Cybersecurity Forecast 2025

Google Cloud Security

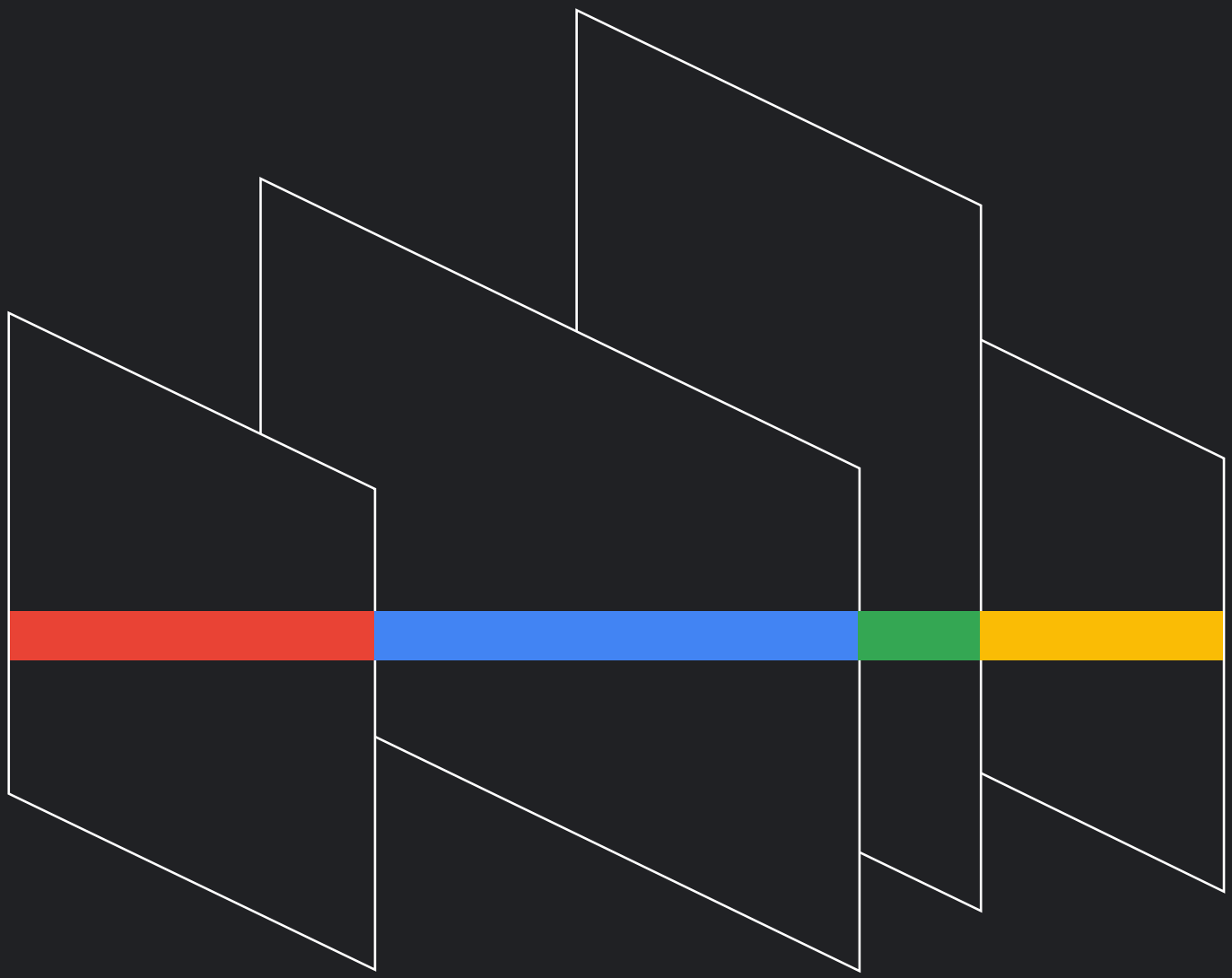


Table of Contents

Introduction

When looking at the year ahead, we never make predictions. Instead, we look at the trends we are already seeing, and provide realistic forecasts of what we expect to see in the wide world of cybersecurity.

