Trend
Research

TREND MICRO

# TREND 2025
# CYBER RISK REPORT

## Outpacing the adversary

**The Trend 2025 Cyber Risk Report sustains our shift towards proactive security. Protecting enterprises is no longer about stopping breaches but is now about staying ahead, making cybersecurity a business enabler. This report looks at our telemetry from 2024: by looking at last year's risk landscape, we recognize exposures and understand attacker behavior to be able to implement countermeasures for the year ahead. This way, we transform security from a challenge to a catalyst for innovation and business growth.**

This report harnesses data from the Cyber Risk Exposure Management[1] (CREM) solution of our flagship cybersecurity platform Trend Vision One™[2]. Telemetry from this solution identifies exposures across attack surfaces to help prioritize and address risk areas. Combined with data from our native eXtended Detection and Response[3] (XDR) tools and threat intelligence, this report primes enterprises with information on adversaries along with risk insights to reduce their Cyber Risk Index and stay ahead of the curve.

# The Cyber Risk Index

**To achieve a proactive approach to cybersecurity, we capitalize on data from our Cyber Risk Exposure Management solution, which is designed to protect organizations' digital assets from attacks by evaluating risks across the attack surface, prioritizing them, and implementing appropriate countermeasures.**

CREM calculates an enterprise's Cyber Risk Index (CRI), a metric that quantifies the overall security risk of an organization based on a consolidation of individual assets and risk factor scores. Our research[4] has found that organizations with a CRI above the average have a greater likelihood to suffer from attacks than those with a lower CRI. Like how preventive health check-ups reveal the overall state of health, analyze risks the body might be exposed to, and creates an action plan on how to prevent these risks, CREM works to identify the CRI and creates a strategy to reduce them and therefore improve an organization's security posture.

While risk is evaluated qualitatively, the CRI quantifies it by using a scale from 0-100 to represent and give a clearer picture of where enterprises or sectors stand in terms of security and risk.

CREM uses the risk event catalog to formulate a risk score for each asset type and an index for organizations by multiplying an asset's attack, exposure, and security configuration by the asset criticality. The risk scores are calculated individually for every asset, with each score considering asset type and criticality. The result is an integer between zero and 100 that falls into one of three levels.

- **Low Risk (0-30):**
    - Organizations in this category are considered relatively secure
    - Immediate significant measures are generally not necessary

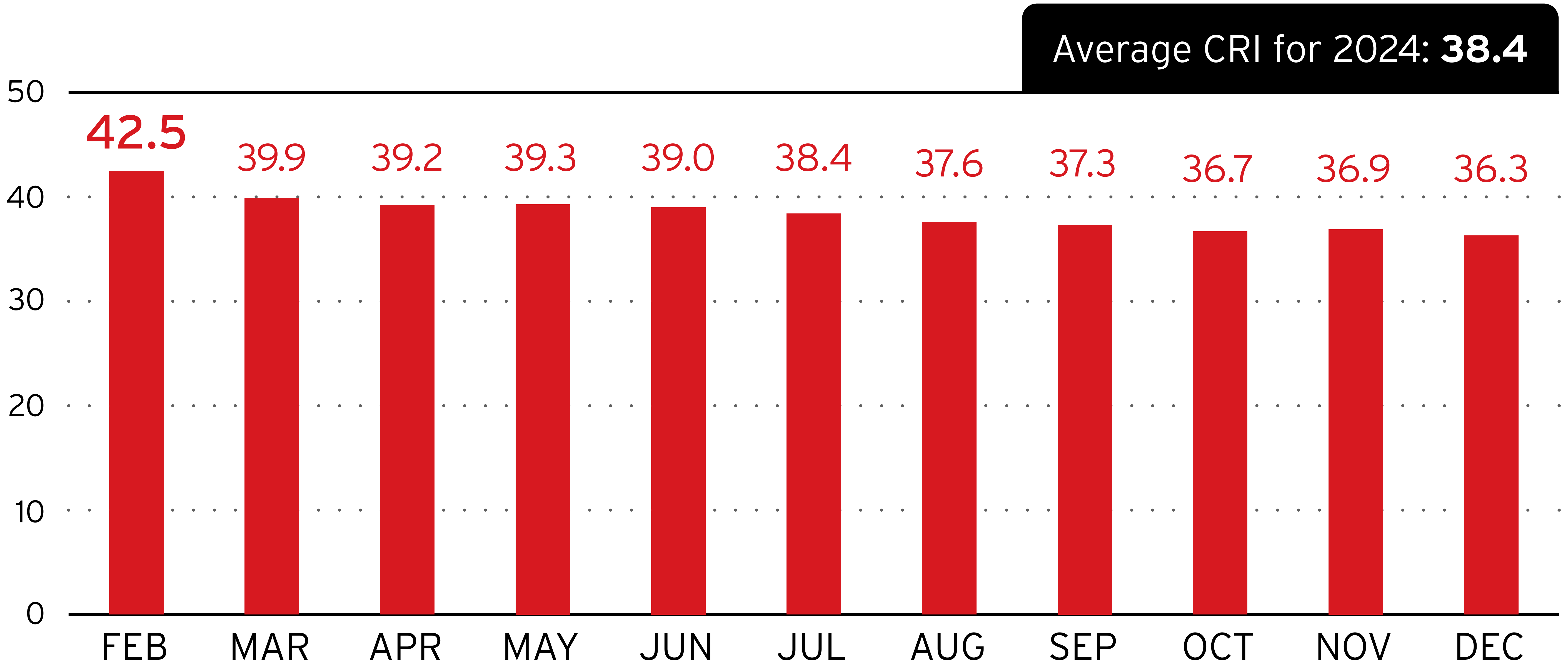
- **Medium Risk (31-69):**
    - Organizations in this category have several risk factors that need to be addressed
    - It is advisable to consider and implement appropriate countermeasures
- **High Risk (70-100):**
    - Organizations in this category are exposed to severe risks
    - Prompt and robust security measures are essential to mitigate potential threats

Learn more with our Cyber Risk Index Overview[5] and our technical report on how to understand risk score calculations[6].

This report covers telemetry from February to December 2024; it excludes data from January as the CREM dashboard algorithm was updated at the end of that month with a weight summation method that affects CRI computation. Telemetry from February to December 2024 was computed with the same algorithm and provides a more accurate average CRI. Future improvements to CREM computation will be disclosed accordingly. Also note that industry CRI data do not include industries with a sample size too small to be statistically relevant.

# Cyber Risk Index Data

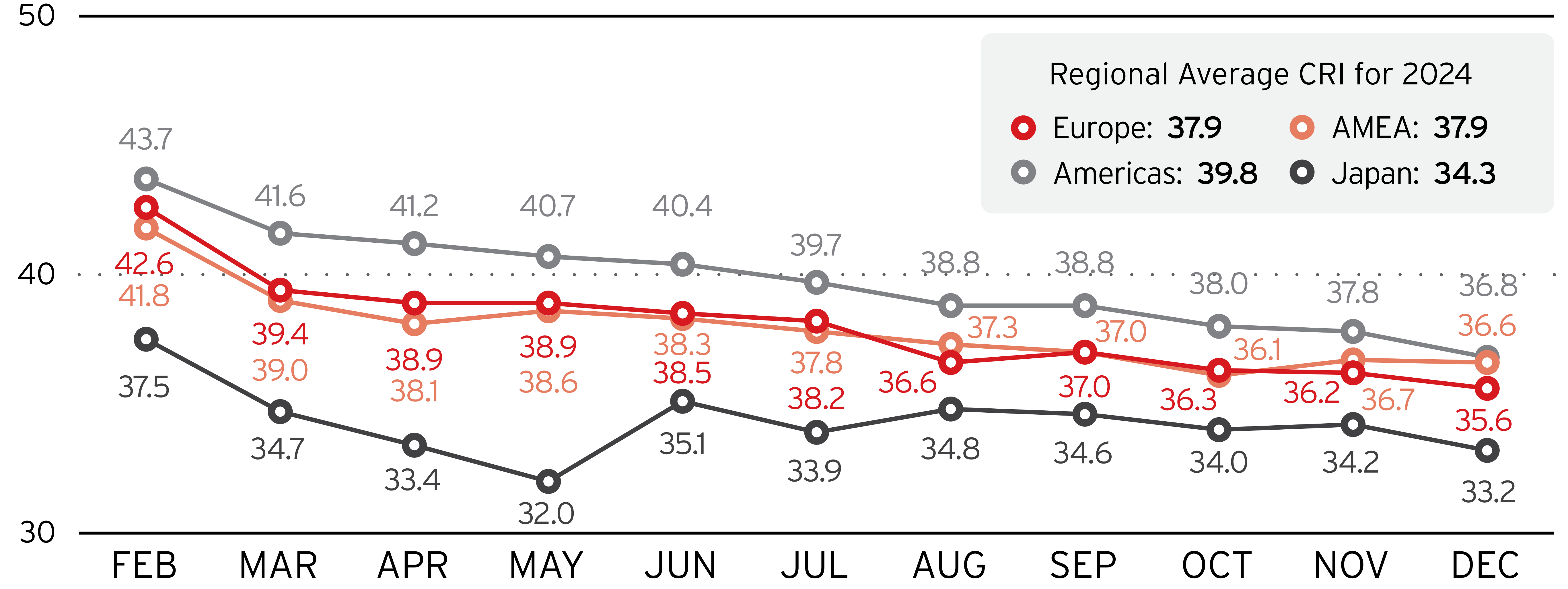
## Overall average CRI



*(February 2024 - December 2024)*

The overall average CRI in 2024 improved consistently per month, with a 6.2-point difference from the overall average in February to December. While this improvement suggests that enterprises have been successfully operationalizing cyber risk management, a 36.3 overall CRI still falls within medium risk, an average indicative that organizations still have several risk factors that need addressing. This emphasizes the need for continuous monitoring of the attack surface risk life cycle, which includes discovery, assessment, and risk mitigation through necessary countermeasures.

## Regional Average CRI per month(February 2024 - December 2024)

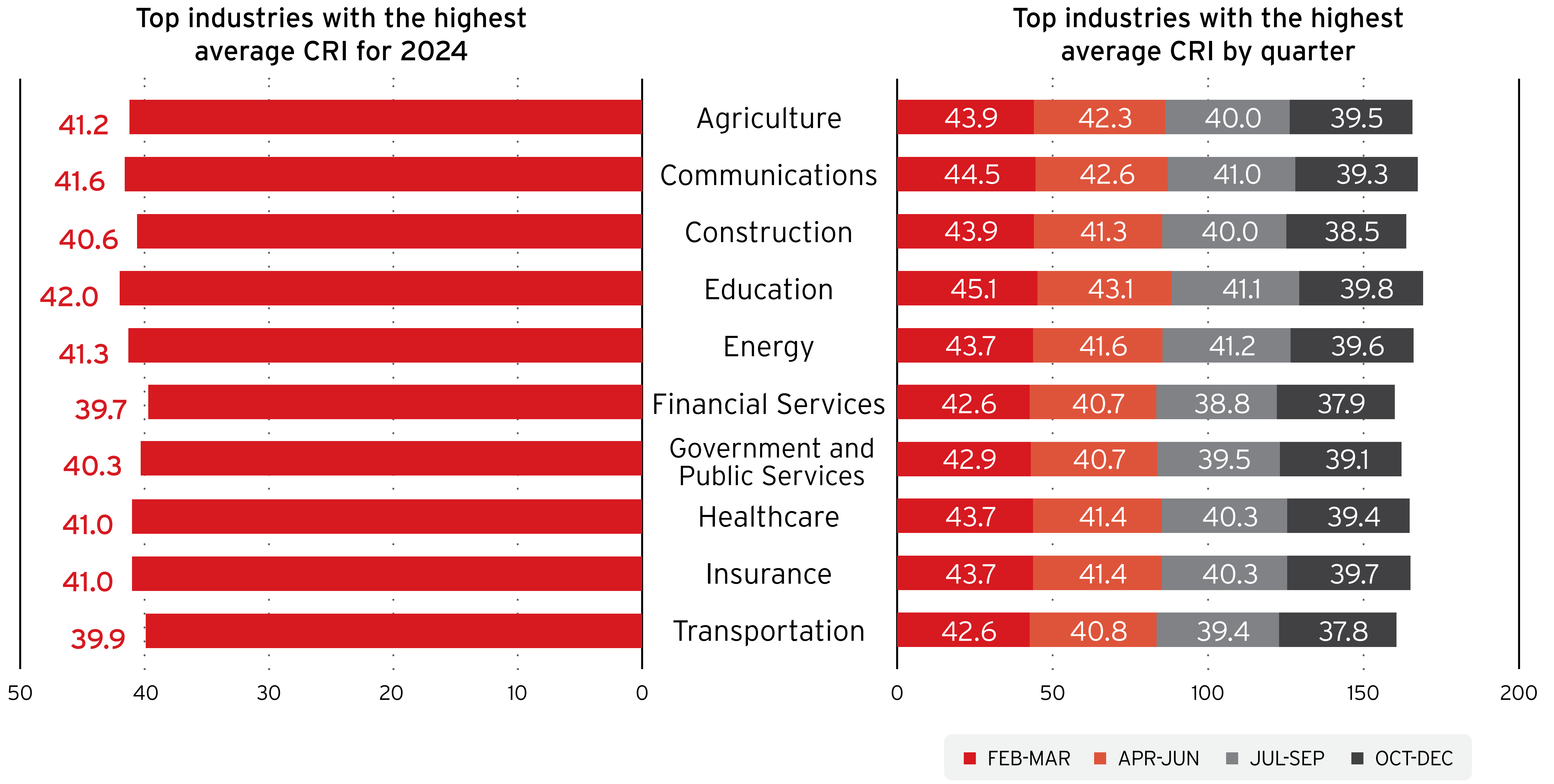


*(February 2024 - December 2024)*

Our regional telemetry is consistent to the overall average CRI data. There is a general downtrend in risk indices among the regions; Europe exhibiting the biggest improvement from February to December with a 7-point difference. The region is pushing for increased cyber hygiene and resilience with the Digital Operational Resilience Act[7] and the Cyber Resilience Act[8], which could influence enterprises to take a more proactive approach in cybersecurity through patching, fixing configurations, and refining user access and permissions, among others.

