Trend Research

TREND MICRO

Critical Scalability

Trend Micro Security Predictions for 2024

Inside this report

Published by

Trend Research

Critical Scalability

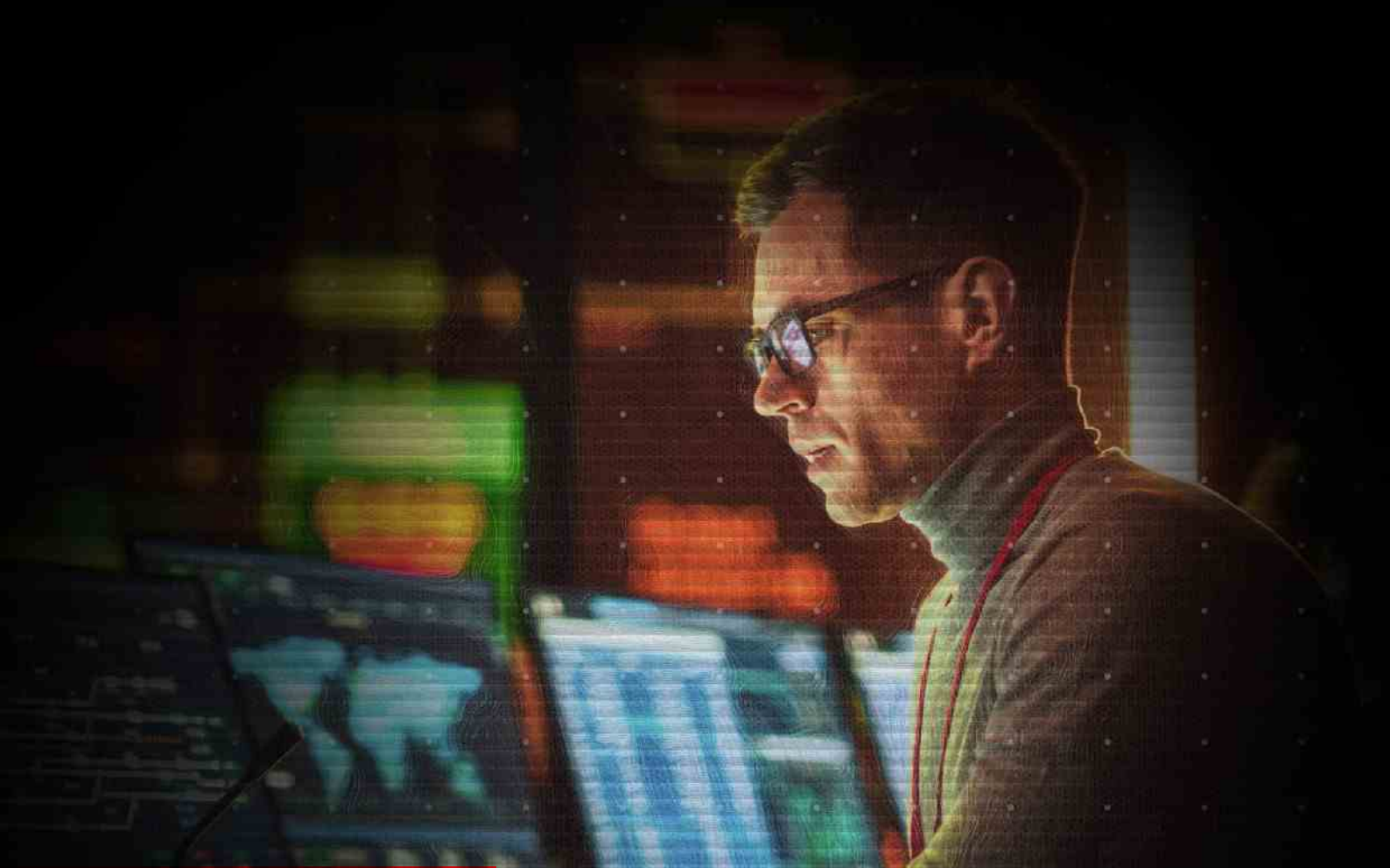
On the heels of a year marked by technological leaps, 2024 is poised to be a hotbed for new challenges in cybersecurity. In a fluctuating economic and political terrain where nearly everything from bank transactions to kidnapping has gone digital, enterprises seeking a strategic advantage have come to rely on the likes of artificial intelligence and machine learning (AI/ML), the cloud, and Web3 technologies. The headwinds from these innovations, which offer use cases for defenders and malicious actors like, inevitably herald turbulent times ahead.