The Cybersecurity Forecast 2025 report is filled with forward-looking insights from Google Cloud security leaders, including Sunil Potti, VP/GM, Google Cloud Security, Sandra Joyce, VP of Google Threat Intelligence at Google Cloud, Charles Carmakal, Mandiant CTO, Google Cloud, and Phil Venables, VP, TI Security & CISO, Google Cloud.

The report also features insights from more than a dozen researchers, analysts, responders and experts across numerous Google Cloud security teams, including Google Threat Intelligence, Mandiant Consulting, Google Security Operations, Google Cloud's Office of the CISO, and VirusTotal. These individuals are regularly on the frontlines, and know what organizations and security teams should be prioritizing next year.

Technology advances, threats evolve, the cybersecurity landscape changes, and defenders must adapt to it all if they want to keep up. The Google Cloud Cybersecurity Forecast 2025 report aims to help the cybersecurity industry frame its fight against cyber adversaries in 2025.

Artificial Intelligence

> **"2025 is the first year** where we'll genuinely see the second phase of AI in action with security."
>
> Sunil Potti. VP/GM, Google Cloud Security

Attacker Use of AI

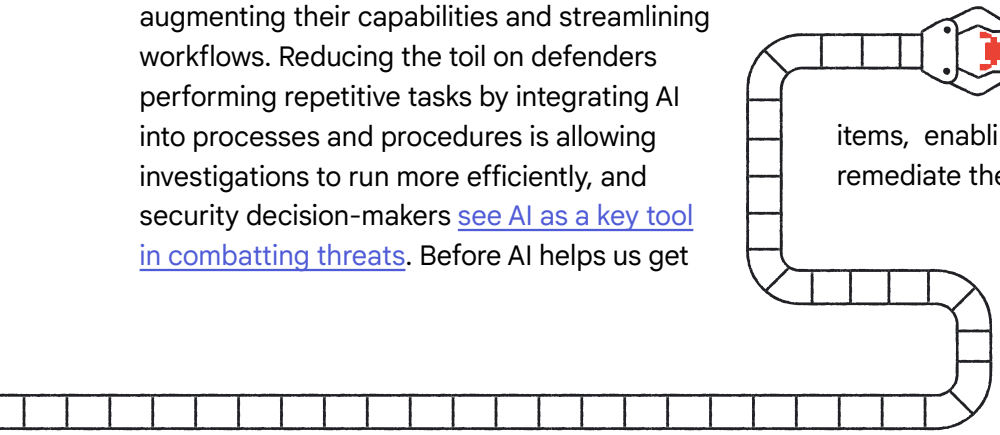
Next year we anticipate malicious actors will continue their rapid adoption of AI-based tools to augment and assist their online operations across various phases of the attack lifecycle. We will see continued use of AI and large language models (LLMs) to develop and scale more convincing phishing, vishing, SMS, and other social engineering attacks. We expect to see cyber espionage and cyber crime actors continue to leverage deepfakes for identity theft, fraud, and bypassing know-your-customer (KYC) security requirements. We expect to observe more evidence of malicious actors experimenting with LLMs and deepfake applications for other use cases, including vulnerability research, code development, and reconnaissance. Additionally, we anticipate more demand in underground forums for LLMs that lack security guardrails, allowing threat actors to query for illicit topics without limit. As AI capabilities become more widely available throughout 2025, enterprises will increasingly struggle to defend themselves against these more frequent and effective compromises.

AI for IO

Information Operations (IO) threat actors will increasingly leverage gen AI tools to support their efforts. Deployment of AI capabilities has expanded beyond early use of generative adversarial network (GAN)-created profiles to backstop inauthentic personas, and has shifted to include the use of large language models (LLMs) to support content creation, and the manufacturing of seemingly genuine articles published to inauthentic websites. This is a significant force multiplier that increases the scale at which actors engaged in this space can produce content, and create additional layers of obfuscation. We expect this trend to continue; actors likely using increasingly available gen AI tooling for a variety of ends, including scaling content creation, producing more persuasive content, and backstopping inauthentic personas.