While CRI among regions improved in the past year, each region's risk index is still within the medium risk level: enterprises from each region still have unsecure assets that might expose the organization to threats.

## **Top industries with the highest average CRI by quarter**(February 2024 - December 2024)



*(February 2024 - December 2024)*

The education sector had the highest average CRI at the beginning of the year and is still among the sectors with the highest CRI by the last quarter of 2024. Enterprises and organizations in this sector are vulnerable to cyberattacks that could mean disruption of educational services, data breaches, intellectual property theft, and reputational damage.

Factors that affect the education sector's CRI could include legacy systems with outdated hardware and software and unpatched applications. The sector's diverse group of users who create a larger attack surface with the adoption of remote learning environments also increases the likelihood of human error that result in security misconfigurations or exposure to phishing attacks. Educational institutions, especially public ones, also grapple with limited resources that could affect how much they are able to secure their systems and networks.

Enterprises in the agriculture and construction industries also have work to do. Attack surfaces of enterprises in these sectors are more vulnerable to attacks than other industries, which could mean operational disruption. Both sectors have a strategic position in global supply chains, so the impact of successful attacks might have a ripple effect on an international scale.

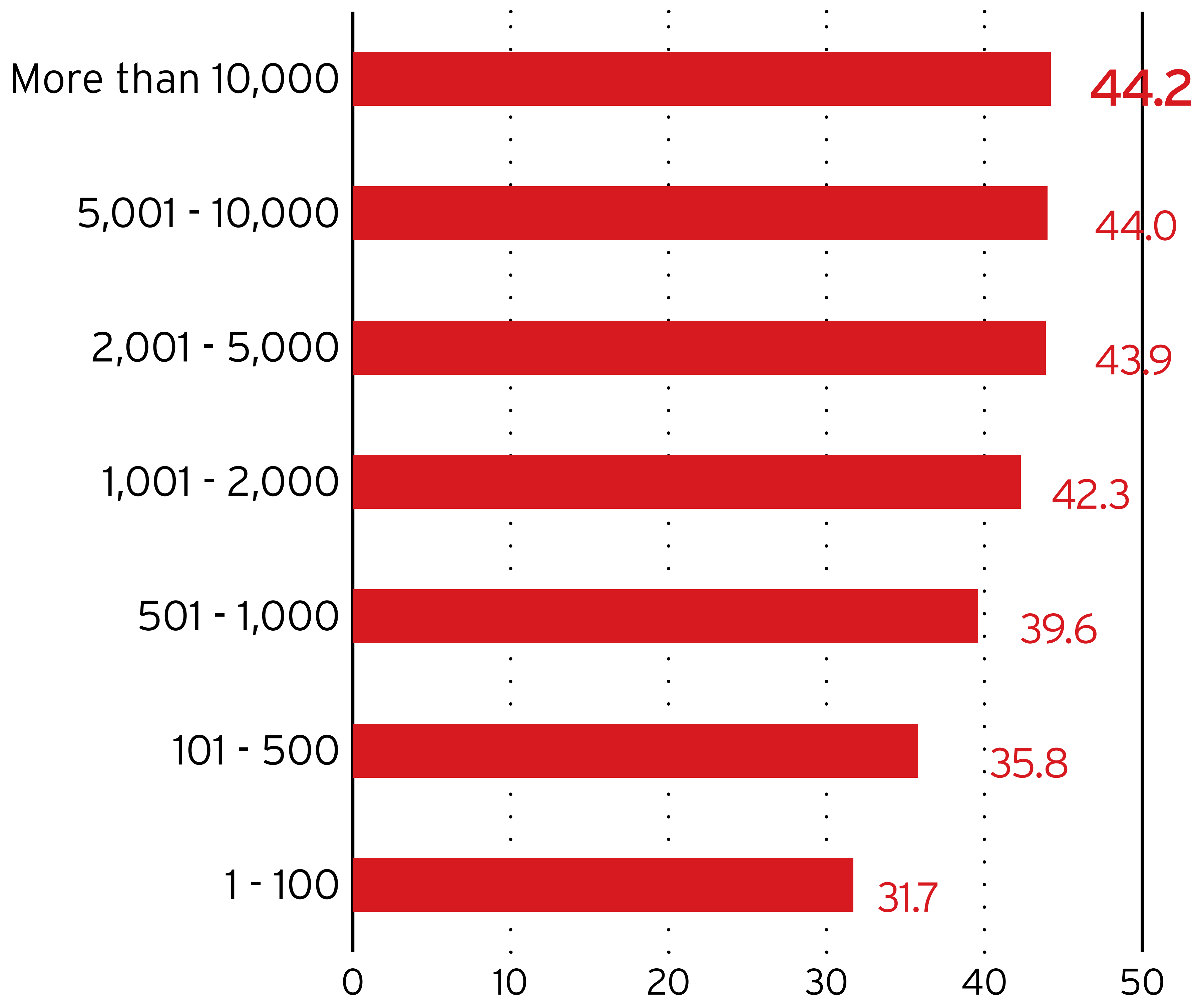
The average CRI of enterprises in the agriculture and construction industries could be affected by the use of legacy systems that might not be adequately secured. The increase in use of automated machinery and IoT devices improve operations in both sectors but also introduces new vulnerabilities with the expanded attack surface. Third-party vendors and service providers can also introduce additional security risks if those parties have weak cybersecurity measures.

Other sectors involved in the supply chain, such as the energy and transportation sectors, should also shift to a more proactive risk management approach to reduce their overall exposure and make their organizations resilient to attacks.

## Average risk index by company size

Larger enterprises typically have more complex networks; with more employees comes a larger attack surface, and so their respective security operations centers face a more challenging task of patching vulnerabilities, maintaining proper security configurations, and securing endpoints.

But any enterprise, regardless of size, has a complex attack surface as businesses globalize and expand. Attackers thrive on this complexity, and complex defense can be an expensive — but worthy — investment. Trend Vision One simplifies defense by centralizing cyber risk exposure management, security operations, and a robust layered protection to help security operations centers predict and prevent threats, thereby accelerating proactive security outcomes. At the center of the capabilities that Vision One provides is a risk-informed approach that allows enterprises to stay ahead of threats.



(February 2024 - December 2024)

# Risk Events and Detections

In this section, we look at the top detections in our telemetry on risky events, misconfigurations, Extended Detection and Response (XDR) model hits, Security Analytics Engine (SAE) and Endpoint Detection and Response (EDR) hits.

We first present the overall top detections for each category, followed by a breakdown by region and by industry of the top detections that contribute to their corresponding CRI. Overall averages show a 2024 view of risk events and detections. In breaking down the top risk events and detections by region and by industry, we provide a narrower and more recent overview by presenting data from July to December 2024.

It is important to note, however, that the average data presented does not comprise the whole equation that results in each CRI; enterprises belonging to each region and industry are still recommended to do a thorough scan of their systems. With Trend Vision One, SOCs can more easily view a comprehensive breakdown of risk factors that contribute to their specific enterprise's CRI. The platform also helps prioritize which issues need attention, focus resources on critical risks, rank issues based on critical impact, and provide clear actionable guidance so security teams can focus on what matters most, in the context of their organization.

| Overall Top 10 Risky Events | |
|---|---|
| 1 | Risky Cloud App Access |
| 2 | Stale Microsoft Entra ID Account |
| 3 | Sandbox Detected Email Threat |
| 4 | On-Premises AD Account with Weak Sign-In Security Policy - Password Expiration Disabled |
| 5 | Advanced Spam Protection - Policy Violation |

| | Overall Top 10 Risky Events |
|---|---|
| 6 | Data Loss Prevention - Email Violation |
| 7 | Microsoft Entra ID Account with Weak Sign-In Security Policy - MFA Disabled |
| 8 | Microsoft Entra ID Account with Weak Sign-In Security Policy - Password Expiration Disabled |
| 9 | Stale On-Premises AD Account |
| 10 | On-Premises AD Account with Weak Sign-In Security Policy - Password Not Required |

*(Sorted by most detections, February 2024 - December 2024)*

Risky cloud app access continues to top the most detected risky event in enterprise environments. This could be influenced by the continuing transition of organizations to cloud environments, which in turn require cloud adoption and user education, a security measure that might not yet be among companies' priorities.

Other risky events are tied to email risk and user accounts and credential security. Risky events related to email risk include the detection of suspicious email attachments. Emails continue to be a favorite vector for cybercriminals to deliver suspicious payloads; in 2024, the Trend Vision One – Email and Collaboration Protection[9] solution detected and blocked 57 million high-risk email threats, a 27% increase from 45 million high-risk emails detected and blocked in 2023. But email can also be a way to exfiltrate or leak data from the victim: data loss prevention violations ranked top six, which indicates that employees in enterprises are sending emails with content or attachments that contain sensitive information, financial data, or intellectual property without the proper security sensitivity settings.

| Risk Event Counts on Weak Authentication | Total Event Count |
|---|---|
| Microsoft Entra ID Account with Weak Sign-In Security Policy - MFA Disabled | 1,011,628,400 |
| Microsoft Entra ID Account with Weak Sign-In Security Policy - Password Expiration Disabled | 606,548,251 |
| On-Premises AD Account with Weak Sign-In Security Policy - Password Not Required | 413,916,224 |
| Microsoft Entra ID Account with Weak Sign-In Security Policy - Strong Password Disabled | 389,998,623 |

Risky events related to user accounts and credential security suggest that protecting, strengthening, and updating user passwords is not a high priority for a number of enterprises. Enterprises need to prioritize and automate mitigation of identity risk to eliminate breaches in today's boundaryless workplace. Trend Vision One™ - Identity Security[10] can help organizations do some spring cleaning on stale user accounts, which can be exploited by attackers, former employees, or insiders for unauthorized access to sensitive data and the enterprise's network.

| Top Detected XDR Model Hits | |
|---|---|
| 1 | Possible OS Credential Dumping* |
| 2 | Possible Data Encrypted for Impact* |
| 3 | Behavior Monitoring Detection for Built-in Windows Tools |
| 4 | Impair Defenses* |
| 5 | Hacking Tool Detection |

| Top Detected XDR Model Hits | |
|---|---|
| 6 | Targeted Attack Detection |
| 7 | Remote Code Execution via HTTP |
| 8 | Possible Malicious Activity via System Services* |
| 9 | System Binary Proxy Execution* |
| 10 | Webshell Detection |

*(Sorted by most detections, February 2024 - December 2024)*

**Heuristic attribute*

Trend XDR collects and correlates data across multiple security layers like email, endpoint, server, cloud, and network to enable faster threat detection, investigation, and response through advanced analytics and automated analysis.

From this telemetry, we extracted data on the top Security Analytics Engine (SAE) and Endpoint Detection and Response (EDR) detections, which revealed that the top hits are threats that are further along in the infection chain. While this might suggest that attackers are employing more sophisticated defense evasion techniques, enterprises should also maximize tools available to them that can provide early detection of suspicious behavior and activity within their environments. Trend Vision One™ - Endpoint Security[11] provides broad coverage for diverse environments that gives enterprises comprehensive visibility, which enables risk mitigation.

| | Overall Top Vision One Misconfigurations | Maximum Risk Score |
|---|---|---|
| 1 | Web Reputation Settings in Trend Vision One™ - Endpoint Security Not Optimized | 69 |
| 2 | Device Control Settings in Endpoint Security Not Optimized | 65 |
| 3 | Endpoint Security Not Supported | 56 |
| 4 | Predictive Machine Learning Settings in Endpoint Security Not Optimized | 69 |
| 5 | Smart Feedback Settings in Endpoint Security Not Optimized | 65 |
| 6 | Anti-Malware Scanning Settings in Endpoint Security Not Optimized | 68 |
| 7 | Firewall Settings in Endpoint Security Not Optimized | 59 |
| 8 | Behavior Monitoring Settings in Endpoint Security Not Optimized | 69 |
| 9 | Application Control Settings in Endpoint Security Not Optimized | 59 |
| 10 | Vulnerability Protection Settings in Endpoint Security Not Optimized | 65 |

*(Sorted by most detections, July 2024 - December 2024)*

In listing the top detected misconfigurations among Trend Vision One customer environments, we also provide their corresponding maximum risk score, which shows they are on the higher end of medium-risk level. These configuration issues emphasize the need for organizations to enable advanced detection capabilities and behavior monitoring AI and ML technology to improve the ability to detect new threats. Enterprises should maximize tools that provide visibility and help eliminate blind spots with a zero-trust approach to minimize their CRI.

