key Findings from the 2024 Cloud Security Report, Fortinet, April 23, 2024.

8 Cybercrime Atlas: Impact Report 2024, World Economic Forum, October 2024.

9 Disrupting Cybercrime Networks: A Collaboration Framework, World Economic Forum, November 11, 2024.

10 Douglas Jose Pereira dos Santos, Key Findings From the 2H 2023 FortiGuard Labs Threat Report, Fortinet, May 6, 2024.

11 Fortinet Training Institute: 2024 Cybersecurity Skills Gap Global Research Report, Fortinet, June 20, 2024.

12 Secure By Design, Cybersecurity and Infrastructure Security Agency, accessed November 14, 2024.

13 Secure by Design Pledge, Cybersecurity and Infrastructure Security Agency, accessed November 14, 2024.

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 SVP Legal and above, 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.

November 20, 2024 4:20 PM / MKTG-311-0-0-EN