Next Phase of AI and Security

In 2025, we expect to see a second phase of AI and security in action. This past year, practitioners have been using AI to democratize security, meaning they've begun using AI-driven tools to automate the summarization of complex reports, querying vast datasets with ease, and obtaining real-time assistance for a multitude of tasks, thereby augmenting their capabilities and streamlining workflows. Reducing the toil on defenders performing repetitive tasks by integrating AI into processes and procedures is allowing investigations to run more efficiently, and security decision-makers see AI as a key tool in combatting threats. Before AI helps us get closer to fully autonomous security operations, 2025 will usher in an intermediate stage of semi-autonomous security operations. This will require enough capabilities in our security workflows that are being done by the system itself, smartly, but there still needs to be a human being who can now accomplish much more with AI support. This includes being able to parse through alerts—even with false positives—to create a list of the highest priority items, enabling security teams to further triage and remediate the risks that matter most.



The Big Four

> **"Geopolitical conflicts** will continue driving cyber activity around the world, creating more complexity."
>
> Sandra Joyce.
> VP of Google
> Threat Intelligence
> at Google Cloud

Russia

In 2025, the Ukraine conflict will likely remain a primary focus of Russian cyber espionage, cyber attack, and information operations efforts. In 2024, we tracked increased targeting of Ukrainian soldiers' mobile devices, with operators likely seeking tactical insight to support kinetic operations and other conventional military activities. While less frequent than in 2022 and 2023, we continued to observe disruptive attacks, including a range of different critical infrastructure operators, as well as use of hacktivist personas such as CyberArmyofRussia_Reborn to publicize threat activity. We expect these types of operations to continue into next year.

Outside of Ukraine, Russian cyber espionage will almost certainly continue to support Moscow's global interests, targeting governments, politicians, civil society, journalists, media outlets, and technology organizations primarily in Europe and NATO member countries. Pro-Russian information operations will continue to use a variety of tactics to promote Russian interests and undermine perceived opponents, and capitalize on high-profile events as we observed during the 2024 Summer Olympics in Paris.

China

We anticipate that institutional investments China has made in equipping its cyber threat operators over the last decade will continue to fuel the volume of threat activity and capability development trends into 2025. We will continue to observe Pro-People's Republic of China (PRC) actors using stealthy tactics, including operational relay box (ORB) networks to obscure operator traffic to and from target environments, targeting of network edge devices to take advantage of vulnerable Internet-exposed attack surface and reduce their footprint in target environments, and exploitation of zero-day vulnerabilities as a byproduct of industrializing collection of software vulnerabilities at a national scale. Additionally, we expect Chinese state-sponsored actors to continue to be aggressive, and demonstrate a high risk tolerance.

Pro-PRC information operations (IO) are expected to directly target elections and voters in countries and regions viewed as top strategic priorities for the PRC, most notably Taiwan and the U.S. This activity is expected to include impersonation of voters, promotion of disinformation about rigged votes, and video content featuring AI-generated news hosts. Pro-PRC IO have been largely ineffective at generating authentic engagement, except for isolated successes. However, narratives and tactics will remain aggressive, including use of ad hominem attacks and intimidation.

Iran

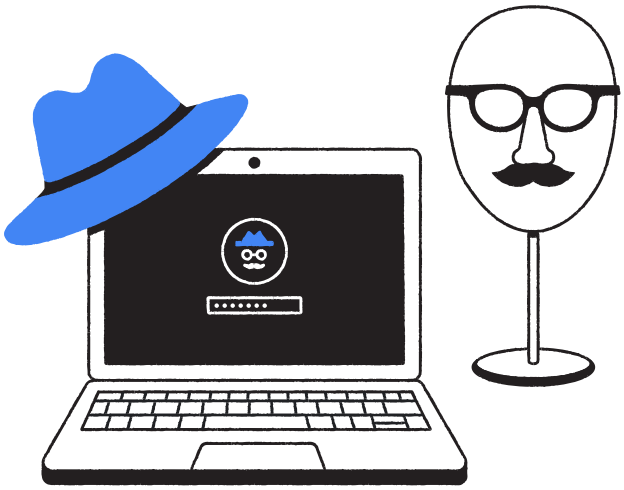
So long as it remains active, the Israel-Hamas conflict will likely continue to dominate Iranian state sponsored cyber threat activity, fueling cyber espionage, disruptive and destructive attacks, and information operations. However, this focus will not prevent Iranian threat actors from continuing operations consistent with long-term patterns, including targeting government and telecommunications organizations across the Middle East and North Africa, or dabbling in cyber crime. We are confident that longstanding objectives of regime stability, economic development, and regional influence will continue to drive monitoring of dissidents, key individuals and organizations linked to Iranian or regional politics, and technologies that could support Iran's military capabilities.