**Overall Top Cloud Misconfigurations**

| | |
|---|---|
| 1 | Non-Compliant AWS Infrastructure Configuration |
| 2 | Non-Compliant Azure Infrastructure Configuration |
| 3 | Non-Compliant Amazon S3 Infrastructure Configuration (Access Control) |
| 4 | Non-Compliant Amazon S3 Infrastructure Configuration (Common Configuration) |
| 5 | Non-Compliant Amazon S3 Infrastructure Configuration (Security Configuration) |
| 6 | Non-Compliant GCP Infrastructure Configuration |
| 7 | Non-Compliant AWS Infrastructure Configuration Revealed by Amazon Inspector Findings |
| 8 | Non-Compliant Amazon S3 Infrastructure Configuration (Amazon Macie Findings) |
| 9 | Non-Compliant Amazon S3 Infrastructure Configuration |

*(Sorted by most detections, July 2024 - December 2024)*

The top detected cloud misconfigurations represent a narrower, but more recent average with data only from July to December of 2024. Our telemetry revealed common issues across various cloud platforms such as AWS, Azure, and GCP. For Non-Compliant AWS Infrastructure Configurations, potential problems could include mismanagement of Identity and Access Management (IAM) policies, security groups, and network access control lists (ACL), as well as risks from unused or excessive permissions. For Amazon S3, various non-compliance issues on access control, common configuration, and security configuration could be related to public read/write settings, overly permissive bucket policies, and lack of encryption and versioning. Enterprises using GCP might also be facing problems with IAM policies and insufficient network security configurations. Meanwhile, Amazon Inspector Findings could mean security issues in workloads and insufficient security assessments.

Regular audits and updates to IAM policies, security groups, and network access controls are essential to prevent unauthorized access. Enterprises should also avoid public access settings, implement strict bucket policies, enable server-side encryption and versioning, and review lifecycle policies and logging mechanisms. Organizations should maximize solutions that enhance visibility on their cloud environments for more effective cloud risk management. Trend Vision One™ - Cloud Security[12] supports operational efficiency by protecting an enterprise's cloud environment from development to deployment, and during operations.

## Risk Events and Detections by Region and by Industry

In breaking down the top risk events and detections, we provide a more recent overview by presenting data from July to December 2024. The following section lists the most detected risky events, XDR model hits, and Vision One misconfigurations from Europe, AMEA, the Americas, and the top five industries with the highest trending average CRI.

## Europe

| | Top Risky Events in Europe | Top XDR Model Hits in Europe | Top Vision One misconfigurations in Europe | Top Cloud Misconfigurations in Europe |
|---|---|---|---|---|
| 1 | Risky Cloud App Access | Possible Disabling of Antivirus Software | Application Control Settings in Trend Vision One™ - Endpoint Security Not Optimized | Non-Compliant AWS Infrastructure Configuration |
| 2 | Sandbox Detected Email Threat | Hacking Tool Detection - Blocked | Device Control Settings in Endpoint Security Not Optimized | Non-Compliant Azure Infrastructure Configuration |
| 3 | Stale Microsoft Entra ID Account | Threat Intelligence Sweeping | File Integrity Monitoring (FIM) Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Access Control) |
| 4 | Advanced Spam Protection - Policy Violation | Possible Spear Phishing Attack via Link | Log Inspection Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Common Configuration) |
| 5 | On-Premises AD Account with Weak Sign-In Security Policy - Password Expiration Disabled | Suspicious Multiple Failed Logons via Windows Event | Firewall Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Security Configuration) |

## AMEA

| | Top Risky Events in AMEA | Top XDR Model Hits in AMEA | Top Vision One misconfigurations in AMEA | Top Cloud Misconfigurations in AMEA |
|---|---|---|---|---|
| 1 | Risky Cloud App Access | Hacking Tool Detection - Blocked | Web Reputation Settings in Trend Vision One™ - Endpoint Security Not Optimized | Non-Compliant AWS Infrastructure Configuration |
| 2 | Stale Microsoft Entra ID Account | Possible Disabling of Antivirus Software | Device Control Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Access Control) |
| 3 | Sandbox Detected Email Threat | Threat Intelligence Sweeping | Behavior Monitoring Settings in Endpoint Security Not Optimized | Non-Compliant Azure Infrastructure Configuration |
| 4 | Microsoft Entra ID Account with Weak Sign-In Security Policy - MFA Disabled | [Heuristic Attribute] Backdoor File Detection | Predictive Machine Learning Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Common Configuration) |
| 5 | Data Loss Prevention - Email Violation | Unknown Threat Detection and Mitigation via Predictive Machine Learning | Endpoint Security Agent Not Supported | Non-Compliant Amazon S3 Infrastructure Configuration (Security Configuration) |

## Americas

| | Top Risky Events in Americas | Top XDR Model Hits in Americas | Top Vision One misconfigurations in Americas | Top Cloud Misconfigurations in Americas |
|---|---|---|---|---|
| 1 | Risky Cloud App Access | Threat Intelligence Sweeping | Web Reputation Settings in Trend Vision One™ - Endpoint Security Not Optimized | Non-Compliant AWS Infrastructure Configuration |
| 2 | Stale Microsoft Entra ID Account | Possible Disabling of Antivirus Software | Endpoint Security Agent Not Supported | Non-Compliant Azure Infrastructure Configuration |
| 3 | Sandbox Detected Email Threat | Hacking Tool Detection - Blocked | Device Control Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Access Control) |
| 4 | Microsoft Entra ID Account with Weak Sign-In Security Policy - Password Expiration Disabled | Unknown Threat Detection and Mitigation via Predictive Machine Learning | Predictive Machine Learning Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Common Configuration) |
| 5 | Advanced Spam Protection - Policy Violation | Possible Spear Phishing Attack via Link | Smart Feedback Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Security Configuration) |

# Agriculture sector

| | Top Risky Events in the Agriculture sector | Top XDR Model Hits in the Agriculture Sector | Top Vision One misconfigurations in the Agriculture Sector | Top Cloud Misconfigurations in the Agriculture Sector |
|---|---|---|---|---|
| 1 | Risky Cloud App Access | Threat Intelligence Sweeping | Web Reputation Settings in Trend Vision One™ - Endpoint Security Not Optimized | Non-Compliant AWS Infrastructure Configuration |
| 2 | Data Loss Prevention - Email Violation | Hacking Tool Detection - Blocked | Intrusion Prevention System (IPS) Settings in Endpoint Security Not Optimized | Non-Compliant Azure Infrastructure Configuration |
| 3 | Advanced Spam Protection - Policy Violation | Cybercrime Malware Mitigation | Anti-Malware Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Access Control) |
| 4 | Stale Microsoft Entra ID Account | Possible Disabling of Antivirus Software | Web Reputation Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Common Configuration) |
| 5 | Microsoft Entra ID Account with Weak Sign-In Security Policy - MFA Disabled | Possible Spear Phishing Attack via Link | Agent Self-Protection Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Security Configuration) |

## Communications industry

| | Top Risky Events in the Communications Industry | Top XDR Model Hits in the Communication Industry | Top Vision One misconfigurations in the Communication Industry | Top Cloud Misconfigurations in the Communications Industry |
|---|---|---|---|---|
| 1 | Sandbox Detected Email Threat | Possible Disabling of Antivirus Software | Application Control Settings in Trend Vision One™ - Endpoint Security Not Optimized | Non-Compliant AWS Infrastructure Configuration |
| 2 | Risky Cloud App Access | Hacking Tool Detection - Blocked | Intrusion Prevention System (IPS) Settings in Endpoint Security Not Optimized | Non-Compliant Azure Infrastructure Configuration |
| 3 | Data Loss Prevention - Email Violation | Threat Intelligence Sweeping | Log Inspection Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Access Control) |
| 4 | Stale Microsoft Entra ID Account | Unknown Threat Detection and Mitigation via Predictive Machine Learning | Activity Monitoring Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Common Configuration) |
| 5 | Advanced Spam Protection - Policy Violation | [Heuristic Attribute] Possible Data Encrypted for Impact | Web Reputation Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Security Configuration) |

## Education sector

| | Top Risky Events in the Education Sector | Top XDR Model Hits in the Education Sector | Top Vision One misconfigurations in the Education Sector | Top Cloud Misconfigurations in the Education Sector |
|---|---|---|---|---|
| 1 | Stale Microsoft Entra ID Account | Threat Intelligence Sweeping | Endpoint Sensor Settings in Trend Vision One™ - Endpoint Security Not Optimized | Non-Compliant AWS Infrastructure Configuration |
| 2 | Risky Cloud App Access | Hacking Tool Detection - Blocked | Anti-Malware Scanning Settings in Endpoint Security Not Optimized | Non-Compliant Azure Infrastructure Configuration |
| 3 | Microsoft Entra ID Account with Weak Sign-In Security Policy - Password Expiration Disabled | Possible Disabling of Antivirus Software | Endpoint Security Agent Not Supported | Non-Compliant Amazon S3 Infrastructure Configuration (Access Control) |
| 4 | Microsoft Entra ID Account with Weak Sign-In Security Policy - Strong Password Disabled | [Heuristic Attribute] Backdoor File Detection | Web Reputation Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Common Configuration) |
| 5 | On-Premises AD Account with Weak Sign-In Security Policy - Password Expiration Disabled | Cybercrime Malware Mitigation | Predictive Machine Learning Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Security Configuration) |

## Energy sector

| | Top Risky Events in the Energy Sector | Top XDR Model Hits in the Energy Sector | Top Vision One misconfigurations in the Energy Sector | Top Cloud Misconfigurations in the Energy Sector |
|---|---|---|---|---|
| 1 | Sandbox Detected Email Threat | Hacking Tool Detection - Blocked | Behavior Monitoring Settings in Trend Vision One™ - Endpoint Security Not Optimized | Non-Compliant AWS Infrastructure Configuration |
| 2 | Risky Cloud App Access | Possible Disabling of Antivirus Software | Predictive Machine Learning Settings in Endpoint Security Not Optimized | Non-Compliant Azure Infrastructure Configuration |
| 3 | Stale Microsoft Entra ID Account | [Heuristic Attribute] Trojan Spy File Detection | Firewall Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Access Control) |
| 4 | Sandbox Detected Cloud App Risk | Unknown Threat Detection and Mitigation via Predictive Machine Learning | Suspicious Connection Service Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Common Configuration) |
| 5 | Advanced Spam Protection - Policy Violation | Threat Intelligence Sweeping | Smart Feedback Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Security Configuration) |

## Insurance industry

| | Top Risky Events in the Insurance Industry | Top XDR Model Hits in the Insurance Industry | Top Vision One misconfigurations in the Insurance Industry | Top Cloud Misconfigurations in the Insurance Industry |
|---|---|---|---|---|
| 1 | Risky Cloud App Access | Possible Disabling of Antivirus Software | Anti-Malware Scanning Settings in Trend Vision One™ - Endpoint Security Not Optimized | Non-Compliant AWS Infrastructure Configuration |
| 2 | Microsoft Entra ID Account with Weak Sign-In Security Policy - MFA Disabled | Hacking Tool Detection | Application Control Settings in Endpoint Security Not Optimized | Non-Compliant Azure Infrastructure Configuration |
| 3 | Sandbox Detected Email Threat | Threat Intelligence Sweeping | Device Control Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Access Control) |
| 4 | On-Premises AD Account with Weak Sign-In Security Policy - Password Not Required | Unknown Threat Detection and Mitigation via Predictive Machine Learning | Smart Feedback Settings in Endpoint Security Not Optimized | Non-Compliant Amazon S3 Infrastructure Configuration (Common Configuration) |
| 5 | Stale Microsoft Entra ID Account | Possible Spear Phishing Attack via Link | Suspicious Connection Service Settings in Endpoint Security Not Optimized | Non-Compliant GCP Infrastructure Configuration |

## Home Network Security Top Events

| Rule name | Rule ID |
|---|---|
| RDP Brute Force Login | 1059803 |
| MISC Bitcoin/LiteCoin/Dogecoin Mining Activity -1 | 1059684 |
| WEB Hikvision Product Web Server Command Injection -1.1 (CVE-2021-36260) | 1139937 |
| TELNET Default Password Login -6 | 1133113 |
| WEB HTTP Invalid Content-Length -2 | 1139797 |
| MISC Cryptocurrency Monero Mining Activity -1 | 1134390 |
| SSH Brute Force Login | 1059418 |
| WEB Remote Command Execution via Shell Script -1.h | 1133253 |
| SMB Microsoft Windows SMB Server SMBv1 CVE-2017-0147 Information Disclosure -1 | 1133710 |
| MALWARE Suspicious IoT Worm TELNET Activity -1 | 1133148 |

*(Sorted by most detections, January – December 2024)*

Apart from our cyber risk management data, our Home Network Security shows security risks within home networks by detecting risky network events occurring in devices connected to home routers; an attack surface worth monitoring in the age of remote work across enterprises. This section covers data from January to December as telemetry for this data set was not affected by the algorithm change and is operated separately.

