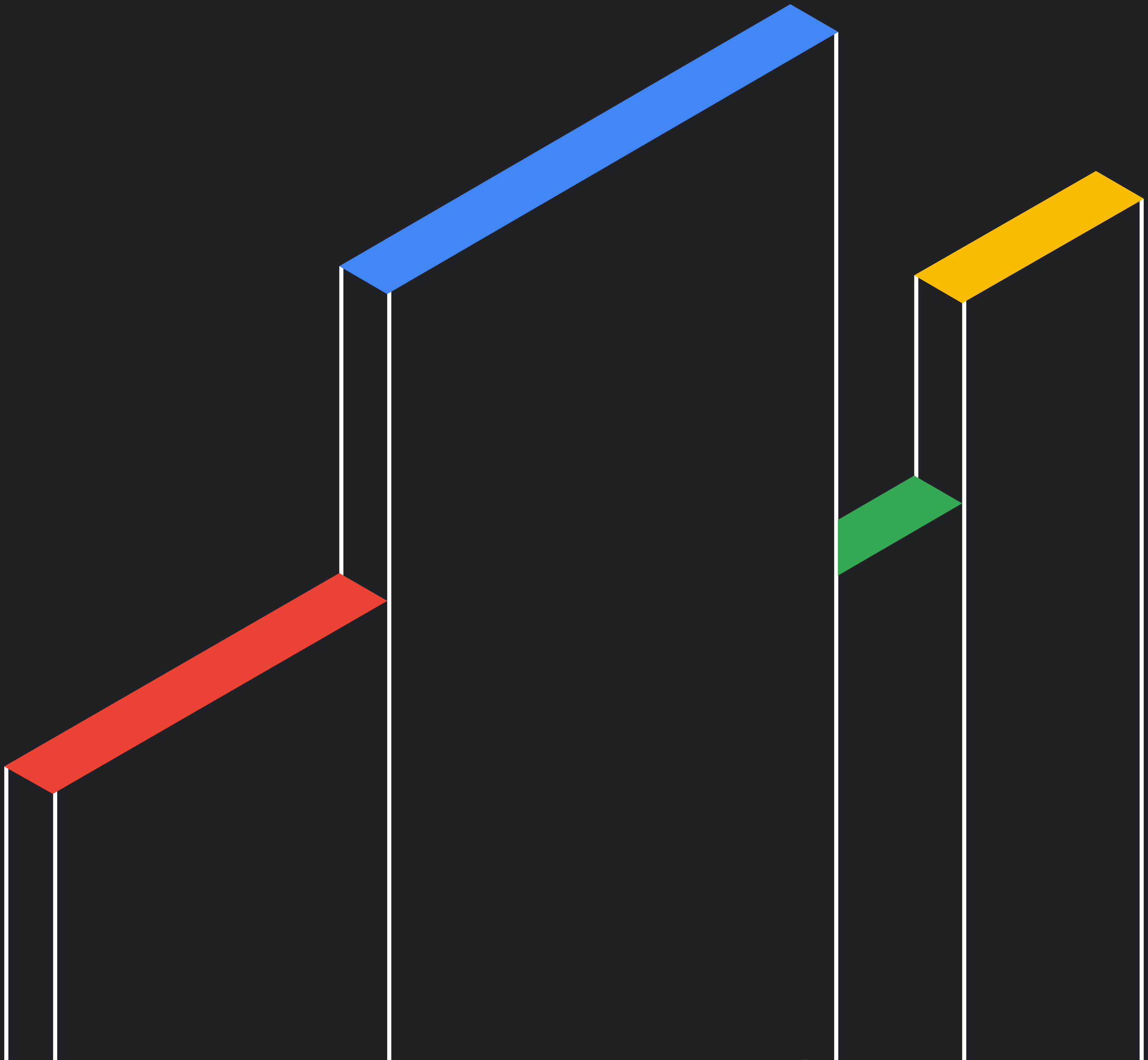
Mandiant

Google Cloud Security

M-Trends

2025 Report

Executive Edition



By the Numbers—The Data of M-Trends

The metrics reported in M-Trends 2025 are based on Mandiant Consulting investigations of targeted attack activity conducted between Jan. 1, 2024 and Dec. 31, 2024.

What do I need to know?

- Financially-motivated actors continue to significantly outnumber others. 55% of threat groups active in 2024 were financially motivated, which marks a steady increase from 52% in 2023 and 48% in 2022. 8% of threat groups were motivated by espionage, which is a slight decrease over 10% in 2023.
- The most common initial infection vector was exploits (33%) for the fifth consecutive year. Stolen credentials (16%) rose to the second most common in 2024, marking the first time this vector has reached this level, and demonstrating its rising popularity. The remaining top five vectors include email phishing (14%), web compromises (9%), and prior compromises (8%).
- The most frequently targeted industries were financial (17.4%), business and professional services (11.1%), high tech (10.6%), government (9.5%), and healthcare (9.3%). These targeting trends are mostly consistent with prior years.
- 57% of the time organizations first heard of malicious activity from an external entity, while 43% of the time it was identified internally. External notifications are divided into 43% from entities such as law enforcement and cybersecurity vendors, and 14% from adversaries, often in the form of ransom notes.
- In ransomware cases, adversaries notified 49% of the time, external entities notified 21% of the time, and internal identification occurred 30% of the time.
- Global median dwell time rose to 11 days from 10 days in 2023, but is still below the 16 days reported in 2022.
- The global median dwell time was 26 days when external entities notified, 5 days when adversaries notified, and 10 days when organizations discovered malicious activity internally.
- Of the 205 malware families observed in investigations, 35% were backdoors, 14% were ransomware, 8% were droppers, 7% were downloaders, 6% were tunnelers, and 5% were credential stealers. These findings are relatively consistent with prior years. We continue to see "living off the land" techniques that don't typically involve traditional malware.

What do we need to do?

- Deploy and optimize advanced threat detection technologies, including endpoint detection and response, security information and event management (SIEM) with advanced analytics, and network traffic analysis.
- Regularly scan for vulnerabilities, prioritize patching based on risk, and automate patching processes where possible to minimize the attack surface.
- Strengthen access controls, practicing sound fundamentals such as least privilege. Limit user and application permissions to only what is necessary, enforce preferably FIDO2-compliant multi-factor authentication (MFA), and regularly review access logs.
- Develop and regularly test incident response and recovery plans. Ensure plans include specific playbooks for ransomware and other threats most relevant to your organization. Conduct regular tabletop exercises and simulations to validate the effectiveness of these plans, and improve response times.
- Engage red teams to test defenses with realistic emulation of adversary tactics. Measure the time it takes security teams to detect and respond, while also identifying vulnerabilities and gaps in defenses.
- Invest in ongoing security awareness training and phishing simulations. Educate employees about the latest and most relevant threats, including phishing, social engineering, and ransomware tactics.

Infostealer Malware Continues to Create a Threat to Enterprise Systems

What do I need to know?

- Infostealer malware, which steals sensitive information like credentials and browser data, is on the rise, and putting organizations at risk of compromise.
- Threat actors are using stolen credentials obtained from infostealer logs for initial access to systems, leading to data theft, extortion, and other malicious activities.
- Credentials stolen via infostealer malware enabled UNC5537 to target Snowflake customer database instances, highlighting the consequence of vast amounts of credentials circulating on the infostealer marketplace.
- Personal devices for work and contractor systems create unique challenges; for example, infostealers can compromise corporate credentials used on infected personal systems or synchronized browsers.

What do we need to do?

- Implement strong multi-factor authentication (MFA), notably adversary-in-the-middle (AiTM) resistant MFA methods such as hardware security keys or mobile authenticator apps.
- Strengthen endpoint security by deploying endpoint detection and response (EDR) and intrusion detection systems (IDS) for monitoring and preventing infections.
- Establish strict policies to separate personal and corporate device use, and review security controls of third-party suppliers and contractors.
- Apply controls to browsers to restrict third-party cookies, disable password autofill, and disable unapproved browser extensions.
- Establish software use policies, educate users with training to prevent downloads from untrusted sources, and consider implementing an enterprise application store for validated applications.

Democratic People’s Republic of Korea Insider Threats

What do I need to know?

- The Democratic People’s Republic of Korea (DPRK) deploys its citizens as remote IT contractors to generate revenue, and fund national interests.
- DPRK IT workers use stolen or fabricated identities, false employment histories, and supporting documentation to secure high-paying positions in technology companies, often in the U.S., but also in Europe.
- Post-hiring, they use virtual private networks (VPNs) and local facilitators to mask their true locations and maintain access to corporate systems, blending into legitimate network traffic to avoid detection.
- While direct malicious activity has been limited, their access to corporate infrastructure poses risks of espionage, data theft, and extortion, with some instances of extortion already observed.

What do we need to do?

- Conduct thorough background checks on employees, including biometric verification, and verify educational and employment histories against independent sources.
- Enhance interview procedures by requiring on-camera interviews, being wary of candidates who are unwilling to appear, and be alert to inconsistencies in personas and physical presentations.
- Require in-person pickup of corporate laptops with ID verification when possible. Apply extra verification when shipping resources to addresses not listed on employment documents, and review background checks in such cases.
- Install endpoint detection and response (EDR) tools, monitor for remote access software and VPN connections (especially Astrill VPN), and log human interface device (HID) connections.
- Enforce least privilege access by limiting user access to only the data and resources necessary for their roles. This minimizes potential damage from espionage, data theft, or extortion attempts.

The 2024 Iranian Threat Landscape

What do I need to know?

- Iran-nexus threat actors increased their cyber operations in 2024, notably targeting Israeli entities, and used a variety of methods to improve intrusion success.
- There was a significant surge in custom malware attributed to Iran-nexus threat actors, with a 35% increase compared to 2023, and over 45 new malware families discovered.
- Israel-based targets were a focus of destructive and disruptive operations often involving wiper malware, which were frequently accompanied by hack-and-leak operations from various online personas affiliated with Iran-nexus threat actors.
- Iran-nexus threat actors leveraged public resources, cloud infrastructure, and legitimate tools such as remote monitoring and management (RMM) software to evade detection.
- Social engineering schemes became more sophisticated, incorporating graphical user interfaces (GUIs) to disguise malware, and using current events and employment themes to trick targets.

What do we need to do?

- Enforce phishing-resistant multi-factor authentication (MFA), particularly certificate-based authentication (CBA) and FIDO2 security keys—especially for privileged accounts—to counter credential harvesting and MFA bypass attempts.
- Implement a security-first design for cloud technology adoption that includes defining security controls, ensuring visibility into all cloud-based activities, and providing data for threat hunting, incident response, and ongoing monitoring.
- Conduct comprehensive user awareness training, focusing on recognizing and responding to increasingly complex social engineering campaigns, including those targeting individuals outside of work perimeters.
- Be vigilant against the use of legitimate tools such as RMM software by threat actors, as they can bypass traditional detection methods. Implement monitoring and auditing for unusual RMM activity. Detections may be tuned to allow the legitimate use of such tools.
- Collaborate across industries and sectors to share threat intelligence and best practices for defending against Iran-nexus actors, as collective defense is crucial.

Evolution of Data Theft in Cloud and Software as a Service Environments

What do I need to know?

- Attackers are shifting from targeting on-premises networks to targeting cloud-based stores of centralized authority, such as single sign-on (SSO) portals, to gain broad access.
- Social engineering is increasingly being used to target users with privileged access to software as a service (SaaS) environments, bypassing traditional network controls.
- Attackers are using hybrid approaches, combining on-premises and cloud resources, and blending malicious activity with legitimate traffic to evade detection.
- Insufficient logging and monitoring in cloud environments is creating blind spots, hindering the detection of attacker activity and slowing investigations.
- Threat actors are exploiting unmanaged risk brought on by organizations not fully understanding the shared responsibility model for cloud.

What do we need to do?

- Ensure comprehensive logging is enabled across all cloud services, including network traffic logs, firewall logs, storage access logs, compute and resource monitoring, audit logs, database logs, and identity and access management (IAM) logs.
- Implement strong IAM practices, including multi-factor authentication (MFA), and closely monitor SSO portals and privileged accounts for suspicious activity.
- Regularly review and validate subscription levels with cloud and SaaS providers to ensure they meet necessary logging and security visibility requirements.
- Educate users about social engineering tactics targeting cloud and SaaS environments, and establish clear procedures for verifying requests related to password resets and MFA enrollment.
- Thoroughly understand the shared responsibility model of cloud security, and clarify the division of security responsibilities between the organization and the cloud provider.
- Ensure incident response plans account for hybrid environments, focusing on procedures for detection, containment, eradication, and recovery for integrated on-premises and cloud systems.

Common Themes in Cloud Compromise Investigations

What do I need to know?

- Threat actors are increasingly exploiting misconfigurations that extend beyond cloud perimeters to gain access to cloud environments, even in organizations with mature cloud security.
- Three major themes contribute to successful cloud compromises: 1) identity solutions lacking sufficiently advanced security policies, 2) improperly secured on-premises integrations, and 3) poor visibility into the extended cloud attack surface.
- Compromised identities can often stem from identity architectures and practices which lack security controls such as multi-factor authentication (MFA), easily bypassed password reset portals, and inadequate third-party access controls.
- Improperly secured integrations between on-premises and cloud infrastructure can allow attackers to move vertically between environments, and bypass cloud security controls.
- The cloud attack surface includes not just network exposure, but also data enumeration, credential sprawl, and publicly exposed resources, requiring organizations to proactively identify and reduce this expanded attack surface.

What do we need to do?

- Strengthen identity security by implementing strong MFA (phishing-resistant), secure password reset processes, and tightly control third-party access. Use privileged identity management (PIM) and ensure separate identity stores for the extended workforce.
- Secure on-premises integrations by auditing and securing trusted service infrastructure, and compute and network integrations between on-premises and cloud environments. Regularly review and restrict access to management interfaces, and ensure network connectivity is properly segmented.
- Proactively identify and reduce the cloud attack surface by managing data enumeration, addressing credential sprawl, and securing publicly exposed resources. Use cloud security posture management platforms for comprehensive visibility and compliance monitoring.
- Adopt a comprehensive, multi-layered security approach that includes access restrictions, hardening measures, ongoing detection strategies, and proactive response actions across all layers, including identities, resources, network, and endpoints.

Threats to Web3 and Cryptocurrency

What do I need to know?

- Web3 technologies, including cryptocurrencies and blockchains, are increasingly being targeted for theft, money laundering, and financing illicit activities.
- Threat actors, including those affiliated with the Democratic People's Republic of Korea (DPRK), have stolen significant amounts of digital assets by using sophisticated social engineering tactics, and exploiting vulnerabilities.
- Cryptocurrency transactions present challenges for tracing and regulation due to obfuscated fund flows, and the immutability of smart contracts, which can also be abused to host malicious infrastructure.
- "Drainers" and malicious smart contracts are used to steal cryptocurrency from users' wallets, and a "drainer-as-a-service" (DaaS) market has emerged, facilitating these attacks.
- Organizations adopting Web3 technologies face challenges in balancing rapid integration with robust security, and often neglect standard security controls, leading to technical debt and expanded attack surfaces.

What do we need to do?

- Combine transaction data analysis with endpoint and security telemetry to better detect malicious activity targeting Web3 and cryptocurrency platforms.
- Go beyond focusing solely on core wallet infrastructure and cryptographic controls, and ensure that standard security controls are implemented and maintained to avoid technical debt, and reduce the attack surface.
- Educate and train personnel on social engineering tactics. Threat actors frequently use social engineering, such as phishing and fake job postings, to gain initial access, so training employees to recognize and avoid these tactics is crucial.
- Since threat actors may compromise software supply chains by trojanizing trading or cryptocurrency software, organizations should thoroughly vet and verify any third-party software before deployment.
- Be vigilant for malicious smart contracts and "drainers" that attempt to steal digital assets. Implement monitoring to detect and prevent unauthorized access to cryptocurrency wallets.

Unsecured Data Repositories

What do I need to know?

- Organizations often overlook the security of internal data repositories such as file shares and SharePoint sites.
- These repositories—commonly accessible to employees with standard privileges—can contain sensitive information, including credentials, financial data, and intellectual property.
- Financially-motivated actors target unsecured data repositories for extortion, and advanced persistent threat (APT) groups target them for espionage.
- Unsecured data repositories lower the effort required for threat actors to achieve their objectives, as they can often accomplish their goals (including privilege escalation) without using more advanced methods such as malware or zero-day exploits.

What do we need to do?

- Perform an inventory and audit of data repositories. Identify where sensitive data resides, regularly review the contents, and remove unnecessary or outdated data.
- Ensure users have only the access required for their roles, distinguish between read and read/write access, and avoid blanket permissions.
- Train employees on data security best practices, the importance of protecting sensitive data, and how to report instances of exposed data.
- Encrypt data both in transit and at rest to limit exposure.
- Use automated tools to identify exposed credentials and secrets, and conduct regular security assessments to evaluate the effectiveness of controls.
- Implement FIDO2-compliant multi-factor authentication (MFA) as a mandatory security measure for all access attempts to critical data stores.
- Implement data loss prevention (DLP) technologies to effectively prevent sensitive data from leaving secure environments via email and file sharing.

Download the full report.

If your organization suspects a cyber incident, or you are experiencing a security breach, please contact Mandiant for Incident Response Assistance.

Google Cloud

For more information, visit **cloud.google.com**.