North Korea

We expect geopolitics and economic need will drive North Korean cyber operations into 2025 and beyond.

North Korean cyber espionage operations will continue to support the country's geopolitical objectives, including targeting government, defense, education, think tank targets primarily in South Korea, and the U.S., with some interest in the UK, Germany, Australia, China, and Russia. North Korean actors placed heavy emphasis on supply chain compromises in 2023 and 2024, usually using trojanized open source software packages in social engineering operations targeting software developers, and we expect these tactics to continue into next year.

North Korean actors will continue to pursue revenue generation through IT workers and cryptocurrency theft. IT workers will use stolen and fabricated identities to apply for high paying software development jobs. Significantly, IT workers have also leveraged privileged access to their employers' systems to enable malicious cyber intrusions, and that trend will continue into next year.



Global Forecasts

PRC Actors Will Continue to Deploy Custom Malware Ecosystems for Embedded Systems

Endpoint detection and response (EDR) platforms continue to be a vital component of an organization's security architecture and enable visibility into endpoint activity that is critical for effective security monitoring. In order to evade detection, People's Republic of China (PRC)-nexus espionage actors have continually demonstrated their proclivity and adeptness in developing highly customized malware ecosystems for embedded systems where EDR solutions are not readily available, and traditional digital forensics and incident response can be difficult. Examples include edge devices like firewalls and VPN gateways, or internal network devices like switches and routers. PRC actors design such malware ecosystems with additional capabilities that are specific to the targeted platform or operating system, and take advantage of native functionality in the underlying operating systems. These ecosystems can consist of several different components that work in unison to achieve their desired functionality.

In 2025, PRC actors will continue to employ this strategy to deploy custom malware that enables them to achieve stealthy backdoor access into environments, such as trojanizing legitimate services to listen for attacker connections. They will also leverage low-level malware like rootkits in order to hide evidence of their activities and hinder investigation efforts.

No End in Sight: Ransomware and Multifaceted Extortion

> **"Without question,** multifaceted extortion and ransomware will continue in 2025, likely with an increase outside the U.S."
>
> Charles Carmakal. Mandiant CTO, Google Cloud

Ransomware, data theft extortion, and multifaceted extortion are, and will continue to be in 2025, the most disruptive type of cyber crime globally—both due to the volume of incidents and the scope of potential damage for each event. The impact of ransomware and extortion operations will also continue to extend far beyond the initial victim. 2024 saw significant ransomware incidents in the healthcare sector that negatively impacted patient care at hospitals, blocked patients from refilling important prescriptions, and prevented doctors from running vital laboratory tests or billing insurance.

Based on available evidence, ransomware and extortion operations to date in 2024 have affected more than 100 countries and every industry vertical. The number of newly identified data leak sites (DLS) doubling in 2024 over 2023, and the emergence of multiple new ransomware as a service (RaaS) offerings, illustrate the thriving and prolific nature of the ransomware and extortion threat landscape.

Post U.S. Election Activity

A variety of campaigns targeted the U.S. presidential election throughout 2024, and we don't expect operations to immediately cease now that the election is over. China, Russia, and Iran will continue to target the U.S. government throughout the rest of the year and into 2025, likely taking advantage of the administration change to seek a decision advantage. We anticipate seeing continued state-sponsored cyber espionage, as well as information operations promoting politically divisive content on social media and other platforms. Gen AI tools will enable these actors to increase the scale and effectiveness of these operations, so these campaigns may feel more prevalent now than in previous elections.

Uncovering Operations From Years Past

We anticipate discovering and helping remediate a number of intrusions in 2025 that had been transpiring for quite some time before. In particular, we expect to identify more China-nexus intrusion operations and espionage campaigns that originally occurred in 2024, or perhaps even prior. What we find today is that China-nexus espionage groups are so good at hiding their tracks, and staying buried in networks for long periods of time, that our teams sometimes just stumble upon them years after the threat actors initially broke into an organization.