Our telemetry shows that attackers continue to rely on time-tested techniques to gain an initial foothold into their victim's systems with the top detected event being brute force login. There is also a significant amount of cryptocurrency mining activity that can impact enterprises in terms of information disclosure.

The vulnerability found in Hikvision cameras[13] (CVE-2021-36260[14]) is notably high in the detections list; when this vulnerability is exploited, an attacker can launch a command injection attack by sending messages with malicious commands. Considering that this vulnerability has been around since 2021, enterprises should allot effort into employee cybersecurity and risk education so they can maximize tools to secure their personal and home devices. These devices can be an extension of the enterprise's attack surface if they connect to the organization's network.

C++ - main/Level01.cpp - Moonlight SDK
Animation.h
Animation.cpp
Entity.h
Entity.cpp
EXPORT_SYMBOL(groups_alloc);
void groups_free(struct group_info *group_info)
{
if (group_info->blocks[0] != group_info->s
int i;
for (i = 0; i < group_info->nblocks; i++)
free_page((unsigned long)group_info
}
kfree(group_info);
}
EXPORT_SYMBOL(groups_free);
nblocks = n
No consoles to display at this time...

# Vulnerabilities, Patch, and Response Data

## Top risky CVEs, most detected and unpatched

| | Top riskiest CVEs, most detected and unpatched | NIST Severity Score |
|---|---|---|
| 1 | CVE-2024-21357[15] | 8.1 High |
| 2 | CVE-2024-30086[16] | 7.8 High |
| 3 | CVE-2024-30082[17] | 7.8 High |
| 4 | CVE-2024-30087[18] | 7.8 High |
| 5 | CVE-2024-35250[19] | 7.8 High |
| 6 | CVE-2024-30091[20] | 7.8 High |
| 7 | CVE-2024-30049[21] | 7.8 High |
| 8 | CVE-2024-30084[22] | 7.0 High |
| 9 | CVE-2024-30050[23] | 5.4 Medium |
| 10 | CVE-2024-30037[24] | 5.5 Medium |

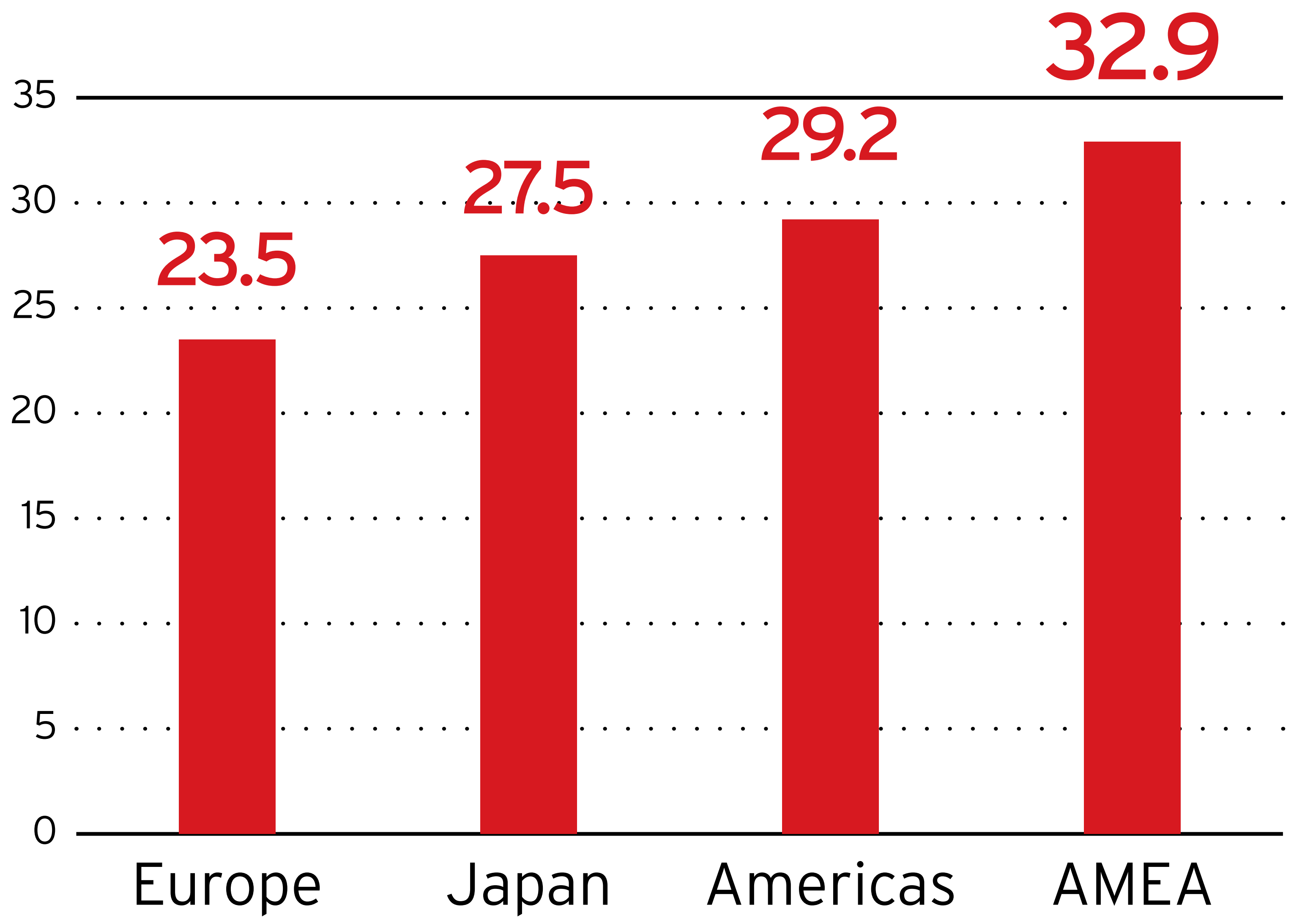
*(Sorted by most detections, February 2024 - December 2024)*

The most detected unpatched vulnerabilities have patches released in the first half of 2024; this emphasizes the need for enterprises to continuously monitor and scan for vulnerabilities and patch as soon as possible.

Most of the top detected vulnerabilities are classified as high severity being related to Elevation of Privilege (EoP), except for the most detected and unpatched among systems, which is a Remote Code Execution (RCE) vulnerability. If successfully exploited, attacks can gain control of enterprise systems, enabling data breaches, system and operational disruption, and major financial loss.

While these vulnerabilities are considered high-risk due to their potential consequences, there have been no confirmed incidents of exploitation for any of them as of writing. Organizations are strongly advised to apply the latest security patches provided by Microsoft to mitigate these vulnerabilities and safeguard their systems from potential threats.

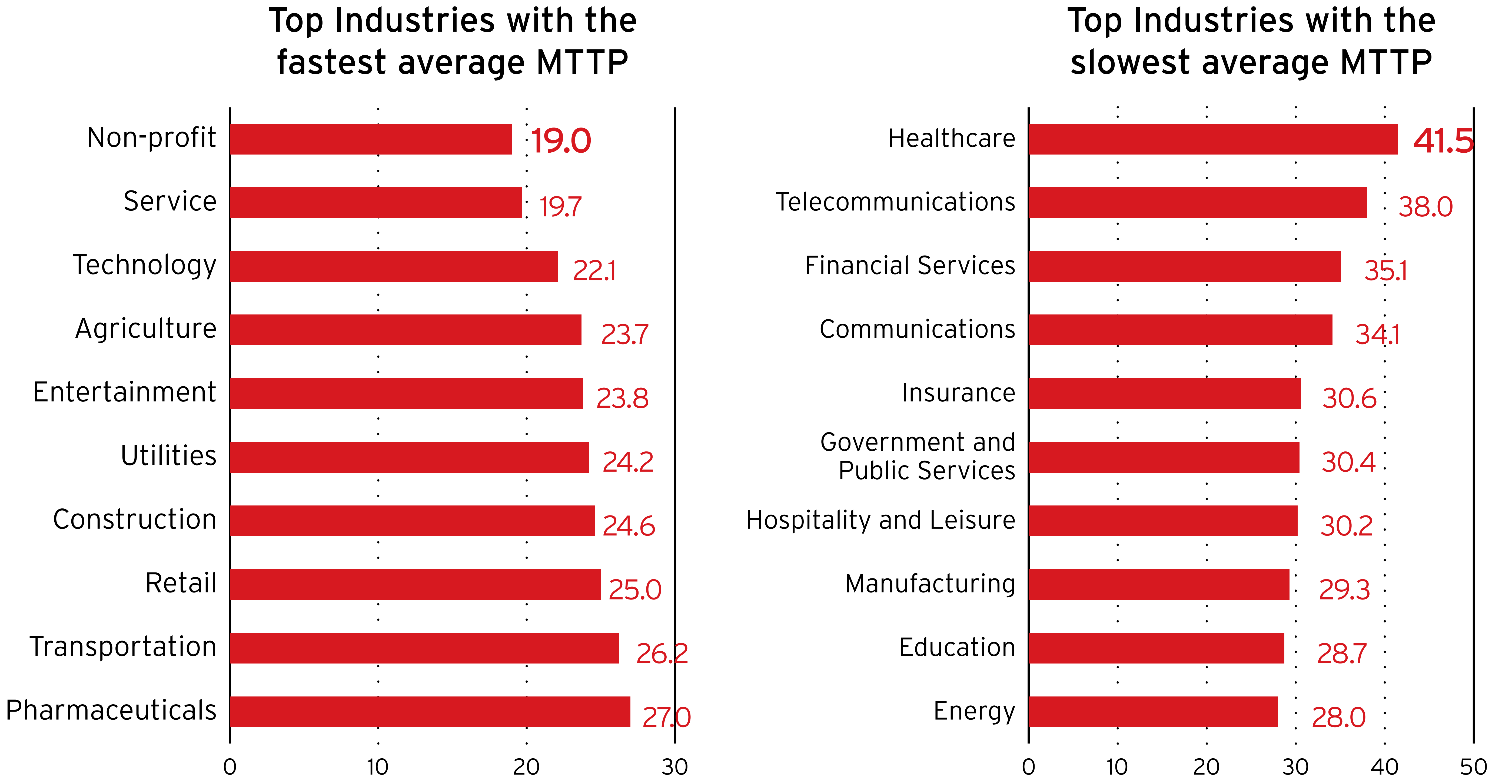
## Average Mean Time To Patch (MTTP) by region



*(Sorted by most detections, February 2024 - December 2024)*

Trend CREM data on mean time to patch shows the average number of days that organizations within a certain category are able to patch vulnerabilities. Europe has the fastest average mean time to patch among regions; the speed with which enterprises patch their vulnerabilities naturally contributes to risk reduction, and therefore a lower CRI as seen in the region's monthly CRI breakdown in the first data section of this report. Japan has the second fastest MTTP, reflecting our telemetry of it having the lowest CRI in 2024. The Americas and AMEA both must improve their MTTP times to help improve their risk indices.