Amid the ongoing conflicts in Ukraine[1] and the Middle East[2] weighing heavily on global leaders, the political landscape is set to be a minefield of cyberthreats that can have far-reaching consequences, with parties from all sides seeking to sway public opinion and shape the course of political events. As the EU,[3] US,[4] and Ukraine[5] gear up for their respective upcoming elections, such electoral periods will prove to be fertile ground for politically motivated cyberattacks, carefully crafted disinformation campaigns, and espionage orchestrated through a web of AI-powered tools and social platforms.

By next year, the transformative potential of these technical breakthroughs is anticipated to reach table stakes, making them the new battlefronts on which cyberattacks will be launched. Similarly, we expect the exploitation of these developments by cybercriminals who are always on the lookout for opportunities to streamline operations, expand the impact of breaches, and reinvent their time-tested tactics.

Business leaders will not only need to demonstrate their willingness to adjust to current events but also reevaluate how well their workflows can accommodate growth. In their attempt to strike a careful balance between foresight and operational hardiness that leverages technological investments, they face a year full of opportunities to examine their capacity to adapt and expand alongside their changing business needs.

In this report, we detail the focal points of next year's threat landscape, along with insights and recommended mitigation measures from our team of cybersecurity experts that are designed to guide decision-makers toward well-informed choices.



Cloud Environments

Security gaps in cloud environments will set the stage for successful cloud-native worm attacks

With their ability to capitalize on vulnerabilities at scale and automate attacks, worms are poised to be one of the go-to tactics in cybercriminals' arsenals next year: By employing automated scripts, malicious actors will be able to pull off a wide range of tasks like reconnaissance, exploitation, and establishing persistence with minimal manual intervention during large-scale attacks within cloud environments.

Cloud misconfigurations serve as easy entry points for attackers; these usually result from overly complicated infrastructures, configuration drift, and improperly configured development environments.[6] Tellingly, misconfigurations also ranked among the top API security risks for organizations, according to the Open Worldwide Application Security Project (OWASP).[7] It will be up to security operation centers (SOCs) to shoulder the added burden of closing these gaps, as cloud security is expected to be absorbed entirely into their operations come 2026.[8]

It would only take a single successful exploit — particularly through misconfigured APIs in the likes of Kubernetes, Docker, and Weave Scope — to trigger rapid propagation in cloud environments. Upon gaining initial access, attackers would then likely resort to rootkits as a stealthy means of achieving persistence.

As cybercriminals execute post-exploitation techniques with greater ease, cyberattacks in Kubernetes environments are expected to become more automated and specialized in 2024. While Kubernetes stands as the most widely used container orchestration platform today, misconfigurations abound among many organizations running Kubernetes in the cloud.[9] This makes the platform a sought-after target, as evidenced by a recent study that found Kubernetes clusters from over 350 organizations and users — among them notable Fortune 500 companies — left unprotected.[10]

Unsurprisingly, at least 60% of these clusters were found to be under attack from malware campaigns, including TeamTNT's Silentbob cloud worm. In addition to its scanning features, this worm-like botnet communicates with a command-and-control (C&C) server that contains tools and scripts designed to prey on insecure cloud infrastructures,[11] serving as a prime example of how attackers can harness infected cloud-native tools to dig their claws into additional victims.

No matter how far along any organization is in its cloud migration journey, it could find itself at the receiving end of "living-off-the-cloud" attacks in which its own cloud-based resources are used against it, underlining the need for security teams to look beyond the usual malware and vulnerability scans. On top of reviewing its security policies, an organization should also proactively scrutinize its cloud environments in anticipation of these worm attacks.

Data and Machine Learning

Data will be weaponized against fledgling cloud-based ML models

Whereas security concerns about the broader cloud environment stem from threats like misconfigurations and cloud-native attacks designed to provide attackers access to stored data, defending machine-learning (ML) models will introduce security teams to a distinct set of challenges that threaten the integrity of the data itself.

In 2024, data poisoning is set to become an emerging threat to cloud-based ML models, leaving defenders to contend with an expansive attack surface — a result of many of these models sourcing data from various origins like third-party data lakes and federated learning systems. Aside from orchestrating such attacks during a model's data-collection phase, threat actors could also orchestrate these by compromising a model's data storage or data pipeline infrastructure.

Between specialized models trained on more focused data sets and large language models (LLMs) and generative AI models with massive data sets, it is the former that will be at higher risk of data poisoning, as the amount of data used by the latter makes them far more difficult for attackers to influence.

An ML model whose performance and behavior has been compromised can open the floodgates to severe consequences for organizations down the line. As opposed to "bug-in-the-system" attacks that generally have a fixed and predictable impact, threat actors can wield data poisoning in specific areas with various outcomes:

- A poisoned natural language-processing model manipulated to divulge confidential data could be used as a means of data extraction.
- Improperly secured Message Queuing Telemetry Transport (MQTT) servers could allow adversaries to write in malicious instructions.
- A tainted recommendation engine could be trained to bring up inappropriate or biased content that might lead to user dissatisfaction — or worse, potential legal repercussions.
- A fraud detection system that has been fed polluted training data could fail to properly detect illicit activities, potentially spelling regulatory penalties for a company.

To stay vigilant against malicious actors looking to poison the well, organizations in 2024 should take a preventative stance that includes the following security measures:

- Thoroughly validating and authenticating all training data sets regardless of origin, whether they be from in-house sources or external providers
- Tightly guarding data sets stored in cloud storage services under a defense-in-depth approach involving multiple practices working in concert and encrypting data whenever it is at rest
- Using more secure transfer mechanisms like HTTPS and SFTP (Secure File Transfer Protocol), as well as cloud-based machine-learning-as-a-service (MLaaS) platforms
- Implementing role-based access control (RBAC) to oversee user access as part of a broader zero-trust defense strategy
- Employing Cloud Security Posture Management (CSPM) tools to help identify and track any changes to their cloud-based resources
- Regularly auditing and monitoring the state of their cloud infrastructure to detect any data-tampering attempts, misconfigurations, and suspicious activity that might pose a danger to their cloud network

Generative AI

Generative AI will allow fraudsters to level up their social engineering lures in targeted attacks

Before long, businesses across the board will have budgets earmarked for generative AI as a fundamental part of their business strategies in IT, advertising, and cybersecurity.[12] The AI boom has also made its way into politics, as proven by the use of AI-generated images in political ads in New Zealand[13] and the US,[14] with Americans anticipating AI to add to the noise of political misinformation ahead of their presidential elections next year.[15] However, it's unlikely that companies will develop their own AI or LLM solutions. Instead, they will seek out vendors that already have these baked into their portfolios, coupled with the expertise to implement them.

The integration of AI in daily operations to harness its maximum potential is not limited to commercial and political institutions alone. Whereas ML, a subset of AI, usually has fixed algorithms, generative AI's algorithms are always evolving; this explains how AI systems are able to create new information based on their previous learnings. These closely related technologies, when added to a threat actor's arsenal, can be useful for different reasons: ML for its data-processing ability, and generative AI for its creative output. However, both are only as good as the information used to train them — even generative AI can be fed bad data, either through accidental exposure or malicious.[16] Like many emergent technologies, AI is a double-edged sword, and its role in the social dimension of cyberattacks will come forward in 2024.

Of the many advances on the AI front, generative AI will stand out as a potent tool for attackers when it comes to impersonation and identity theft, blurring the lines of our digital reality in social engineering schemes like business email compromise (BEC), spear phishing, and harpoon whaling.

According to the latest annual report of the FBI's Internet Complaint Center, cybercrimes with a social engineering aspect racked up some of the highest victim counts, cementing their place among the most profitable criminal revenue streams for attackers.[17]

Given ongoing developments, being cheap and appearing convincing are still mutually exclusive for deepfakes. Of all the AI-powered tools that have become progressively more sophisticated and are thus ripe for hyper-realistic audio and video misrepresentation in real time,[18] we predict that voice cloning will see more abuse in near-future scams. We also predict that this will remain more of a targeted threat since adversaries need to collect numerous audio sources from specific individuals to pull off a successful AI-driven voice impersonation.

The accessibility of AI technologies will clear the path for more convincing and pervasive scams aimed at these select victims. In the wake of WormGPT's shutdown in August under the weight of media scrutiny[19] — and while malicious actors lie in wait before releasing other tools of WormGPT's ilk — other actors could quickly pivot to alternatives. Security researchers have shown that it's possible to trick generative AI systems into circumventing their own censorship rules,[20] so it would not be inconceivable for a resourceful imposter to find a workaround via an LLM jailbreak used in conjunction with stolen user credentials and virtual private network (VPN) connectivity to maintain anonymity.

An initial crop of fraudsters piggybacking on what the US Federal Trade Commission calls "synthetic media"[21] has already been spotted in the wild. The amalgamation of various AI tools like chatbots and voice clones powers multifaceted threats like virtual kidnapping. Since it only takes a few successful attacks for virtual kidnapping to be lucrative, cybercriminals resorting to such tools would not need to play the numbers game.[22] To avoid falling victim to these souped-up scams, defenders should implement zero-trust policies coupled with a paradigm shift where any online interaction is never taken at face value.

Software Supply Chains

Software supply-chain attacks will serve as a clarion call to protect suppliers' CI/CD systems

A piece of software is never more ubiquitous than when it becomes a launchpad to spread malware, as we will see in 2024. When businesses implement commonly used software, they're tapping into solutions that may be considered the industry standard, come with a wealth of support documentation, and can ensure compatibility and interoperability with multiple partners. This enables growing organizations to stay agile even as they incorporate more third-party applications, vendors, and distribution channels to their supply chains. But such software, once compromised, can also be weaponized so that the damage cascades to everyone in a tightly connected network.

Cybercriminals looking to disrupt supply chains will do so through any soft spots in defenses. For example, eSIMs, the latest version of subscriber identity modules or SIM cards, have not only become an integral component of fleet and inventory management in the 5G era but have also proven useful for enterprises in tracking and identifying assets.

However, the sobering reality is that eSIMs are at risk of various SIM-jacking threats[23] such as improper configurations, timing SIM-jacking, or fleet-jacking. Exploiting eSIMs as attack vectors has the potential to imperil entire supply chains, enabling malicious actors to tamper with the inventory management functions that oversee the inventorying of eSIM-enabled devices.

Supply chains have become an attractive target for cybercriminals who want to victimize multiple organizations through a single supplier: A global study commissioned by Trend Micro showed that over half of global organizations have had part of their supply chain compromised by ransomware.[24] Most of the polled IT leaders were also concerned that their organization was at higher risk of being targeted by ransomware because of their network of partners and customers. By using insufficiently defended supply chains as an access vector, threat actors are able to cut out initial access suppliers from their ransomware business models and further maximize their profits.[25]

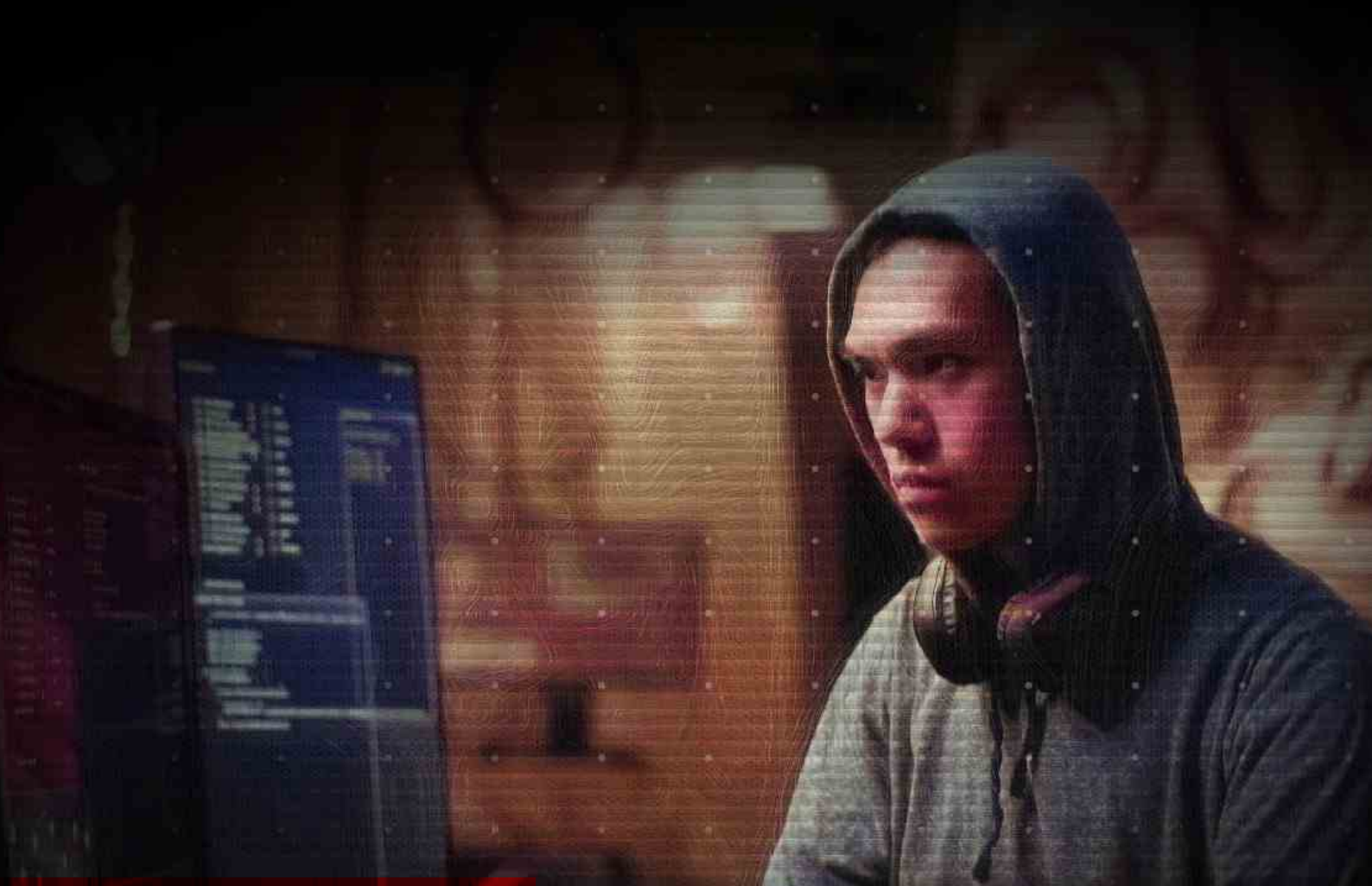
We also predict that malicious actors will attempt to infiltrate vendors' software supply chains through their continuous integration and continuous delivery (CI/CD) systems. Despite the fact that these systems have allowed developers to automate many stages in software development, each project is different: There is no one way of setting up CI/CD pipelines[26] as they are built on multiple tools and processes that come with a number of dependency risks.[27] In 2024, vendors should anticipate that ambitious threat actors will strike at the source — the very code on which IT infrastructures are built — with attacks that will persistently focus on third-party components like libraries, pipelines, and containers

Although they can help fast-track development and cut down time-to-market, these external sources are not without their share of the following security blind spots:

- **A lack of thorough security audits.** While some third-party libraries and containers do use vulnerability scanners, certain bugs could go under the radar if these don't have a Common Vulnerabilities and Exposures (CVE) designation. As long as these vulnerabilities remain undisclosed and unaddressed, they remain a break in the trust chain.
- **Outdated components.** Developers might also inadvertently access outdated components that come with lurking vulnerabilities. Even if the current version of a library or container is secure, there's no guarantee it will stay that way when vulnerabilities are introduced in future updates, either accidentally or via compromised maintainer accounts.
- **Risk of code-injection attacks.** Vulnerable third-party libraries can also allow threat actors to insert malicious code in them that will execute as soon as the library is called. Adversaries could then exploit unauthorized access to systems and data for credential harvesting, hijack system resources to mine cryptocurrency, or launch distributed denial-of-service (DDoS) attacks.

Container registries and platforms use multifactor authentication (MFA), employ carefully scooped tokens, and conduct secret scanning in repositories and the like. However, organizations also need to proactively reduce risks to their CI/CD systems. On their end, we advise security teams and developers to consider the following actions:

- Implement application security tools that can quickly recognize any signs of suspicious behavior.
- Lend these security tools over the entire CI/CD pipeline.
- Conduct in-depth research on libraries and containers before use.
- Scan all libraries and containers — doubly so when updating to a new version — to avoid any hijacked code.
- Monitor any external dependencies, especially those from upstream sources, for any hidden vulnerabilities.



Blockchain Technology

Attackers will look to the blockchain for fresh hunting grounds and extortion plans

The blockchain's ability to create tamper-resistant online ledgers and facilitate transparent transactions holds various use cases for businesses, from the development of social networking platforms to e-commerce websites.[28] Despite its frequent use in digitally distributed record keeping, blockchain technology is still flexible enough that it can also function within predefined limits. This is the case with private or permission-based blockchain networks, which more enterprises around the world are adopting to cut down on operational expenditures in areas like supply chain management and intra-company accounting.

The blockchain's promise of data integrity, cost savings, and resistance to single-point failures nevertheless bely an assortment of implementation and security pitfalls, especially in today's internet-of-things (IoT) era. Blockchains, which are notorious for their latency issues, also generate so much data that they need their own dedicated management system. On top of these concerns, blockchains are not immune to denial-of-service (DoS) and cloud storage attacks that could lock users out.[29]

Restricting user access isn't the worst that adversaries will be up to next year: With more companies turning to private blockchains, it's only a matter of time before threat actors are drawn to the valuable data and assets in them. A steady stream of cybercriminals will not only be gunning for public blockchains but also ramping up attacks on private blockchain networks. Contrary to the common misconception that internal systems are more secure by default, private blockchains will generally face fewer stress tests and lack the same level of resilience as battle-hardened public blockchains that fend off constant attacks.

Owing to their centralized nature, permissioned blockchains hold a lot of appeal for tightly monitored institutions, especially those in the financial sector.[30] Still, this increased level of control might prove to be a cold comfort for enterprises once threat actors begin developing extortion business models dedicated to targeting private blockchains. Knowing that the operators of a private blockchain can modify, override, or erase any entry, attackers will no doubt also try to seize these administrative rights.

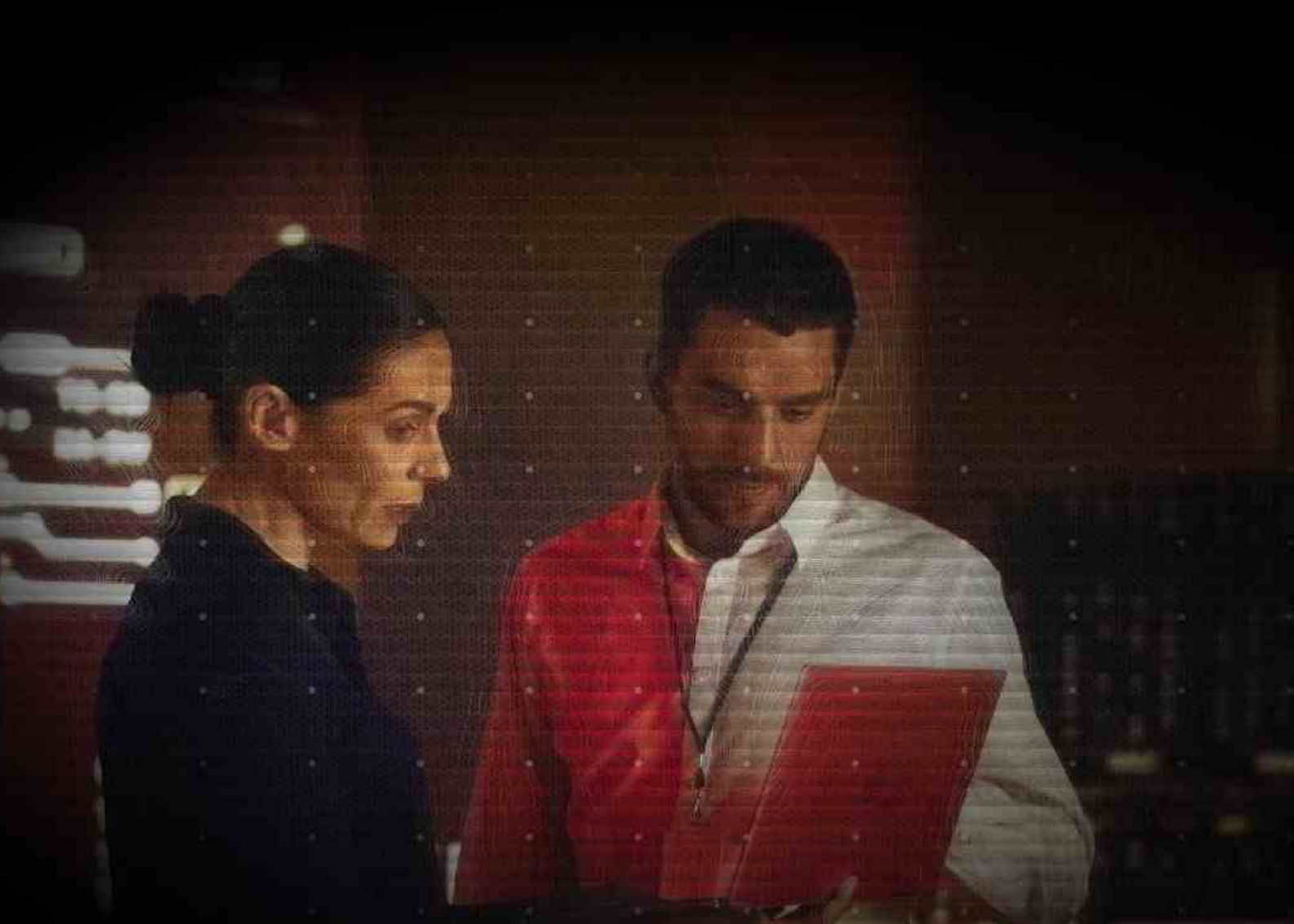
The coming year will also see extortion schemes where threat actors attempt to pilfer keys that will allow them to tamper with aspects of their victim's blockchain, such as writing in malicious data or editing existing records, after which they can demand a ransom in exchange for keeping mum about the extent of the damage they inflicted.

If they were to seize control of enough key nodes, extortionists would be able to encrypt the entire blockchain and prevent it from working altogether until they get a hefty payoff. Unfortunately, private blockchains typically have less nodes that validate transactions compared to their public counterparts, which means less work for attackers planning to compromise the entire network.[31] Organizations offering services that rely on permissioned blockchain networks therefore need to ensure that their network of nodes is adequately distributed so that these can stand up to potential cyberattacks and outages.[32]

This increased criminal attention on Web3 technologies[33] will also lay the groundwork in 2024 for the first criminal groups that run entirely on decentralized autonomous organizations (DAOs), which are governed by self-executing smart contracts hosted on blockchain networks. The buildup to these new threat groups has been observed among malicious actors who have already found ways of weaponizing smart contracts to add layers of complexity on cryptocurrency-related crimes against decentralized finance platforms, such as using fake[34] or overtly malicious contracts.[35]

Since competencies in novel technologies like the blockchain take time to develop, for now organizations will have to depend on external providers to run their blockchains. In the future, there may be a bigger market for products that can monitor blockchain deployments for vulnerabilities and attacks to help businesses manage their blockchains in-house. Until then, organizations will have to work closely alongside their vendors on the following security considerations:

- **Weighing the security needs of cloud-based versus on-premises solutions.** For example, the latter would require businesses to host the blockchain themselves and properly configure network nodes. Cloud-based solutions help simplify the process of setting up blockchain networks, but it is unlikely that these can offer as much control or room for customization compared to blockchains with a tangible on-site infrastructure.
- **Properly developing any smart contracts.** Most smart contracts are written in Solidity, so organizations will need to stay on top of any security risks that are unique to this programming language.



The Road Ahead

Enterprises making bold bets on ML models, generative AI tools, blockchain networks, and the cloud in the hopes of productivity gains should stay sharp for the unvarnished truths and unexpected pain points that will inevitably come with these engines of innovation. As organizations increasingly adopt additional software solutions, they also become more interconnected and data-dependent. In their continuous pursuit of growth, it is therefore paramount that they maintain the ability to manage increased workloads and defense measures across expanding attack surfaces.

As enterprises scale up their operations, they also need to prioritize safeguarding digital assets, confidential data, and the overall integrity of their technological infrastructure. Ultimately, it is a strong security posture built to support business expansion that will future-proof an organization's growing IT stack as it keeps pace with new technologies that will only heighten certain cyber risks or create new ones. For defenders to hold the line against the ever-evolving cyberthreats that lie in wait next year, they will need to ensure protection at every point of the threat life cycle, on top of employing a multi-dimensional security strategy grounded on trusted and forward-thinking threat intelligence.

Endnotes

1 Rob Picheta and Gul Tuysuz. (Nov. 5, 2023). *CNN*. "Tensions grow in Kyiv over status of war, as Zelensky insists conflict with Russia is not at a 'stalemate.'" Accessed on Nov. 6, 2023, at Link.

2 BBC. (Nov. 15, 2023). *BBC*. "Israel Gaza war: History of the conflict explained." Accessed on Nov. 22, 2023, at Link.

3 European Parliament. (Oct. 25, 2023). *European Parliament*. "European elections 2024: MEPs' proposals for the lead candidate system." Accessed on Nov. 6, 2023, at Link.

4 Robert Costa. (Nov. 5, 2023). *CBS News*. "Election 2024: One year to the finish line." Accessed on Nov. 6, 2023, at Link.

5 Yuliia Dysa. (Nov. 3, 2023). *Yahoo! News*. "Ukraine's Zelenskiy ponders idea of 2024 election during war." Accessed on Nov. 6, 2023, at Link.

6 Michael Langford. (Feb. 21, 2023). *Trend Micro*. "Common Cloud Configuration Errors & Fixes." Accessed on Nov. 13, 2023, at Link.

7 OWASP API Security Project team. (2023). *Open Worldwide Application Security Project*. "OWASP Top 10 API Security Risks – 2023." Accessed on Oct. 13, 2023, at Link.

8 Trend Micro. (June 9, 2023). *Trend Micro*. "Trend Micro Predicts Cloud Security Will Be Consumed by the SOC by 2026." Accessed on Nov. 9, 2023, at Link.

9 Magno Logan and David Fiser. (May 25, 2021). *Trend Micro*. "TeamTNT Targets Kubernetes, Nearly 50,000 IPs Compromised in Worm-like Attack." Accessed on Oct. 13, 2023, at Link.

10 Aqua Security. (Aug. 8, 2023). *Aqua Security Software Ltd*. "Aqua Nautilus Researchers Find Kubernetes Clusters Under Attack in Hundreds of Organizations." Accessed on Oct. 10, 2023, at Link.

11 Lucian Constantin. (July 13, 2023). *CSO Online*. "Silentbob worm attack targets multiple cloud technologies." Accessed on Oct. 13, 2023, at Link.

12 Bloomberg Intelligence. (June 1, 2023). *Bloomberg*. "Generative AI to Become a $1.3 Trillion Market by 2032, Research Finds." Accessed on Oct. 13, 2023, at Link.

13 Tess McClure. (May 24, 2023). *The Guardian*. "New Zealand's National party admits using AI-generated people in attack ads." Accessed on Nov. 6, 2023, at Link.

14 Matt Novak. (April 25, 2023). *Forbes*. "GOP Releases First Ever AI-Created Attack Ad Against President Biden." Accessed on Nov. 6, 2023, at Link.

15 Ali Swenson and Matt O'Brien. (Nov. 3, 2023). *Time*. "Poll Shows Most U.S. Adults Think AI Will Add to Election Misinformation in 2024." Accessed on Nov. 6, 2023, at Link.

16 Greg Young. (June 1, 2023). *Trend Micro*. "Generative AI: What Every CISO Needs to Know." Accessed on Nov. 19, 2023, at Link.

17 Internet Crime Complaint Center. (2023). *Federal Bureau of Investigation*. "2022 Internet Crime Report." Accessed on Oct. 20, 2023, at Link.

18 Jon Healey. (May 11, 2023). *Los Angeles Times*. "Real-time deepfakes are a dangerous new threat. How to protect yourself." Accessed on Oct. 13, 2023, at Link.

19 David Sancho and Vincenzo Ciancaglini. (Aug. 15, 2023). *Trend Micro*. "Hype vs. Reality: AI in the Cybercriminal Underground." Accessed on Oct. 13, 2023, at Link.

20 Matt Burgess. (April 13, 2023). *Wired*. "The Hacking of ChatGPT Is Just Getting Started." Accessed on Oct. 13, 2023, at Link.

21 Michael Atleson. (March 20, 2023). *Federal Trade Commission*. "Chatbots, deepfakes, and voice clones: AI deception for sale." Accessed on Oct. 13, 2023, at Link.

22 Craig Gibson and Josiah Hagen. (June 28, 2023). *Trend Micro*. "Virtual Kidnapping: How AI Voice Cloning Tools and ChatGPT are Being Used to Aid Cybercrime and Extortion Scams." Accessed on Oct. 22, 2023, at Link.

23 Craig Gibson. (Nov. 15, 2019). *Trend Micro*. "From SIMjacking to Bad Decisions: 5G Security Threats to Non-Public Networks." Accessed on Nov. 6, 2023, at Link.

24 Trend Micro. (Sept. 6, 2022). *Trend Micro*. "Over Half of Global Firms' Supply Chains Compromised by Ransomware." Accessed on Nov. 18, 2023, at Link.

25 Feike Hacquebord, Stephen Hilt, and David Sancho. (Dec. 15, 2022). *Trend Micro*. "The Future of Ransomware." Accessed on Nov. 18, 2023, at Link.

26 Trend Micro. (Oct. 24, 2023). *Trend Micro*. "CI/CD Pipeline: How to Overcome Set-Up Challenges." Accessed on Nov. 9, 2023, at Link.

27 Trend Micro. (Aug. 29, 2023). *Trend Micro*. "How to Protect Your CI/CD Pipeline." Accessed on Nov. 9, 2023, at Link.

28 Trend Micro. (Jan. 13, 2022). *Trend Micro*. "Blockchain 101: What Is It? How Does It Work? And What Are Its IIoT Applications?" Accessed on Nov. 20, 2023, at Link.

29 Trend Micro. (May 17, 2018). *Trend Micro*. "Blockchain: The Missing Link Between Security and the IoT?" Accessed on Nov. 20, 2023, at Link.

30 Statista Research Department. (Sept. 6, 2023). *Statista*. "Size of the blockchain technology market worldwide in 2018 and 2019, with forecasts from 2020 to 2025." Accessed on Oct. 13, 2023, at Link.

31 Maria Korolov. (July 16, 2018). *CSO Online*. "5 ways to hack blockchain in the enterprise." Accessed on Oct. 13, 2023, at Link.

32 Eric Piscini, David Dalton, and Lory Kehoe. (n.d.). *Deloitte EMEA Grid Blockchain Lab*. "Blockchain & Cybersecurity Point of View." Accessed on Oct. 13, 2023, at Link.

33 Matt Wixey. (Aug. 29, 2023). *Sophos*. "For the win? Offensive research contests on criminal forums." Accessed on Oct. 10, 2023, at Link.

34 Fyodor Yarochkin, Vladimir Kropotov, and Jay Liao. (Jan. 18, 2023). *Trend Micro*. "'Payzero' Scams and The Evolution of Asset Theft in Web3." Accessed on Nov. 9, 2023, at Link.

35 Cifer Fang et al. (March 24, 2022). *Trend Micro*. "An Investigation of Cryptocurrency Scams and Schemes." Accessed on Nov. 9, 2023, at Link.

Critical Scalability

Trend Micro Security Predictions for 2024

TREND MICRO™

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our unified cybersecurity platform protects over 500,000 organizations and millions of individuals across clouds, networks, devices, and endpoints.

The Trend Micro One unified cybersecurity platform delivers advanced threat defense techniques, extended detection and response (XDR), and integration across the IT ecosystem, including AWS, Microsoft, and Google, enabling organizations to better understand, communicate, and mitigate cyber risk.

Trend Micro's global threat research team delivers unparalleled intelligence and insights that power our cybersecurity platform and help protect organizations around the world from 100s of millions of threats daily.

We have 7,000 employees across 65 countries, singularly focused on security and passionate about making the world a safer and better place.

Trend Micro enables organizations to simplify and secure their connected world.

trendmicro.com