The Rising Threat of Infostealer Malware: A Gateway to High-Impact Data Breaches

Infostealer malware, though not a novel threat, has demonstrated a concerning surge in sophistication and effectiveness. In 2024, threat actors leveraged stolen credentials, obtained through widespread infostealer campaigns, to infiltrate a significant number of prominent organizations, resulting in various high impact intrusions. The alarming accessibility of credentials from these tools, even to low-skilled threat actors, amplifies their potential for widespread impact.

We anticipate the use of stolen credentials to persist into 2025, with infostealers continuing to serve as a primary vector to obtain them, particularly in environments where two-factor authentication remains unenforced. The absence of this additional security layer leaves organizations susceptible to data breaches of varying degrees of severity. Furthermore, the sophistication of infostealer malware has escalated in recent years, with advancements in anti-evasion techniques and capabilities to bypass endpoint detection and response (EDR), rendering them even more formidable challenges in the cyber threat landscape.

Rising Impact of Compromised Identities in Hybrid Environments

With today's hybrid integration of identities that span on-premises and multi-cloud architectures, the overall impact of a compromised identity will result in elevated risks for organizations. In 2025, it is important that organizations align processes, security controls, and validation efforts to minimize the overall impact of a single compromised identity resulting in downstream consequences, and also to reinforce the strategy of strong authentication.

Historically, authentication for an established identity was based upon a singular transaction, which typically consisted of password-based, single-factor authentication. Now, based on the distributed nature of operations, organizations need to transition from a singular action to one that includes multiple criteria for validation as part of the authentication transaction. The multiplier element should not only include the identity (user) performing the authentication request, but can also require strong phishing-resistant multifactor authentication (MFA) verification of the device associated with the identity, shorter session lifetime (re-validation) when accessing sensitive resources or applications, and identity risk reviews and verifications.

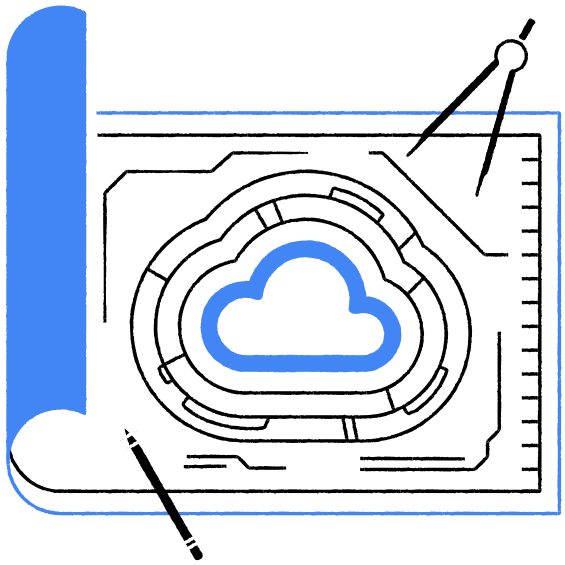
Following this model, organizations can not only enforce proper guardrails to minimize impacts, but increase the confidence of a successful authentication transaction correlating to an authorized and expected activity.

Democratizing of Cyber Capabilities Will Continue to Lower Barriers to Entry for Less-Skilled and Newer Actors

In 2025, organizations will continue to be challenged by a landscape in which an increasing number of barriers to entry will be eroded for cyber criminals and state actors with less sophistication. As more tools, phishing kits, and "as-a-service" resources incorporate advanced capabilities, less skilled threat actors and new entrants into malicious cyber activity will have opportunities to carry out operations with greater efficiency and skill. From web skimming to multifactor authentication (MFA) bypass, the growing professionalization of such services will expand the number of threat actors defenders will have to contend with. Additionally, increasing experimentation by threat actors with gen AI at different parts of the attack lifecycle will also start playing a greater role in increased efficiencies on the adversary side of the security equation.