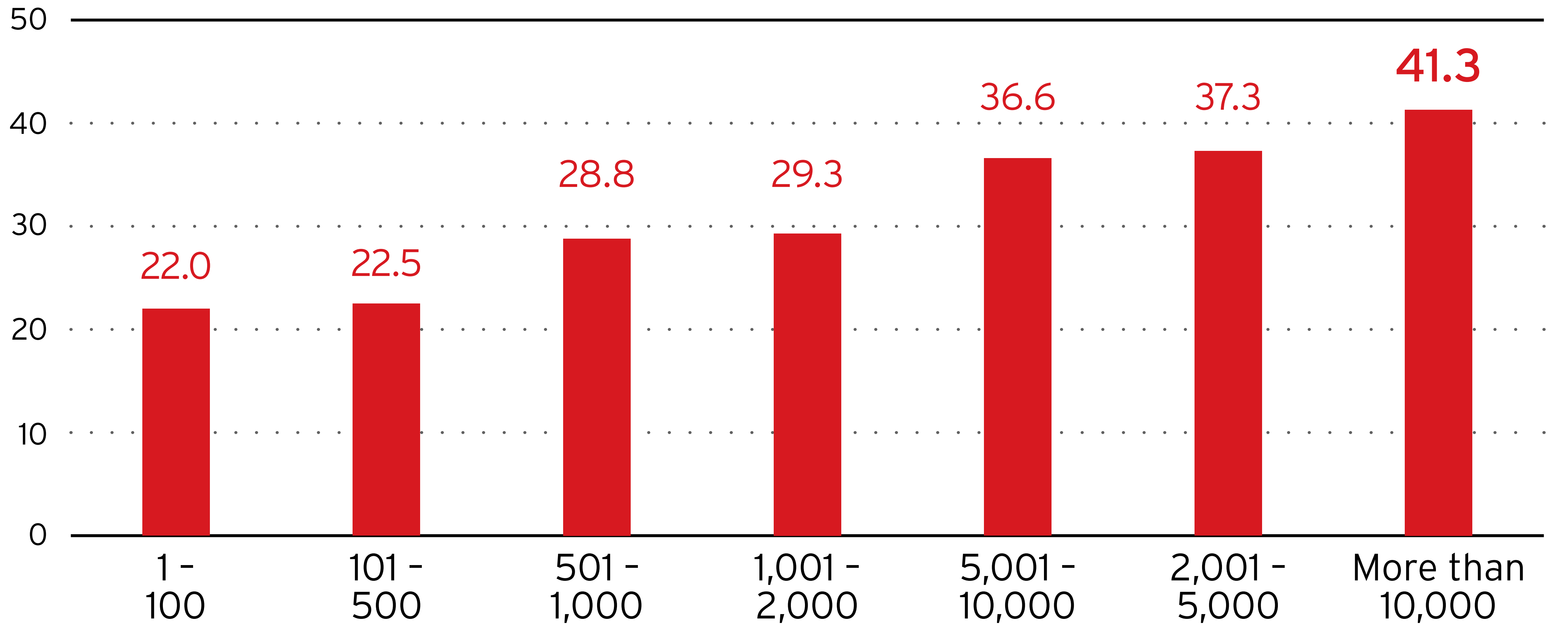
## Average MTTP by industry



*(February 2024 - December 2024)*

Non-profit organizations have the fastest MTTP, followed by the service and technology industries. Other industries, such as the agriculture sector, construction, and transportation industries, also record good average patch time compared to other industries. Their inclusion in the sectors with highest risk indices suggest that their risk could be caused by attack risk factors such as risky or malicious events detected at endpoints and connected applications, or security configuration risk factors.

## Average MTTP by company size



*(February 2024 - December 2024)*

Larger enterprises often operate with more complex networks, which make for a demanding task of patching vulnerabilities. Trend Vision One simplifies this challenge by centralizing cyber risk management, and mitigating risk with automated actions and AI guided remediation that allows security teams to act fast with configurable playbooks that can orchestrate across multiple security controls.

## Overall Top Response Playbooks in Use

| | |
|---|---|
| 1 | Automated Response Playbook |
| 2 | Custom |
| 3 | CVEs with Global Exploit Activity - Internal Assets |
| 4 | CVEs with High or Medium Global Exploit Activity |
| 5 | Risk Event Response |
| 6 | Account Response |
| 7 | CVEs with High or Medium Global Exploit Activity - Internet-Facing Assets |
| 8 | CVEs with Global Exploit Activity - Internet-Facing Assets |
| 9 | Account Exposure - Weak Sign-in Policies, Excessive Admin Accounts, and Stale Accounts |
| 10 | Endpoint Response |

*(July 2024 – December 2024)*

Security playbooks enable automation of a variety of actions, helping reduce workload while speeding up security tasks and investigations. Enterprises can create playbooks from scratch or use templates to create playbooks and customize the settings to suit their specific needs. Depending on the playbook type, they can be designated to run manually, periodically, or automatically in response to a trigger.

The top response playbook is the automated response to Vision One workbench alerts, followed by custom playbooks; enterprises are maximizing both the ready-made AI-powered playbooks and the customization capability of the platform in automating response to XDR alerts. The third and fourth playbooks, as well as the seventh and eighth playbooks, are updated versions of each and making it to the top detected playbooks in use indicate that enterprises recognize the importance of patching vulnerabilities and are focusing on automating their detection.

Account response (top 6 and 9, the former being an updated version of the latter) also made it to the top detected playbooks in use. Despite this, the risk events related to account compromise such as weak sign-in policies and stale accounts are among the top detected risk events specified in an earlier section. While playbooks can guide enterprises in the right direction and alert them on what to prioritize, SOCs must take risk management a step further by maximizing tools available to automate mitigation actions and ensuring compliance beyond the platform through user education and policy implementation.

# External Threat Data Sections

# Notable uses of AI in cybercrime

While most experts agree that the current state of AI cannot generate wholly novel threats, its capabilities can certainly scale existing attack vectors and cost businesses a lot of money. Watch out for these threats, which are made easier to carry out with the use of AI:

## LLM risks[25]

The Open Worldwide Application Security Project (OWASP) released the Top 10 Risk List for LLMs, which includes new additions, such as vector and embedding weaknesses, misinformation, and unbounded consumption, to the list.

## Rogue AI[26]

An artificial intelligence threat that security experts are focusing on in the long-term. Attackers can deploy malicious rogues or subvert AI resources, but rogue AI can also be caused by human error and technology limitations.

## Improved Reconnaissance[27]

After a successful breach, cybercriminals can use AI to pull a vast amount of information from a company to help them identify potential victims. It can also be used for reconnaissance tactics and to expedite the analysis of exfiltrated data, further increasing the scale and severity of cyberattacks.

### Disinformation campaigns[28]

Deepfake content is continuously observed to shape public perceptions. These campaigns range from low-impact misleading information that make the rounds on social media to high-impact and large-scale disinformation campaigns that can affect events such as national elections.

### Pig butchering[29] and virtual kidnapping[30]

Cybercriminals use deepfake technology to manipulate benign photos and videos in extortion schemes, as in pig butchering. Scammers can also use deepfake audio or voice cloning in extortion schemes like virtual kidnapping.

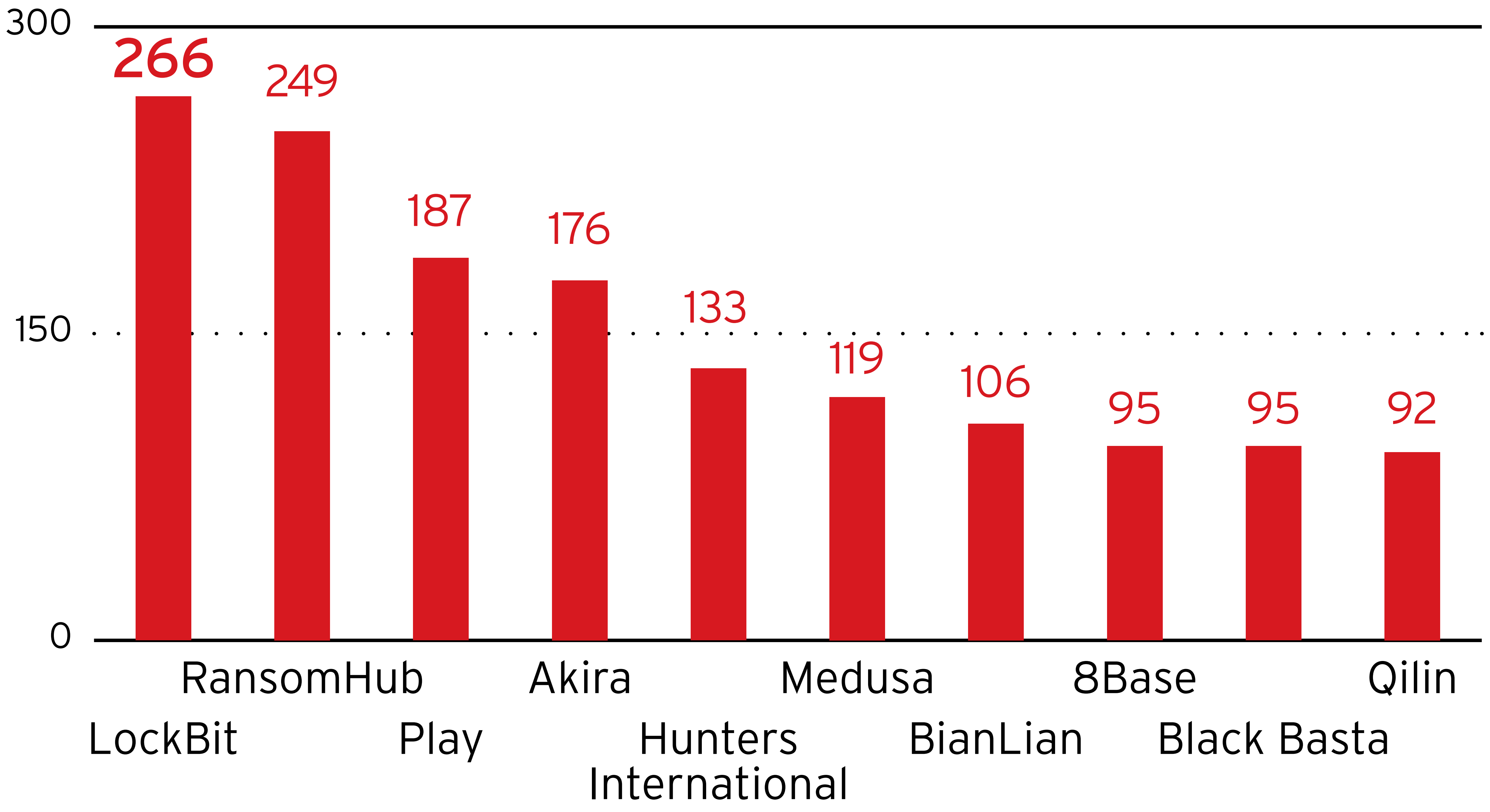
### Intensified phishing schemes and malicious digital twins[31]

Generative AI aids cybercriminals to produce more convincing messages, and to scale operations through automation. Breached and leaked personal information (PII) is used to train LLM, and when deployed in combination with deepfake video and audio they could be used for identity fraud and honey trapping.

While threat actors are making the most of AI, this innovation can be harnessed for improved and more efficient cybersecurity as well. Trend Vision One – AI Security balances enterprises' needs for AI innovation with securing AI initiatives. It uses AI for security and provides security for AI by eliminating blind spots, preventing AI model poisoning, mitigating AI stack vulnerabilities, using AI-generated threat protection, proactive threat mitigation, and advanced threat detection and response. Enterprises will also benefit from its compliance capabilities, as regulatory standards for the use of AI are set by the industry.

# Ransomware

## Top Ransomware Intrusion Sets



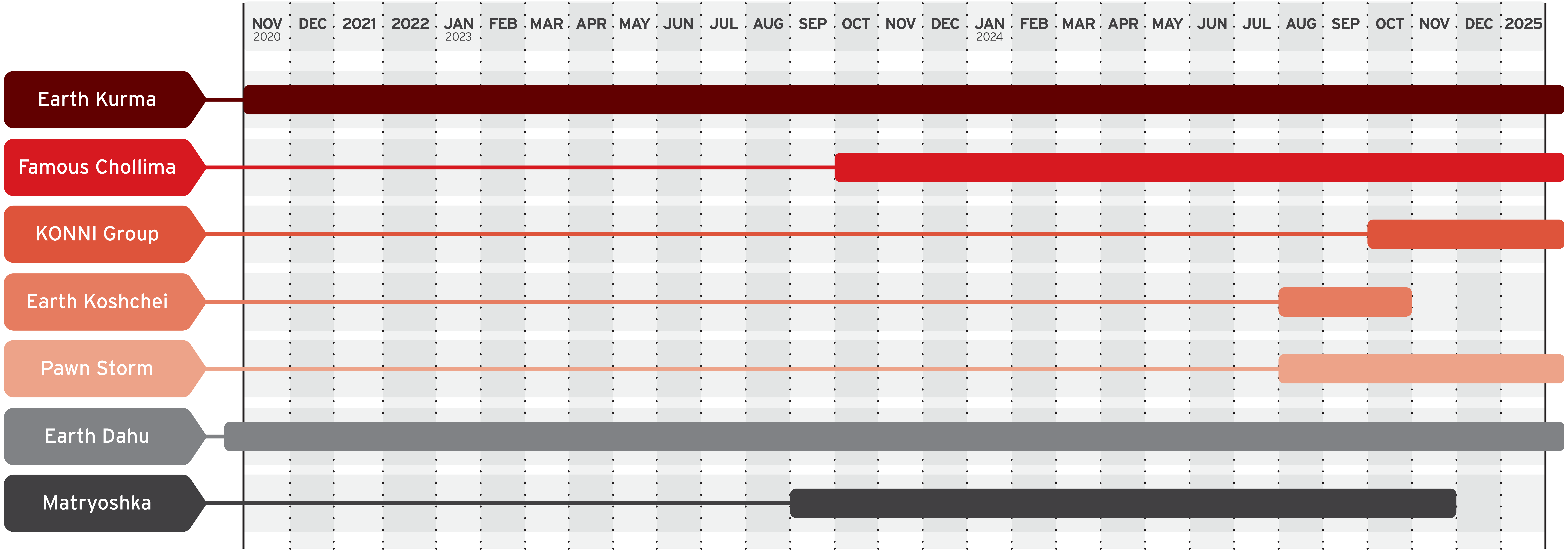
Our monitoring of the cybercriminal underground monitors data uploaded on ransomware groups' leak sites. In the Top Ransomware Intrusion Sets table, "breaches" refer to successful ransomware attacks on enterprises that chose not to pay ransom. This means that the actual number of successful attacks might be higher as some companies might have paid the ransom.

Our leak site monitoring shows that ransomware groups have the most victim enterprises from North America, with 369 successful breaches on companies that did not pay ransom in that region. Leak sites also published 104 successful breaches from enterprises in Europe and 47 from Asia. Companies in retail, wholesale, and distribution make up most of the breaches published in leak sites (13.9%), followed by enterprises from industrial products and services (9.4%). Ransomware groups also published that they have victims from the transportation industry, information technology, and technology industries which make up the top five industries affected by ransomware attacks.

Region and industry rankings on successful ransomware attacks likely reflect more on the resilience against ransomware attacks of enterprises from each region and industry, rather than ransomware group behavior, as they do not target regions or industries specifically. Enterprises can increase their resilience against ransomware attacks by making endpoint sensors work for them. Vision One's Endpoint Security solution provides all-in-one endpoint protection with native threat detection and response, proactive risk mitigation, and centralized visibility to streamline operations and enhance IT security posture.

# Notable APT campaigns

This section includes highlights from the Trend Micro APT Research Report from December 2024 that contains independently collected information, as well as excerpts from publicly available information issued by security vendors or public institutions. Our researchers have analyzed and provided insights on topics that are deemed particularly noteworthy.



## Earth Kurma targets Southeast Asia governments

November 2020 - ongoing

**Targets:**

- Government sectors and government-related telecommunication sectors in the Philippines, Vietnam, Malaysia, Brunei, Thailand

**Motivation:**

- Espionage

- Earth Kurma targets multiple government sectors as well as government-related telecommunication sectors.
- Earth Kurma's primary focus is data exfiltration, with a tendency to leverage public cloud services. The group reuses the same code base from the previous known campaigns to customize their toolsets and can even leverage the victim's infrastructure to achieve their goals. They have customized toolsets like TESDAT and SIMPOBOXSPY, and developed rootkits to cover their tracks like KRNRAT, and MORIYA.

## Famous Chollima exploits job listings to propagate malware

October 2023 – ongoing

**Targets:**

- Developers

**Motivation:**

- Acquisition of foreign currency for arms development, possibly also confidential information theft

- In this campaign, attackers post job listings for system developers for cryptocurrency-related organizations on job sites, along with GitHub URLs of the code they claimed to be currently using. Additional payloads are downloaded along with the code packages. If a cryptocurrency wallet is found in the developer's environment, Famous Chollima steals it, and if executed in a corporate environment, they infiltrate the company and steal confidential information as needed.

## Attacks targeting Russia potentially by KONNI Group

October 2024 – ongoing

**Targets:**

- Russia

**Motivation:**

- Espionage aimed at gathering diplomatic information

- Continued activity from the KONNI group consistently use LNK files. Our recent investigation reveals decoy PDF files with metadata that can be linked to APT37 attacks in the past. The same decoy files seem to target Russians, as they contain text in Russian.

## Earth Koshchei's rogue RDP campaign

August - October 2024

**Targets:**

- Governments, military organizations, think tanks, cybersecurity companies, IT and cloud providers, academic researchers, and other Ukrainian targets

**Motivation:**

- Espionage

- Earth Koshschei (Midnight Blizzard, APT29) launched yet another massive spear-phishing campaign that used a rogue Remote Desktop Protocol (RDP) attack methodology; it involves an RDP relay, a rogue RDP server and a malicious RDP configuration file. This attack gives partial control of victim machines to the attacker, potentially leading to data leakage and malware installation.

## Clipboard and reCAPTCHA abuse attributed to Pawn Storm

August 2024 - ongoing

**Targets:**

- Ukranian government organizations

**Motivation:**

- Espionage

- This campaign saw the use of a web page mimicking reCAPTCHA's bot prevention mechanism as a point of entry. The site used JavaScript to place a malicious PowerShell command in the clipboard and prompted the user to press Windows + R, followed by Ctrl + V, and then the enter key, to execute the clipboard contents under the guise of a reCAPTCHA screen. Additionally, in September, CERT-UA observed emails exploiting a vulnerability in Roundcube (CVE-2023-43770). In both attacks, the infrastructure *mail[.]zhblz[.]com (203[.]161[.]50[.]145)* was used, and were attributed to Pawn Storm.

## Earth Dahu abuses TryCloudFlare

Ongoing

**Targets:**

- Ukrainian central and local government and military organizations

**Motivation:**

- Espionage, particularly military intelligence activities

- Earth Dahu is observed to use remote template injection, drop compressed files from HTA and executing LNK files within them using *mshta.exe* to run resources via TryCloudFlare as C&C, and execute resources on the HTAC2 also using *mshta.exe*.

## Matyoshka campaign related to the US presidential elections

September 2023 - November 2024

**Targets:**

- US, Ukraine, Europe

**Motivation:**

- Disinformation and influencing public opinion

- This campaign is characterized by the creation and dissemination of videos and images that misuse the logos of major media outlets, spread primarily through Telegram and X (formerly Twitter). Fact-checking organizations and media outlets have also reported receiving emails with links to this content.

## Chinese threat actor targeting sensitive industries

September 2023 - November 2024

**Targets:**

- Manufacturing, technology and other industries in Austria, Italy, Argentina, Kazakhstan, France, Philippines, Israel, Czech Republic, Spain, and Turkey

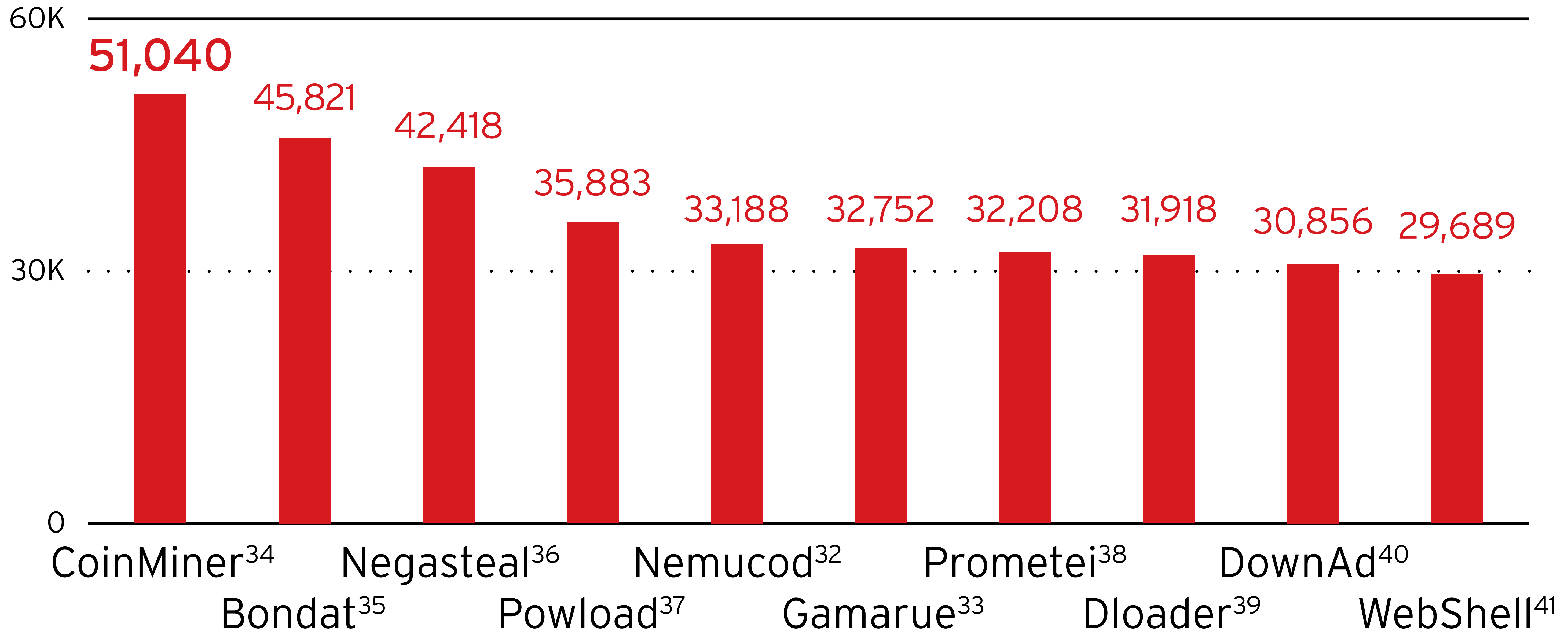
**Motivation:**

- Possibly intellectual property theft

- In November 2024, we had two incident response cases in Europe with similar C&C and TTPs, suggesting a single threat actor behind both operations. Both incidents involved Shadowpad, a malware family used by advanced Chinese threat actors performing espionage. In both cases, a malicious DLL was sideloaded by legitimate executables signed by SentinelOne, Microsoft and Nvidia. We could not attribute with high confidence these incidents to a known threat actor as of writing but found low confidence links to Teleboyi.