Maturing Security Operations in the Cloud

In 2025, we expect to see more widespread adoption of cloud-native security information and event management (SIEM) solutions. Scalability and cost-effectiveness will drive mass adoption, even by those hesitating to move away from on-premises deployments. We expect SIEM to reemerge as the central nervous system to the security operations center (SOC), ingesting everything from cloud logs to endpoint telemetry. Security orchestration, automation, and response (SOAR), usually a part of SIEM, will likely move beyond basic playbook execution to handle more complex incident response. This includes automated malware analysis, phishing takedowns, and even patching of vulnerabilities before they're exploited. Additionally, cloud-specific risks such as identity and access management (IAM) misconfigurations, serverless vulnerabilities, and container escapes will be better tackled head-on with purpose-built tools and strategies.



Criticality Drives More Regulations for Cloud Providers

We expect that as more critical infrastructure moves onto hyperscale cloud services, more and more regulators will be directly targeting cloud providers around the world rather than just coming through customers to drive the expected levels of control and resilience on the cloud. In 2025, cloud providers are going to be dealing with more regulation, and also increased expectations. This is appropriate given the extent of their criticality, and how in general an increasing number of services have been moving on to hyperscale cloud, including Google Cloud.

More Interest in Web3 and Crypto Heists

As Web3 and cryptocurrency organizations continue to grow into 2025 and beyond, we expect that attackers will continue targeting smart contract vulnerabilities and private key theft to conduct heists. Web3 organizations are high-value targets for attackers. Since 2020, there have been hundreds of Web3 heists reported, which has resulted in over $12 billion in stolen digital assets.

We anticipate Democratic People's Republic of Korea (DPRK) threat actors will continue to leverage social engineering tactics when targeting Web3 organizations, as well as targeting the supply chain to gain an initial foothold. Web3 companies will need to invest in enhanced security controls and 24x7 monitoring to help detect attacks earlier in the lifecycle to help prevent heists.

Faster Exploitation and More Vendors Targeted

In our 2024 analysis of exploited vulnerabilities disclosed in 2023, the average time-to-exploit (TTE), which we define as the time between disclosure and exploitation of a vulnerability, was five days, down significantly from our previous analysis' average of 32 days. This pace of exploitation is expected to continue, if not quicken, in 2025 and beyond. This average continues to be driven by both n-day and zero-day usage, as both remain lucrative to threat actors. Even when n-day exploitation timelines are observed alone, we still see faster exploitation, as seen by the drop from 23 n-days first exploited after six months in 2021-2022, to only two first exploited after six months in 2023.

Additionally, the number and variety of targeted vendors in these attacks is expected to continue growing in 2025 and beyond, as we have seen increases in the number of vendors targeted for exploitation almost every year since 2018. The number of targeted vendors reached an all-time high of 56 in 2023, over double the 25 observed in 2018. We expect that the number of targeted vendors will continue expanding beyond historically observed targets, requiring more awareness around attack surfaces and their components.

Preparing for an Age of Post-Quantum Cryptography

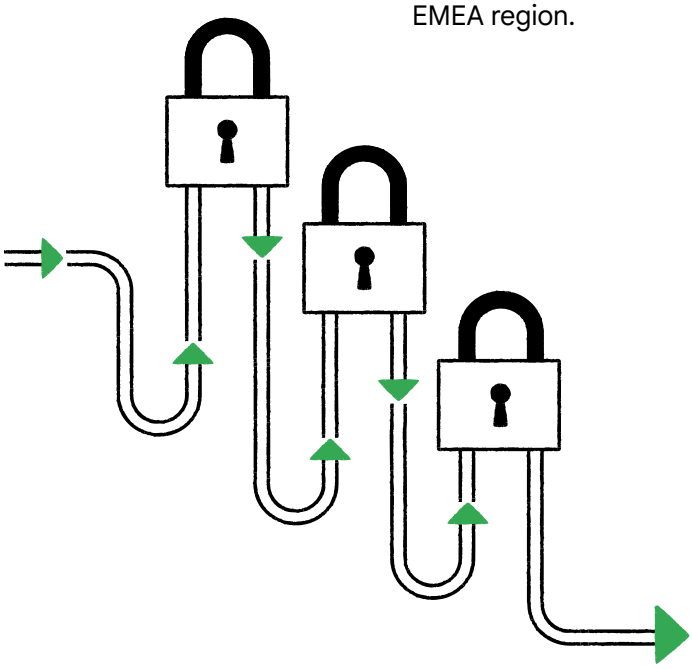
Many organizations in 2025 will be starting their journeys towards adopting new post-quantum cryptography standards finalized by the National Institute of Standards and Technology (NIST) in 2024. The latest guidance from NIST on quantum-safe encryption/key transport and cryptographic signing is designed to help mitigate attacks by adversaries with large-scale quantum computers. These attacks could potentially break encryption, and ultimately compromise sensitive data.

Although quantum threats likely won't have a widespread impact next year, organizations in 2025 will need to start understanding the risks posed by quantum computing, planning their transitions to quantum-resistant solutions, inventorying where they are using cryptography, regularly rotating encryption keys, and generally staying informed of quantum developments using threat intelligence and other guidance.

EMEA Forecasts

A Pivotal Year for Compliance

NIS2, the updated Network and Information Security Directive, will significantly reshape cybersecurity practices across EMEA in 2025. It introduces stricter security requirements, and expands its scope to include a wider range of sectors and organizations, including essential and important entities. This means more businesses will need to implement robust security measures, conduct risk assessments, and report incidents promptly. NIS2 emphasizes risk management, incident response, and supply chain security, forcing organizations to adopt a more proactive and comprehensive approach. Increased oversight and enforcement will lead to greater accountability for cybersecurity failures. Organizations will need to invest in staff training, security technologies, and incident response planning to comply with NIS2. The directive promotes collaboration and information sharing, fostering a stronger cybersecurity ecosystem in EMEA. NIS2 aims to harmonize cybersecurity standards across member states, improving overall resilience against cyber threats. By setting a higher bar for security practices, NIS2 will drive significant improvements in cybersecurity posture across the EMEA region.



Geopolitical Conflicts Drive Threat Activity

Geopolitical conflicts will continue to be a major driver of 2025 threat activity in EMEA, impacting entities all across the region. The ongoing conflict in Ukraine and the persistent tensions in the Middle East are key factors contributing to this trend, and so long as they continue into next year, organizations and countries in the region will feel direct and indirect effects.

While private entities and individuals have limited direct influence over geopolitical challenges, countries that align themselves with one side or another in conflicts can face consequences. One of the ways we see this is through the targeting of digital services and infrastructure. Increasing reliance on these technologies has made them more attractive targets to opposition, and consequently more vulnerable to disruption.

There is no evidence to suggest this trend will decrease in 2025. We anticipate more targeting of digital services by opposing patriotic forces, such as hacktivists or state-sponsored campaigns that disrupt or compromise digital infrastructure. Therefore, organizations must prioritize understanding and staying informed about geopolitical events as they unfold in the cyber domain.

More Focus on Cloud Security

In 2025, cloud security will be paramount for EMEA enterprises. While cloud security is a global concern, Mandiant incident response teams have observed a significant increase in EMEA investigations stemming from misconfigurations, inadequate monitoring, credential reuse, and weak security practices within unmanaged cloud environments. This trend is expected to continue next year. Organizations in the EMEA region are experiencing rapid cloud adoption, and the division of responsibilities between business owners, DevOps, and SecOps teams have a tendency to exacerbate these issues and challenges. Organizations in the EMEA region will have to prioritize cloud security to protect sensitive data and maintain customer trust. They will also need to invest in robust security solutions, implement stricter access controls, and enhance monitoring capabilities.

JAPAC Forecasts

North Korea Threat Actors Setting Their Sights on JAPAC

As cryptocurrency investments continue to grow in the JAPAC region, we expect to see increased targeting of cryptocurrency exchanges, particularly from North Korean threat actors. Throughout 2024, North Korea has continued its attacks against cryptocurrency exchanges, and in September 2024 the FBI issued an alert on the problem. JAPAC has among the highest adoption and growth rates for cryptocurrencies, and this past year there were reports of significant cryptocurrency breaches in the region—including theft of tens and hundreds of millions of dollars worth of digital assets.

One of the ways North Korea is targeting JAPAC countries is by impersonating remote IT workers. The U.S. Department of Justice and other agencies warned "of attempts by Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) information technology (IT) workers to obtain employment while posing as non-North Korean nationals". As part of these operations, some of the fake IT workers worked for organizations located in JAPAC countries.

Chinese-Controlled Websites Posing as Local News Outlets Target Global Audiences with Pro-Beijing Content

In 2022, we exposed the HaiEnergy campaign, which consisted of a network of 72 suspected inauthentic news sites and a number of suspected inauthentic social media assets, used to disseminate content strategically aligned with the political interests of the People's Republic of China (PRC). The sites published content in 11 languages. Since then, we have uncovered at least two other campaigns where third-party companies or PR firms have been hired to promote government narratives via fictitious "Local News" outlets.

This threat poses a heightened risk of inadvertent amplification by other local media outlets owing to a lack of due diligence or readers who chance upon these fake "Local News" outlets. Even though these campaigns have not been very effective in changing the global perception towards China in 2024, we believe these campaigns will persist into 2025, and it is crucial that we continue to uncover and track these fake news outlets to educate global readers. Therefore, organizations must prioritize understanding and staying informed about geopolitical events as they unfold in the cyber domain.

Cyber Criminals in Southeast Asia Continue to Innovate

In 2025, we anticipate seeing continued innovation by Southeast Asia cyber criminals. A new report by the United Nations Office on Drugs and Crime found that Asian crime syndicates are now integrating new service-based business models and technologies—including malware, gen AI, and deepfakes—into their operations, while establishing new underground markets and cryptocurrency solutions for their money laundering needs. According to the report, organized cyber crime in the region is evolving rapidly, and this trend will likely lead to an escalation of activity in the JAPAC region. It is critical for governments and enterprises to formalize regular intelligence-sharing to understand these tactics, techniques and procedures in greater detail, and to be able to trace it to illicit financial flows.

Conclusion

> "**2025 is going to be the year** when AI moves from pilots and prototypes into large-scale adoption."
>
> Phil Venables.
> VP, TI Security & CISO,
> Google Cloud

In 2025, the cybersecurity industry will continue to innovate, while organizations will face evolving challenges across the vast threat landscape.

Rapid advancements in technology, particularly in artificial intelligence, are reshaping tactics for both defenders and adversaries. While AI is rapidly bringing new tools for threat detection and response, it also provides malicious actors with powerful capabilities for social engineering, disinformation, and other attacks.

We will continue to see activity from The Big Four—Russia, China, Iran, and North Korea—who will pursue their respective geopolitical goals through cyber espionage, disruption, and influence operations. Additionally, ransomware and multifaceted extortion, as well as the proliferation of infostealer malware, pose significant risks to organizations worldwide.

In 2025, organizations must prioritize a proactive and comprehensive approach to cybersecurity. This includes adopting cloud-native security solutions, implementing robust identity and access management controls, and staying ahead of emerging threats through continuous monitoring and threat intelligence. It also means preparing for the post-quantum cryptography era, and complying with evolving regulations.

The Cybersecurity Forecast 2025 report aims to equip organizations with the insights and knowledge they need to navigate this complex landscape. By understanding evolving trends and potential threats, organizations can strengthen their defenses, and build a more resilient future.

Contributors

The Cybersecurity Forecast 2025 report features insights from our security leaders:

Charles Carmakal
Mandiant CTO, Google Cloud

Sandra Joyce
VP of Google Threat Intelligence
at Google Cloud

Sunil Potti
VP/GM, Google Cloud Security

Phil Venables
VP, TI Security & CISO, Google Cloud

Many other security experts contributed to the report:

Tufail Ahmed

Dan Black

Sarah Bock

Michelle Cantos

Casey Charrier

Anton Chuvakin

Jamie Collier

Jennifer Fernick

Felix Gröbert

David Grout

Adrian Hernandez

Cris Brafman Kittner

Steve Ledzian

Yihao Lim

Keith Lunden

David Mainor

John McGuiness

Luke McNamara

Matthew McWhirt

Jens Monrad

Mathew Potaczek

Mike Raggi

Kelli Vanderlee

Alden Wahlstrom

Robert Wallace

Jess Xia

Google Cloud

For more information, visit cloud.google.com