# Malware

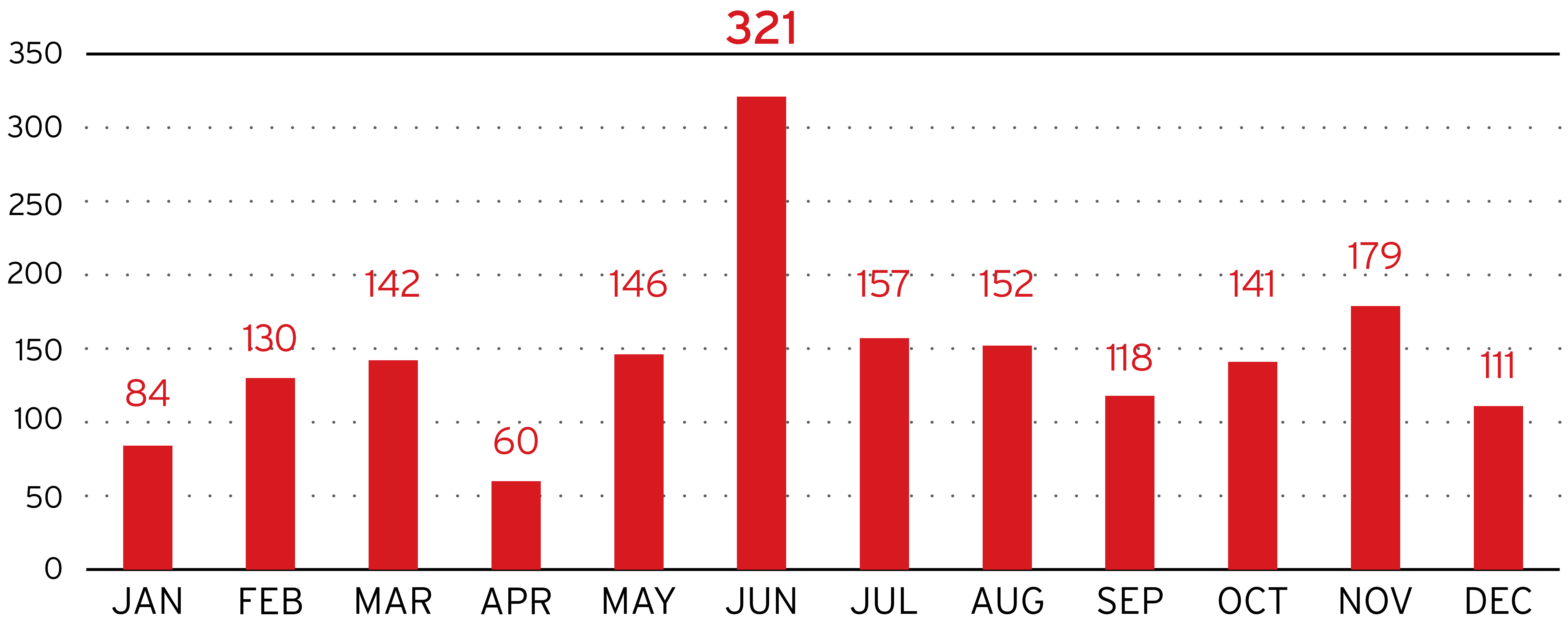
## Top malware families

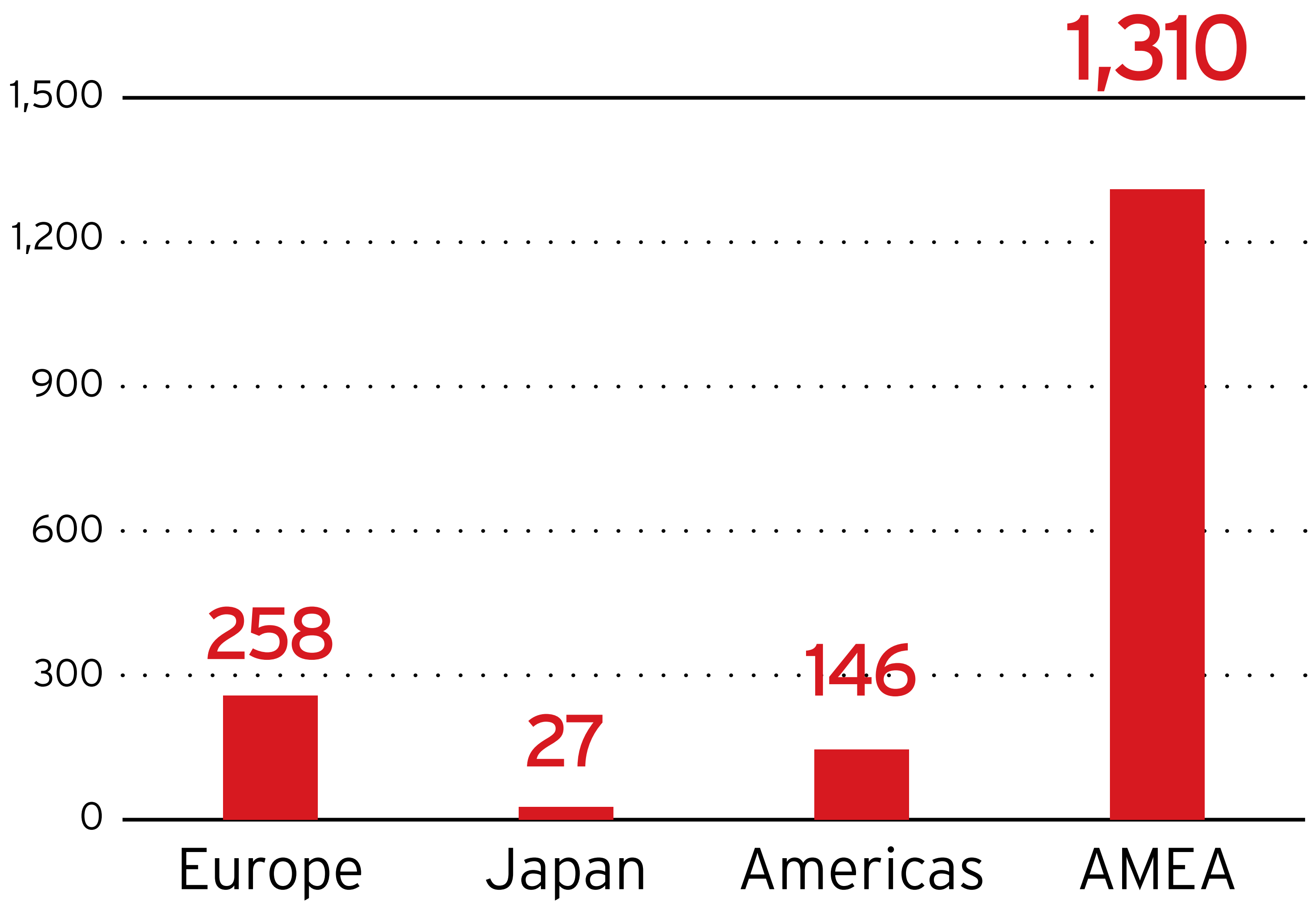


This section shows the top detected malware families in Trend customer environments. Trend Vision One – Endpoint Security provides prevention and protection capabilities across every stage of the attack chain. Industry-leading intrusion prevention empowers enterprises to mitigate known but unpatched threats, predict if files are malicious, and detect indicators of attack before they get a chance to execute.

# ZDI

## Total vulnerabilities and monthly breakdown



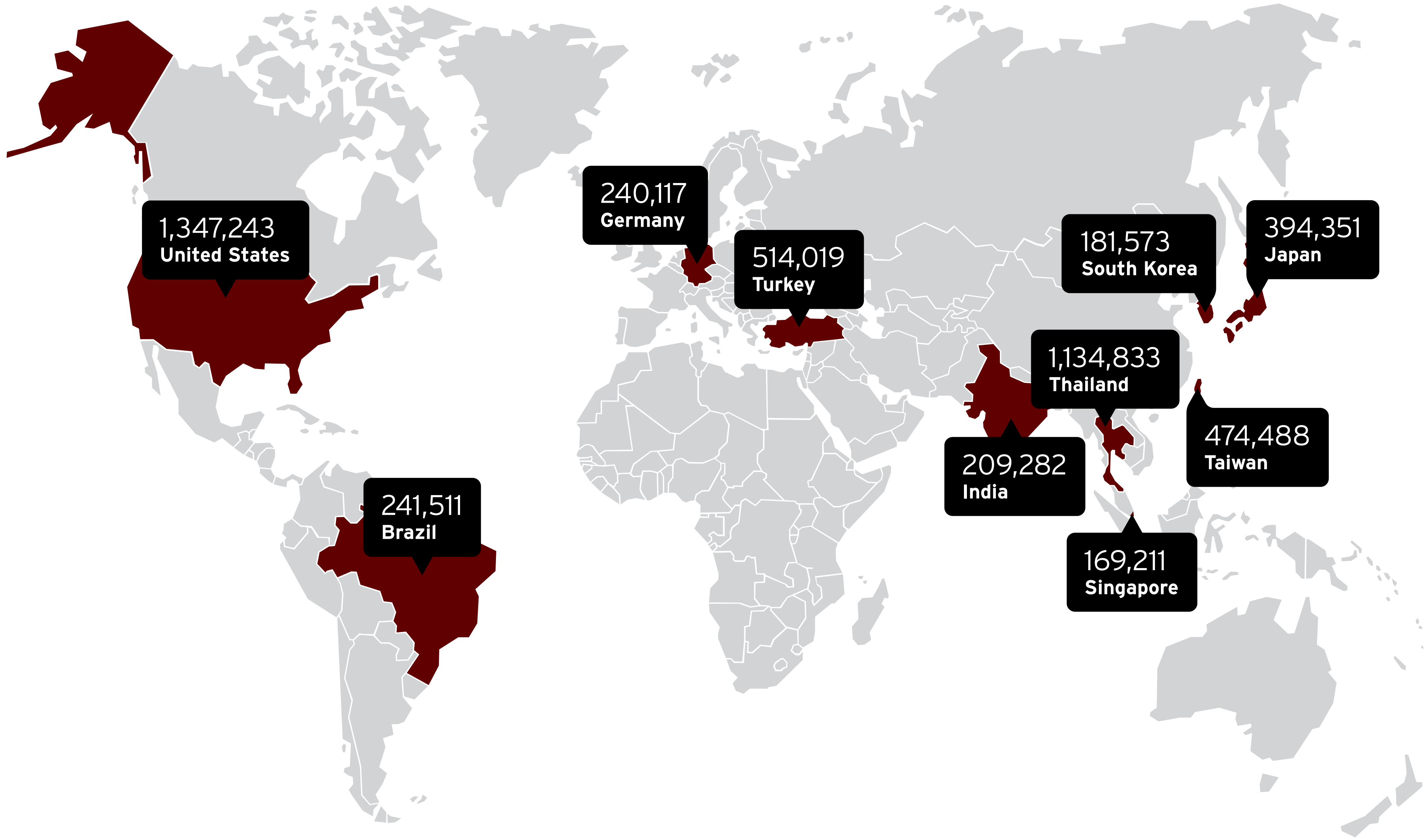


Trend Zero-Day Initiative is the world's largest agnostic bug bounty program. Our ZDI data represents the number of vulnerabilities discovered and reported by independent researchers and shared with ZDI. ZDI then shares the findings with affected software vendors, including major companies like Microsoft and Adobe.

Our ZDI monitoring shows an increase in the use of zero-day exploits (a vulnerability exploited before a patch is made available) by ransomware groups. Prior to 2020, the use of zero-day exploits by ransomware groups was extremely rare, but there have been 59 zero-day exploits leveraged by ransomware attacks since then. It's possible that ransomware attacks have become profitable enough that groups can now pay for zero-days instead of relying on N-day exploits (vulnerabilities exploited after a patch is available). The lack of alternative markets might also be an influence, in that exploit developers lean more toward taking their wares to underground auctions.

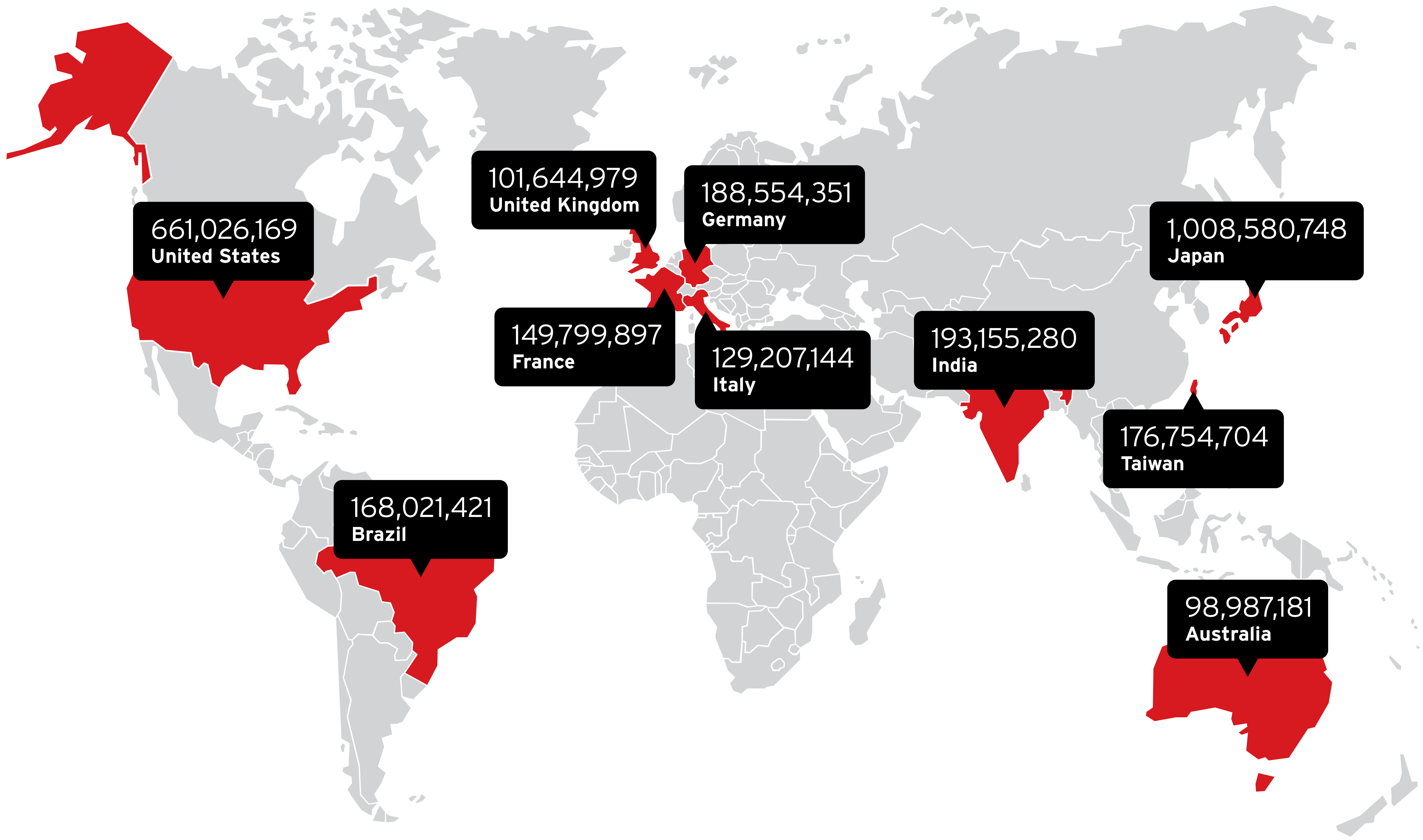
# External threat monitoring heatmap

## Top countries with the most ransomware attacks



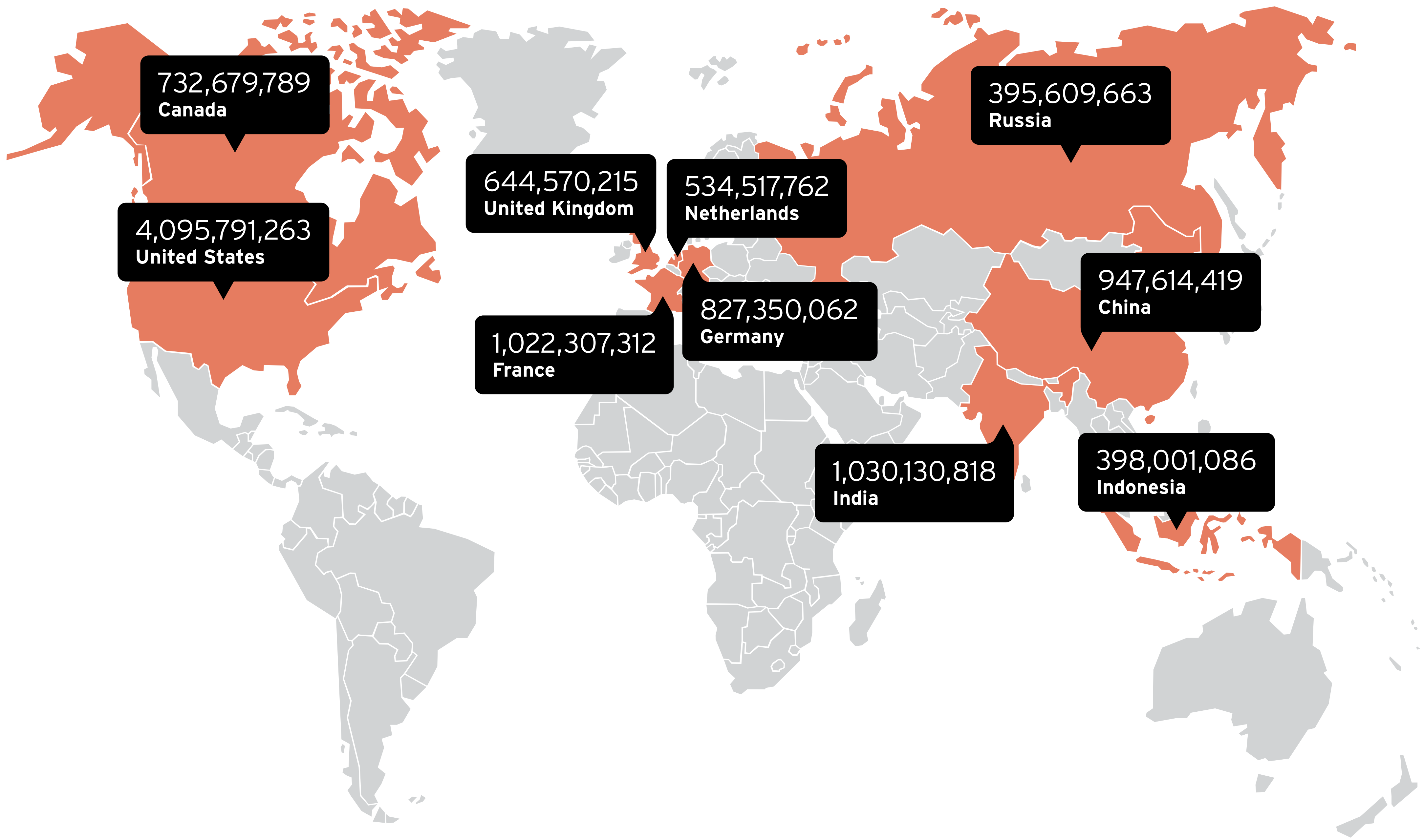
This heatmap presents the regions and countries that our telemetry tracked as having the most ransomware threat activity. Figures in each map represent ransomware threats that have been detected and blocked by our sensors. It's important to note that cybercriminals do not target any country or region specifically. However, these numbers show areas that should take extra precautions to make enterprise systems more resilient against ransomware attacks.

# Top countries with the most malware detections



This heatmap presents the regions and countries that our telemetry tracked as having the most malware threats detected and blocked by our sensors. It's important to note that cybercriminals do not target any country or region specifically. However, these numbers show areas that should take extra precautions to make enterprise systems more resilient against malware attack campaigns.

# Top countries with the most detected email threats



This heatmap presents regions and countries where our telemetry tracked email threats originated from. Email threats detected by our sensors deployed globally scan for their originating IP addresses and reveal where they come from.

# From Reactive to Proactive

A risk-based approach to cybersecurity will shift an enterprise's strategy from being reactive to proactive. By identifying the weaknesses in the defenses and by understanding how cybercriminals are using these exposures to their benefit, enterprises can take the necessary countermeasures to create a more secure defense before the inevitable next cyberattack happens. When an enterprise recalibrates to be more proactive, it can make its time and resource allocation more efficient even as it expands and demands more security coverage.

Trend's Cyber Risk Exposure Management enables teams to uncover risks and thereby thwart attacks by prioritizing mitigation actions to lower organizational risk exposure. Its use of AI empowers security teams to swiftly predict, anticipate, and detect threats with state-of-the-art cybersecurity solutions. Looking at the trends in the past year's risk indices and contributing risk factors extracted from our Cyber Risk Exposure Management data and threat intelligence, enterprises are recommended to do the following:

1. Optimize security settings to maximize product features and be alerted on misconfigurations, vulnerabilities, and other risks. Leverage native sensors or utilize third-party sources to build a comprehensive view of your attack surface.

2. When a risky event is detected, contact the device and/or account owner to verify the event, and investigate the event using the Vision One Workbench. Utilize the Vision One Workbench search function to find more information about the event or check the event details on product management server.

3. Inventory stale accounts to delete inactive and unused ones. Disable risky accounts, or reset their passwords with strong ones, and enable multi-factor authentication (MFA).

4. Apply the latest patches or upgrade the version of applications regularly.

5. Apply the latest patches or upgrade the operating system version regularly.

Adopt a risk-based approach to anticipate threats, strategize resource allocation, tailor security measures, and enhance situational awareness with the continuous discovery, assessment and mitigation of an enterprise's IT ecosystem. By identifying high, medium, and low risk components of the attack surface, organizations can create an action plan to prevent attacks before they even happen and lower their overall risk in the near, medium, and long term.

# Endnotes

1 Trend Micro. (n.d.). *Trend Micro*. "Cyber Risk Exposure Management". Accessed on Mar. 21, 2025, at: Link.

2 Trend Micro. (n.d.). *Trend Micro*. "One Platform". Accessed on Mar. 21, 2025, at: Link.

3 Trend Micro. (n.d.). *Trend Micro*. "XDR (Extended Detection and Response)". Accessed on Mar. 21, 2025, at: Link.

4 Trend Micro. (February 10, 2025). *Trend Micro*. "From Vulnerable to Resilient: Cutting Ransomware Risk with Proactive Attack Surface Management". Accessed on Mar. 21, 2025, at: Link.

5 Trend Micro. (n.d.). *Trend Micro*. "Trend Vision One Risk Index Overview". Accessed on Mar. 21, 2025, at: Link.

6 Trend Micro. (n.d.). *Trend Micro*. "More Than a Number: Your Risk Score Explained". Accessed on Mar. 21, 2025, at: Link.

7 Digital Operational Resilience Act. (n.d.). *Digital Operational Resilience Act*. "Official Website". Accessed on Mar. 21, 2025, at: Link.

8 European Commission. (n.d.). *Digital Strategy - European Commission*. "Cyber Resilience Act". Accessed on Mar. 21, 2025, at: Link.

9 Trend Micro. (n.d.). *Trend Micro*. "Email and Collaboration Security". Accessed on Mar. 21, 2025, at: Link.

10 Trend Micro. (n.d.). *Trend Micro*. "Identity and Access Management". Accessed on Mar. 21, 2025, at: Link.

11 Trend Micro. (n.d.). *Trend Micro*. "Endpoint Security". Accessed on Mar. 21, 2025, at: Link.

12 Trend Micro. (n.d.). *Trend Micro*. "Hybrid Cloud Security". Accessed on Mar. 21, 2025, at: Link.

13 CISA. (Sep. 28, 2021). *Cybersecurity & Infrastructure Security Agency (CISA)*. "RCE Vulnerability in Hikvision Cameras (CVE-2021-36260)". Accessed on Mar. 21, 2025, at: Link.

14 NIST. (Sep. 22, 2021). *National Institute of Standards and Technology (NIST)*. "CVE-2021-36260 Detail". Accessed on Mar. 21, 2025, at: Link.

15 NIST. (Feb. 13, 2024)". *National Vulnerability Database (NVD)*. "CVE-2024-21357". Accessed on Mar. 21, 2025, at: Link.

16 NIST. (June 11, 2024). *National Vulnerability Database (NVD)*. "CVE-2024-30086". Accessed on Mar. 21, 2025, at: Link.

17 NIST. (June 11, 2024). *National Vulnerability Database (NVD)*. "CVE-2024-30082". Accessed on Mar. 21, 2025, at: Link.

18 NIST. (June 11, 2024). *National Vulnerability Database (NVD)*. "CVE-2024-30087". Accessed on Mar. 21, 2025, at: Link.

19 NIST. (June 11, 2024). *National Vulnerability Database (NVD)*. "CVE-2024-35250". Accessed on Mar. 21, 2025, at: Link.

20 NIST. (June 11, 2024). *National Vulnerability Database (NVD)*. "CVE-2024-30091". Accessed on Mar. 21, 2025, at: Link.

21 NIST. (May 14, 2024). *National Vulnerability Database (NVD)*. "CVE-2024-30049". Accessed on Mar. 21, 2025, at: Link.

22 NIST. (June 11, 2024). *National Vulnerability Database (NVD)*. "CVE-2024-30084". Accessed on Mar. 21, 2025, at: Link.

23 NIST. (May 14, 2024). *National Vulnerability Database (NVD)*. "CVE-2024-30050". Accessed on Mar. 21, 2025, at: Link.

24 NIST. (May 14, 2024). *National Vulnerability Database (NVD)*. "CVE-2024-30037". Accessed on Mar 21, 2025, at: Link.

25 Gennai Security Project. (Nov. 17, 2024). *Gennai Security Project*. "OWASP Top 10 for LLM Applications 2025". Accessed on Mar. 21, 2025, at: Link.

26 AI Team. (Aug. 15, 2024). *Trend Micro*. "Rogue AI: Part 1". Accessed on Mar. 21, 2025, at: Link.

27 Nada Elrayes. (Sep. 26, 2024). *Trend Micro*. "Countering AI-Driven Threats with AI-Powered Defense". Accessed on Mar. 21, 2025, at: Link.

28 Trend Micro. (Sep. 19, 2024). *Trend Micro*. "The Illusion of Choice: Uncovering Electoral Deceptions in the Age of AI". Accessed on Mar. 21, 2025, at: Link.

29 Trend Research. (n.d.). *Trend Micro*. "Unmasking Pig Butchering Scams and Protecting Your Financial Future". Accessed on Mar. 21, 2025, at: Link.

30 Craig Gibson, Josiah Hagen. (June 28, 2023). *Trend Micro*. "How Cybercriminals Can Perform Virtual Kidnapping Scams Using AI Voice Cloning Tools and ChatGPT". Accessed on Mar. 21, 2025, at: Link.

31 Trend Micro. (Dec. 16, 2024). *Trend Micro*. "Trend Micro Predicts Emergence of Deepfake-Powered Malicious Digital Twins". Accessed on Mar. 21, 2025, at: Link.

32 Trend Micro. (n.d.). *Trend Micro*. "Coinminer.Win32.MalXMR.Ads". Accessed on Mar. 21, 2025, at: Link.

33 Trend Micro. (n.d.). *Trend Micro*. "LNK_Bondat.SM". Accessed on Mar. 21, 2025, at: Link.

34 Trend Micro. (n.d.). *Trend Micro*. "Tspy_Negasteal". Accessed on Mar. 21, 2025, at: Link.

35 Trend Micro. (n.d.). *Trend Micro*. "Trojan.PS1.Powload.JKP". Accessed on Mar. 21, 2025, at: Link.

36 Trend Micro. (n.d.). *Trend Micro*. "JS_Nemucod.SMC". Accessed on Mar. 21, 2025, at: Link.

37 Trend Micro. (n.d.). *Trend Micro*. "Worm_Gamarue.SMJA". Accessed on Mar. 21, 2025, at: Link.

38 Trend Micro. (n.d.). *Trend Micro*. "Trojan.Win32.Prometei.E". Accessed on Mar. 21, 2025, at: Link.

39 Trend Micro. (n.d.). *Trend Micro*. "Worm.Win32.Dloader.LGA". Accessed on Mar. 21, 2025, at: Link.

40 Trend Micro. (n.d.).*Trend Micro*. "Troj_Downad.E". Accessed on Mar. 21, 2025, at: Link.

41 Trend Micro. (n.d.). *Trend Micro*. "Trojan.PHP.Webshell.SBJKUC". Accessed on Mar. 21, 2025, at: Link.

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, Trend's AI-powered cybersecurity platform protects over 500,000 organizations and millions of individuals across clouds, networks, devices, and endpoints.

Trend's platform delivers advanced threat defense techniques, extended detection and response (XDR), attack surface management (ASM), and integration across the IT ecosystem, including AWS, Microsoft, and Google. This enables organizations to better understand, communicate, and mitigate cyber risk.

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

With 7,000 employees across 70 countries, Trend is singularly focused on cybersecurity by enabling organizations to simplify their connected world. TrendMicro.com.

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy