Trend Research

TREND MICRO™

INTERCEPTING IMPACT

2024 TREND MICRO CYBER RISK REPORT

As cybercriminals shift their attacks with new technologies and strategies, maintaining visibility across the attack surface becomes increasingly challenging. Achieving one-hundred percent security is realistically impossible, and attempting to achieve it will progressively require an exponential amount of resources. It is therefore more productive to prioritize identifying the areas where the likelihood and impact of potential attacks on users and devices is highest.

With this report, Trend Micro shifts towards a risk-based approach in network defense by demonstrating a new technique that calculates risk based on the attack landscape, user exposure, and security configuration. We collect telemetry data from our Attack Surface Risk Management (ASRM) solution in our flagship cybersecurity platform Vision One, combined with our native eXtended Detection and Response (XDR) tools. This report is divided into two sections: the user side that covers risk in assets, processes, and vulnerabilities, and the adversary side, which maps adversary behaviors, MITRE and TTPs. The following data points are based on our telemetry for the first half of 2024 (December 25, 2023, to June 30, 2024).

Differentiating threat data and risk data

THREAT DATA

- Typically measures the prevalence and criticality of threats to users
- Analyzes threats themselves
- Attacks or attack attempts have already happened

RISK DATA

- Factors that contribute to the likelihood and impact of an attack
- Considers threat detection, system configuration, malicious activity, accountand network security, and more
- Provides an insight on the likelihood of attacks or attack attempts

Asset Risk

What is the risk index?

The risk index metrics calculate the overall risk presented to enterprises through various risk organized in a catalog with three categories: Exposure, Attack, and Security Configuration.

Exposure Risk Factors

Risk Factor	Indicator	Description
Account compromise	Leaked account	The detection of a user's account on the dark web
	Suspicious user activity	Activity that may indicate the malicious intent of a user purposefully creating anomalous activity
	Targeted user account	The most at-risk user accounts that exhibited high risk anomalous activities or were specifically targeted by malicious email campaigns during the evaluation period
Vulnerabilities	OS vulnerability	The detection of exploitable operating system vulnerabilities on the endpoint
	Application vulnerability	The detection of exploitable application vulnerabilities on the endpoint
	Cloud VM vulnerability	The detection of exploitable operating system and application vulnerabilities in a cloud VM

Risk Factor	Indicator	Description
Activity and behaviors	Network activity	Anomalous or malicious network activity
	Storage activity	Cloud storage use by the account appears abnormal compared to use by other company accounts
	User activity	Abnormal user behavior patterns or preferences
	Device activity	Abnormal device behavior patterns or preferences
Cloud app activity	Cloud app reputation	Calculated by Trend Micro threat experts based on historical app data, known security features, and community knowledge
System Configuration	Internet-facing asset configuration	Misconfigured settings on public-facing domains and IP addresses
	Cloud infrastructure configuration	Misconfigured settings on cloud infrastructure, such as cloud instances and platforms
	Identity and access configuration	Misconfigured settings on IAM services
	Cloud service configuration	Misconfigured settings on cloud-based applications, software, and services
	Endpoint configuration	Misconfigured security settings on endpoint devices

Attack Risk Factors

Risk Factor	Indicator	Description
XDR detection	Workbench alerts	Detection of malicious or risky events by XDR sensors
	Targeted Attack Detection	Detection of early attack indicators through the scanning of global threat intelligence data
Threat detection	Web threats	The web reputation score of the URLs the user visited or the detection of malicious activity within network traffic
	Email threats	Detection of malicious or anomalous email activity
	Network threats	Detection of malicious activity in monitored endpoint traffic
	Endpoint threats	Detection of events on endpoints that may be malicious
	Mobile device threats	Detection of possible malicious events on mobile devices
	Connected app activity	Detection of possibly malicious events on Office 365 apps (Teams, SharePoint, OneDrive)

Security Configuration Risk Factors

Risk Factor	Indicator	Description
Security Configuration	Endpoint security	This is based on the deployment of Trend Micro products and the status of its settings that include agent and sensor deployment, key feature adoption, license health, and agent versions, plus adoption rates for key product features. Endpoint security considers: • The number of endpoint protection agents deployed throughout your network and on different operating systems throughout your network • The number of endpoint agents running end-of-life, older versions, or the latest version of the agent software • A list of the major protection features offered by agent and sensor products and the total number of endpoints to which each feature is applied, the number of endpoints with outdated patterns for each key feature, and the number of endpoints running up-to-date or outdated component versions; and the respective adoption rate and compliance information of each

Risk Factor	Indicator	Description
	Email security	Email security considers the following: • A list of configured Trend Micro email protection solutions and the number of assets protected, as well as the number of email accounts and domains for which each feature is enabled • A list of your email account assets that have Email Sensor detection enabled • The number of email accounts with and without a policy assigned • The number of email domains that are and are not properly configured
	Network security	Network security considers the following: • The number of Deep Discovery Inspector appliances deployed in your environment • The number of network sensors enabled in your environment • The number of Virtual Network Sensor and Deep Discovery Inspector appliances that are properly connected and the number of appliances that are not receiving traffic • The software version status of your connected Virtual Network Sensor and Deep Discovery Inspector appliances, and the number of appliances using the latest version or outdated versions of components. • The major protection features offered by Virtual Network Sensor and Deep Discovery Inspector, and the number of appliances that have each feature enabled or configured, as well as the detailed adoption rate and compliance information

Calculating risk scores

Trend Vision One 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 impact. The risk scores are calculated individually for every asset, with each score considering asset type and 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. Learn more with our Risk Index Overview and our technical report on how to understand risk score calculations.

Level	Score
Low	0-30
Medium	31-69
High	70-100

Enterprise expansion full speed ahead, challenging the traditional approaches to security as SOCs catch up

Average risk index by region, company size, and industry

Overall figures show that enterprises average at medium-risk scores. This is a good indicator of good risk management practice: while companies could still get a high-risk score, they rarely persistently do so or stay within that level, indicating that they continuously monitor their risk score and mitigate as necessary to keep their index low or at least at an acceptable level.

The Americas ranked the highest among regions with an average risk index of 44.6, within the medium risk level. The past year was characterized by vulnerabilities in the region's banking sector. Its critical infrastructure is also being targeted by Volt Typhoon, a hacker group that deploys malicious software that exploits vulnerabilities such as weak administrator passwords, factory-default logins, and devices that have not been updated. Meanwhile, the Latin Americas since 2023 experienced an onslaught of online scams.

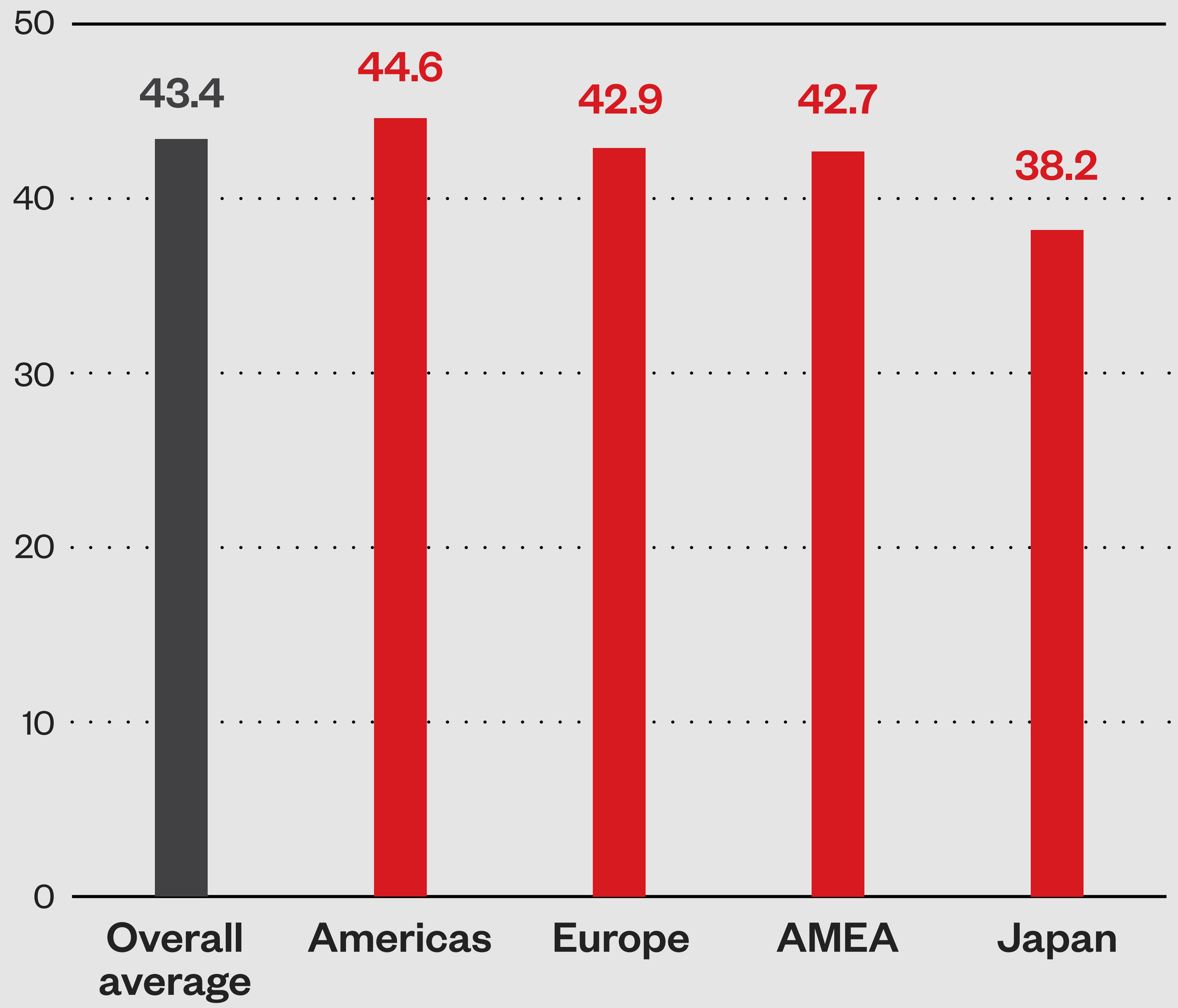

Figure 1. Average risk index by region (1H 2024)

Enterprise expansion full speed ahead, challenging the traditional approaches to security as SOCs catch up

Average risk index by region, company size, and industry

Large enterprises have the highest risk level among company sizes at 48.4, within the medium risk level. This could be attributed to the naturally wider attack surface of companies with more assets to equip over 10,000 employees, making it more difficult to patch and fix misconfigurations. Logically, fewer employees should make it easier for an enterprise to manage its risk levels, but other factors can still hinder this: non-application of best practices, poor cybersecurity hygiene, and lack of user education, among others. But as companies expand, so will the need for systems that simplify and unify security coverage without increasing bandwidth on SOCs and operations.

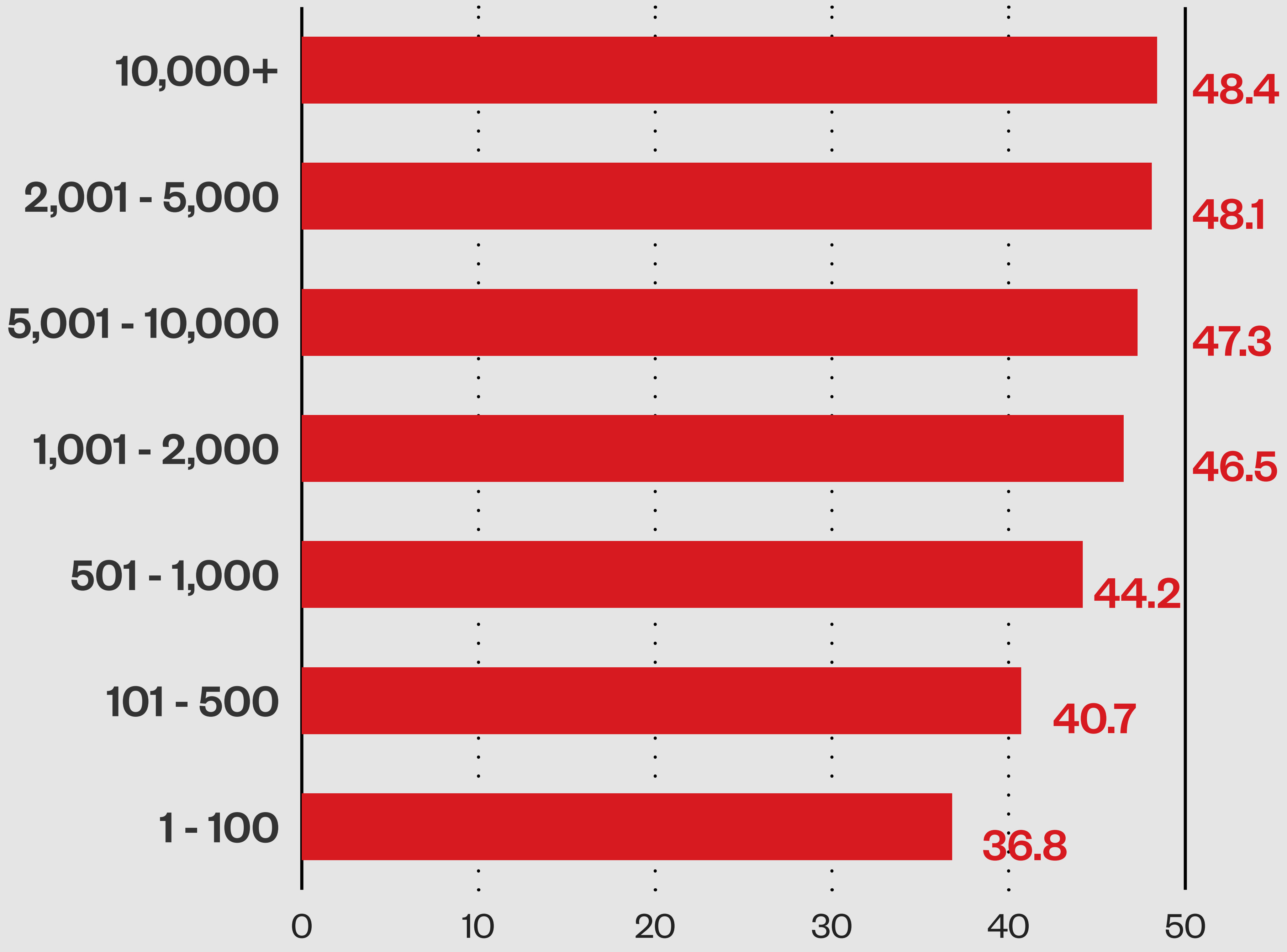

Figure 2. Average risk index by company size (1H 2024)

Enterprise expansion full speed ahead, challenging the traditional approaches to security as SOCs catch up

Average risk index by region, company size, and industry

The aerospace sector has the highest average risk index rating of 59.5, closely followed by the defense industry at 59.4, both within the medium-risk level. Organizations within these industries face a heightened risk of attacks as geopolitical tensions fuel cybercriminal motivations. The aerospace industry as critical infrastructure makes it more attractive and more vulnerable to cyberthreats; sensors on almost every part of aircraft exponentially increase potential attack vectors. The manufacturing and utilities industry should also bolster their security systems, as these sectors are an attractive target for cybercriminals to disrupt supply chains.

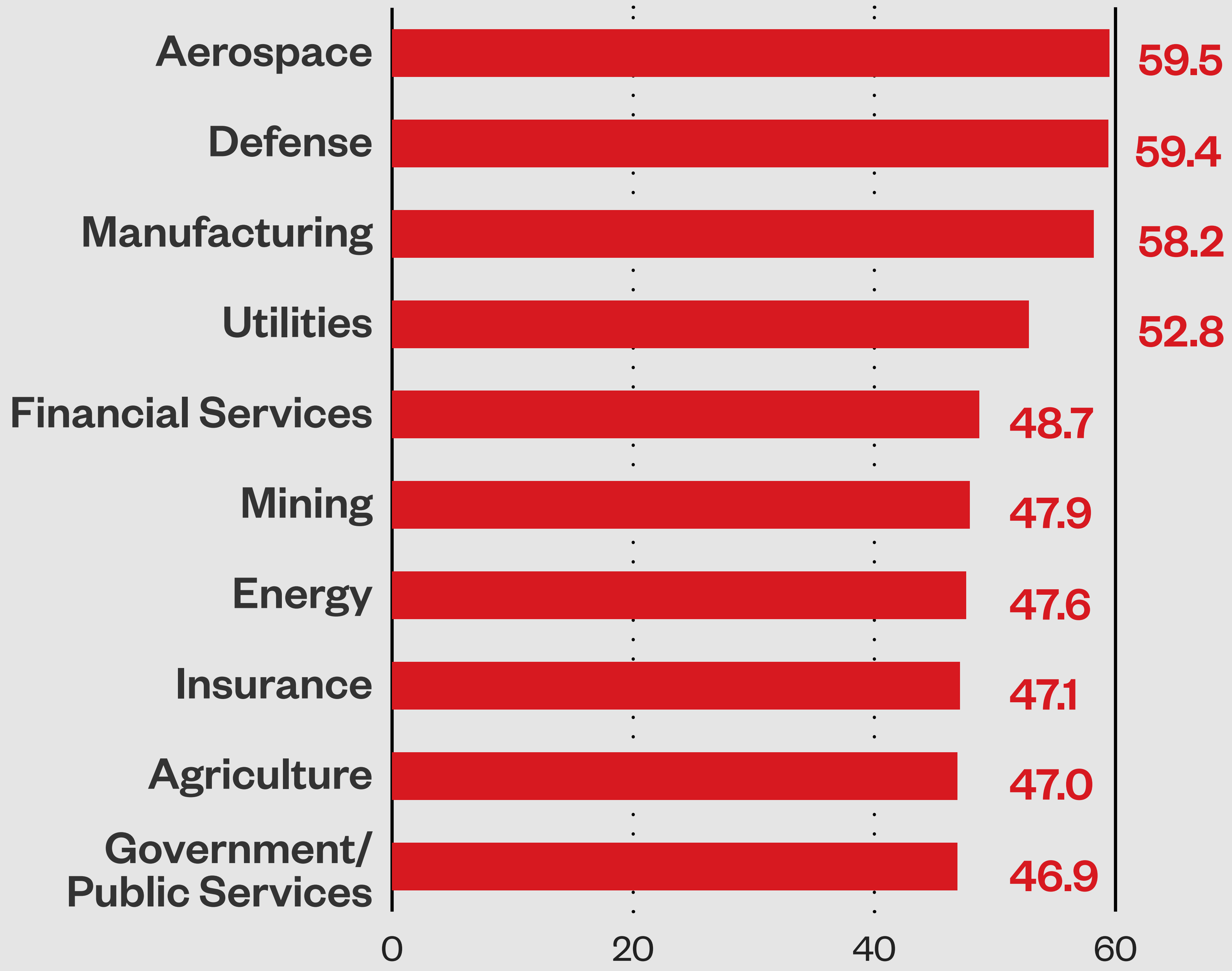

Figure 3. Average risk index by industry (1H 2024)

Secure endpoints with zero-trust approach, educate users on security control compliance and against accessing risky cloud applications

Average high risk asset count by asset type

Our telemetry shows that 3.9% of devices register a high-risk score, emphasizing the need for endpoint security, particularly on security configurations and user education to ensure that risk is minimized on every device under enterprises.

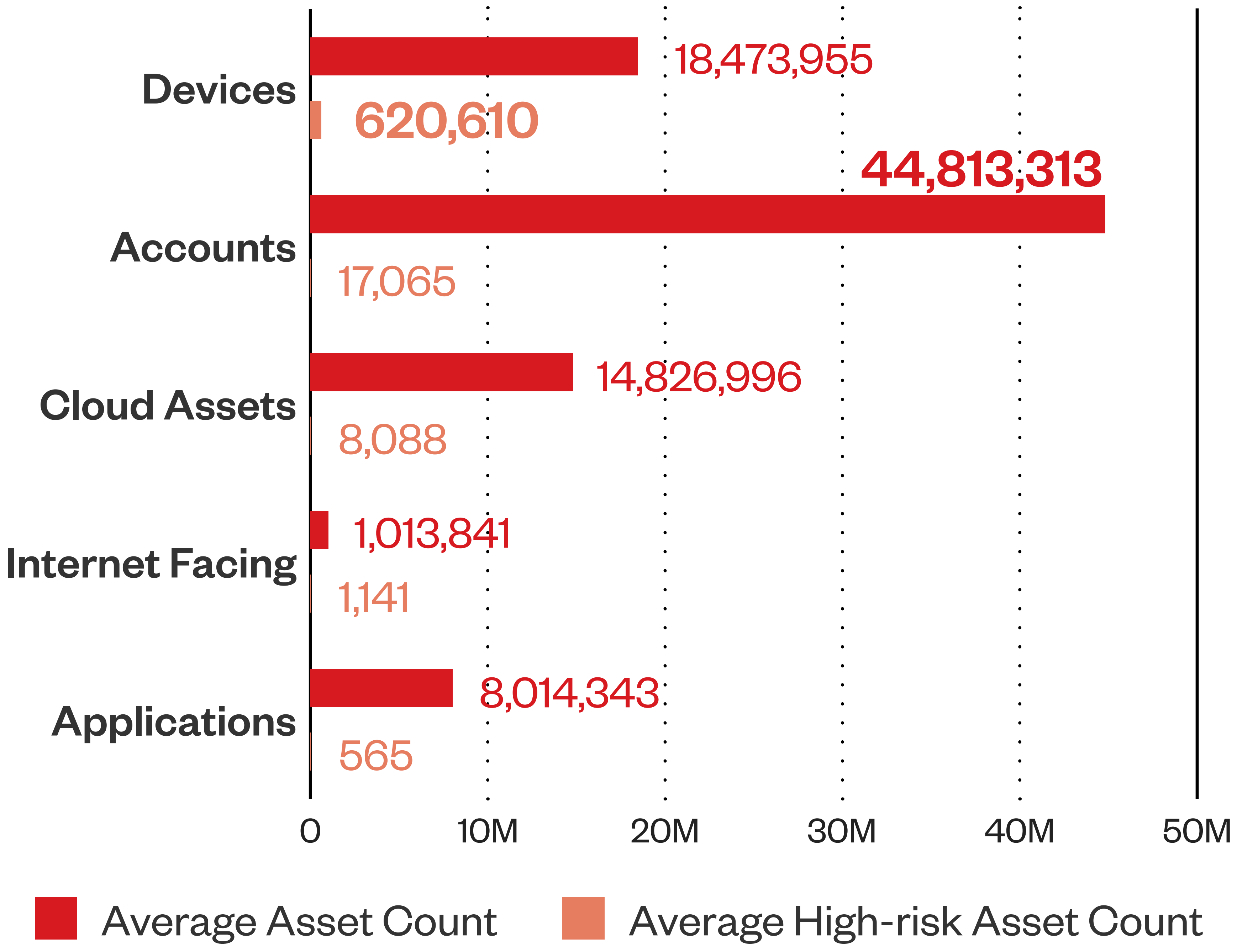

Figure 4. Average high risk asset count by asset type (1H 2024)

Secure endpoints with zero-trust approach, educate users on security control compliance and against accessing risky cloud applications

Accounts

Top 10 events

In the first half of 2024, users accessed cloud applications with a high-risk level based on historical application data, known security features, and community knowledge at an average of 821 million times.

Old and inactive accounts, accounts with disabled security controls, and sensitive data being sent outside the network are other risk events with high event counts. We recommend prioritizing user education, especially as enterprises are increasingly online and rely more on cloud services.

Event name	Average event count
Risky Cloud App Access (Detected: Access to a cloud app with high-risk level)	821,148,651
Stale Microsoft Entra ID Account (Detected: An on-premises Entra ID account with roles inactive for more than 180 days)	131,606,979
Virtual Analyzer - Email Risk (Detected: A high-risk event to an email account and took the configured action)	82,159,848

Event name	Average event count
Data Loss Prevention - Email Violation (Detected: An account sent sensitive data and took the configured action)	30,250,685
On-Premises AD Account with Weak Sign-in Security Policy (Detected: Password Expiration Disabled)	27,016,177
Microsoft Entra ID Account with Weak Sign-In Security Policy - Password Expiration Disabled (Detected: Password expiration disabled)	23,676,849
Advanced Spam Protection - Policy Violation (Detected: An account violated a policy and took the configured action)	21,835,469
Stale On-Premises AD Account (Detected: An on-premises AD account with roles has been inactive for more than 180 days)	18,649,882
Microsoft Entra ID Account with Weak Sign-In Security Policy (Detected: Strong Password Disabled)	17,773,668
On-Premises AD Account with Weak Sign-In Security Policy (Detected: Password Not Required)	15,778,244

Table 1. Top 10 risky events from (1H 2024)

Secure endpoints with zero-trust approach, educate users on security control compliance and against accessing risky cloud applications

Accounts

Average asset count by account type risk level

While devices make up the most high-risk assets, a closer look at our asset analysis on accounts reveals that internal account assets have the highest average asset count with a high-risk score level, and the highest average asset count with a medium-risk score level. Guest accounts follow in terms of highest average asset count with a medium-risk score level. Security teams should check and monitor these types of accounts and look out for misconfigurations and vulnerabilities that could be leveraged by cybercriminals to gain a foothold on an enterprise's network.

Account type	Risk score level	Average asset count
Internal	High	16,091
Guest	High	61

Account type	Risk score level	Average asset count
Internal	Medium	7,473,020
Guest	Medium	1,256,288
Local	Medium	602

Figure 5. Average asset count by account type risk level (1H 2024)

More information:

Trend Micro's Vision One categorizes user accounts into three: guest accounts, local accounts, and internal accounts:

1. **Internal Account:** These are accounts that belong to the enterprise domain and are managed centrally within the organization's infrastructure. They are used by employees and are operated on enterprise-owned devices.

2. **Local Account:** These accounts are not managed by the enterprise domain but are operated on devices owned by the enterprise. Examples include:

    - **Testing and Development:** Developers or IT staff create local accounts on new servers or computers to test configurations or software in an isolated environment.

    - **Kiosk or Public Access Computers:** Machines in public areas, like lobbies or kiosks, use local accounts to provide limited access to specific applications without domain login.

    - **Temporary Access:** Contractors or technicians may use local accounts on devices they need for short-term tasks without accessing the full corporate network.

    - **Legacy Systems:** Older systems that are not integrated into the corporate domain use local accounts for access and administration.

    - **Offline Scenarios:** Devices in environments with limited or no network connectivity use local accounts since they can't communicate with domain controllers.

3. **Guest Account:** These are accounts belonging to external users given limited access to the company's resources. Defined as guests in Azure, they are typically used by partners, vendors, or temporary collaborators.

Secure endpoints with zero-trust approach, educate users on security control compliance and against accessing risky cloud applications

Average managed and unmanaged devices count

As shown in Figure 4, devices have the highest average high-risk asset count at 620,610. Our telemetry reveals that of the total device count, there are more unmanaged devices.

Unmanaged devices are discovered by security solutions as not under Trend Micro control or oversight within an organization’s IT or security management systems; they pose greater risk to enterprises, as they are likely to lack updated endpoint protection. Managed devices, on the other hand, are detected as having installed and enabled Trend Micro endpoint security solutions, actively monitored and maintained by an organization’s cybersecurity team.

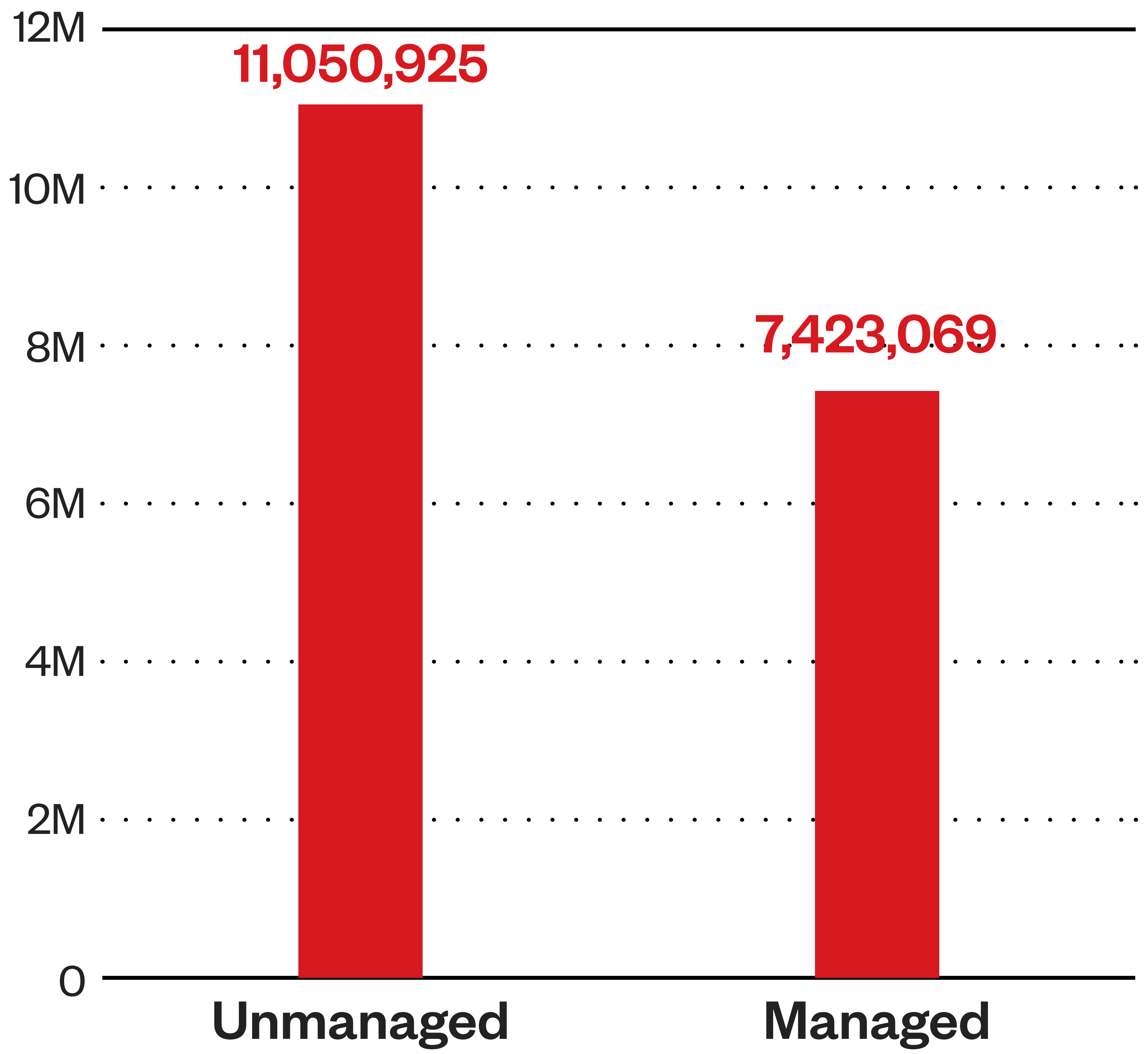

Figure 6. Average Managed and Unmanaged Devices Count (1H 2024)

Maximize tools available, such as enabling advanced detection capabilities and behavior monitoring to identify risk ahead of attacks

Average mean time to patch (MTTP) by region, company size, and industry

Europe is the quickest region to patch vulnerabilities with an MTTP for the first half of 2024 averaging just over 26 days. Meanwhile, the Asia Pacific, Middle East, and Africa region patches vulnerabilities at over 28 days. The Americas has an average MTTP of just over a month, a good turnaround time – but could be better; its MTTP is above the overall average, and this region has the highest average risk index among the regions.

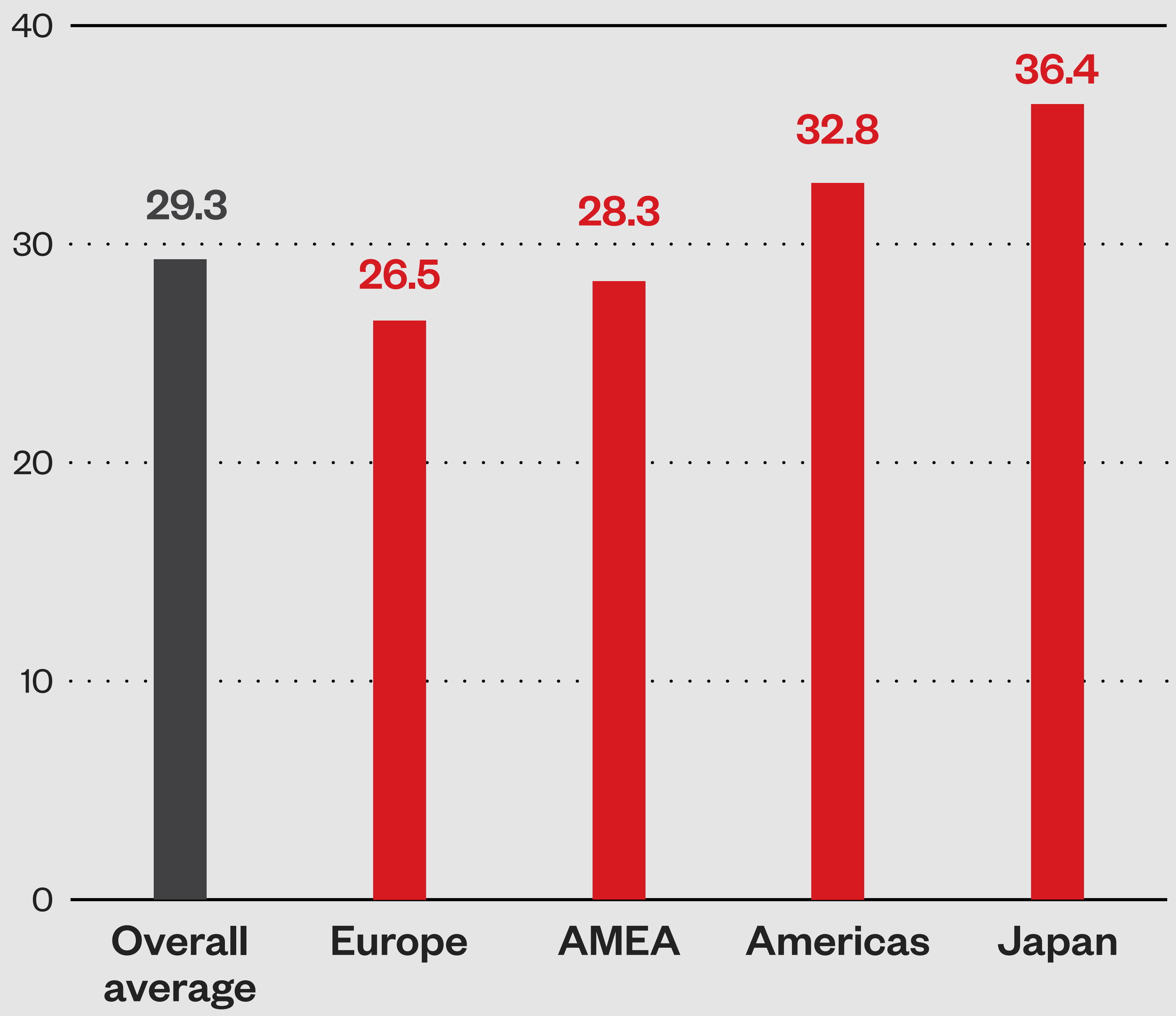

Figure 7. Average MTTP by region (1H 2024)

Maximize tools available, such as enabling advanced detection capabilities and behavior monitoring to identify risk ahead of attacks

Average mean time to patch (MTTP) by region, company size, and industry

Small businesses take the shortest amount of time on average to patch vulnerabilities, which could be attributed to a smaller attack surface that is easier to manage. Interestingly, enterprises with 2,000 to 5,000 employees struggle with patching, taking an average of 39 days to patch, which could be attributed to deprioritizing security as business expands. Large enterprises take the longest average time to patch; their SOCs naturally grapple with a larger attack surface and could also be bogged down by legacy internal applications that slow down patch roll out.

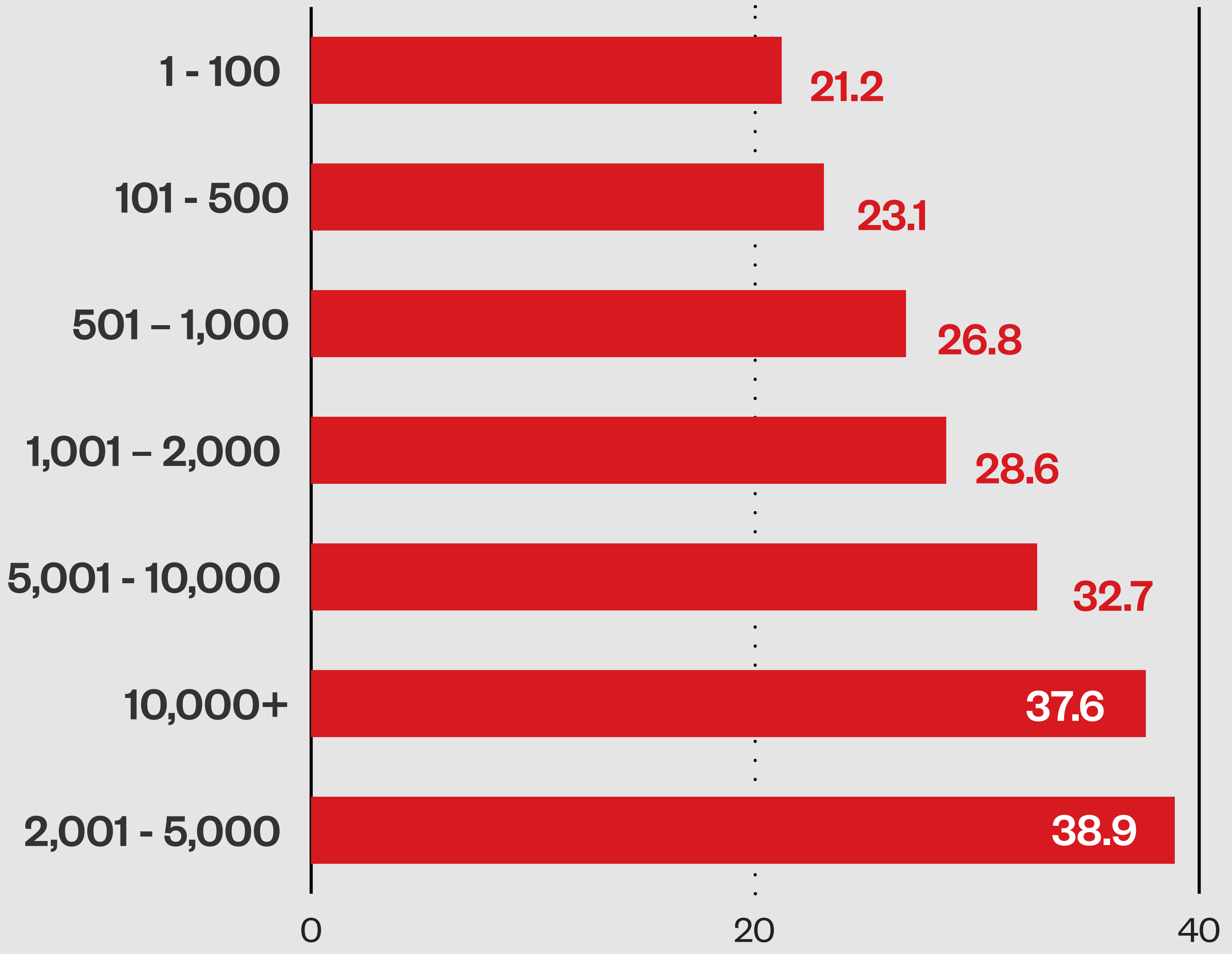

Figure 8. Average MTTP by company size (1H 2024)

Maximize tools available, such as enabling advanced detection capabilities and behavior monitoring to identify risk ahead of attacks

Average mean time to patch (MTTP) by region, company size, and industry

The defense industry takes the shortest average time to patch vulnerabilities at just over a week; an ideal MTTP, as the sector is a hot target due to its critical role in respective national securities, apart from the sector registering an average risk index rating of 59.4. Public safety, security and peace could be affected by how well the defense sector equips itself against cyberattacks. The aerospace sector takes twice as long as the defense industry to patch vulnerabilities; we recommend allotting resources to improve this.

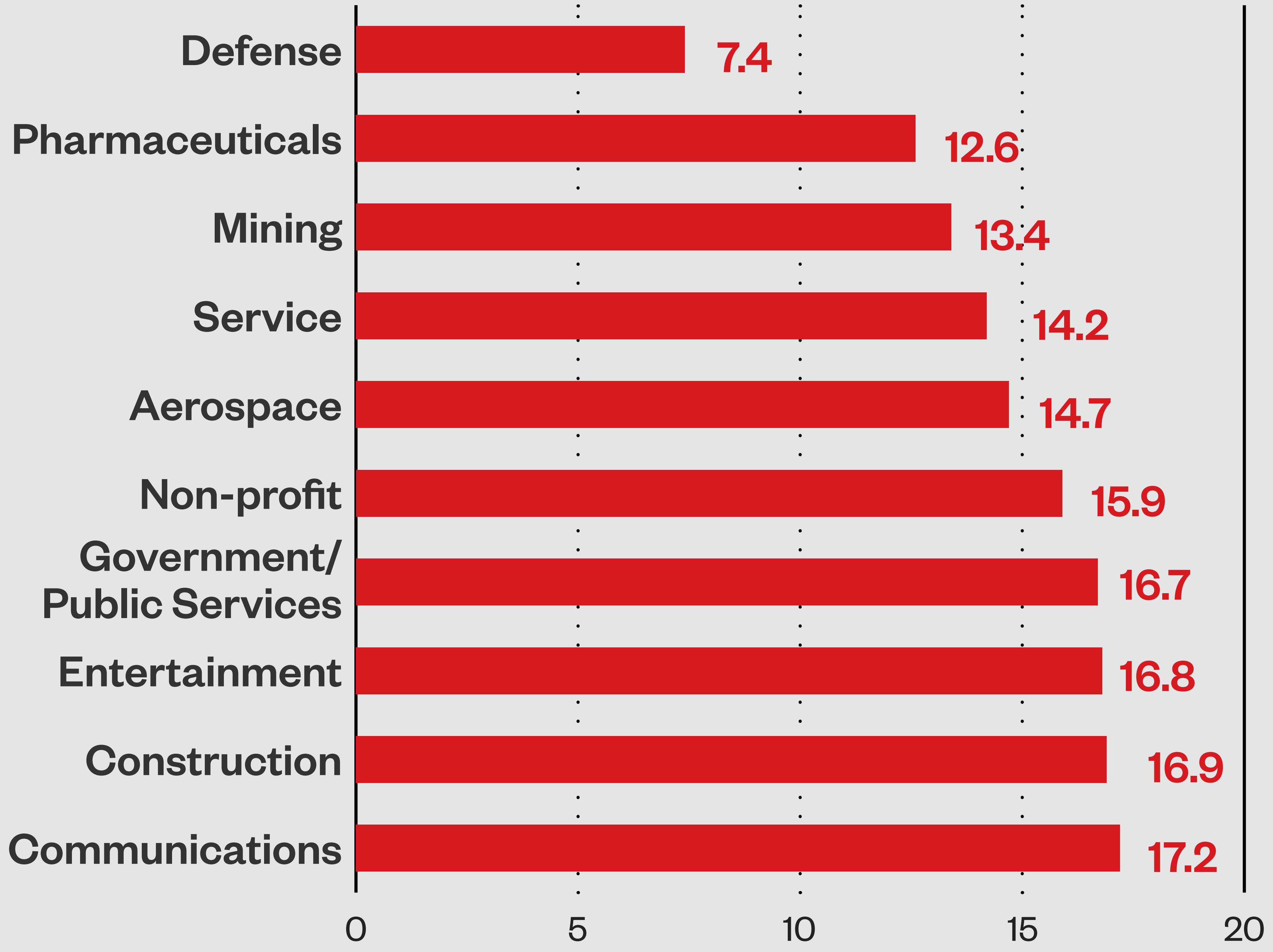

Figure 9. Average MTTP by industry (1H 2024)

Security configuration analysis

Top 10 configurations most widely detected across environments

Configurations issues we spotted in our telemetry emphasize the need for organizations to enable advanced detection capabilities and behavior monitoring in AI and ML technology to improve the ability to detect new threats. The list shows the configurations most widely detected in our customer environments.

1. Vulnerability Protection Settings in Trend Micro Apex One as a Service Not Optimized
2. Suspicious Connection Service Settings in Trend Micro Apex One as a Service Not Optimized
3. Web Reputation Settings in Trend Micro Apex One as a Service Not Optimized
4. Device Control Settings in Trend Micro Apex One as a Service Not Optimized
5. Trend Micro Apex One as a Service Agent Not Supported
6. Predictive Machine Learning Settings in Trend Micro Apex One as a Service Not Optimized
7. Smart Feedback Settings in Trend Micro Apex One as a Service Not Optimized
8. Anti-Malware Scanning Settings in Trend Micro Apex One as a Service Not Optimized
9. Endpoint Sensor Settings in Trend Micro Apex One as a Service Not Optimized
10. Behavior Monitoring Settings in Trend Micro Apex One as a Service Not Optimized

Attack Behavior Analysis

MITRE attack analysis

Cybercriminals continue to find ways to abuse legitimate tools to avoid detection, with Metasploit Meterpreter and DNS tunneling among the top detected MITRE sub-categories in our telemetry. Attackers are also working smarter by targeting the very services that should detect them, such as leveraging PowerShell scripts to interact with Local Security Authority Subsystem Service (LSASS).

Top detected MITRE sub-categories

01 Detection for Metasploit Meterpreter

02 LSASS Access via Suspicious Powershell Parameters

03 High Volume Multiple SSH Connections

04 DNS Tunneling

05 Remote Code Execution via HTTP

06 Powershell AMSI Scan Bypass

07 Possible Renamed TCPDump Execution

08 Screen Capture and Keylogging via Powershell

09 Suspicious Command and Control Connection

10 Behavior Monitoring Detection for Built-in Windows Tools

Exploitable vulnerabilities

Looking at the prevalent CVEs detected and the high exploit vulnerabilities across region and company size, organizations can see specifically see what the attackers are targeting and where they are at risk. A CVE’s risk event risk score is calculated based on the following formula:

$$\text{Risk score} = \sqrt{(\text{likelikood} * \text{criticality})}$$

In this formula, likelihood is the assessment result that considers CVE static attributes, exploit status, report status, threat intelligence, and mitigation measures (such as patch status, IPS enablement, among others). Criticality on the other hand, is the projected business impact of the affected asset.

We recommend identifying if you or your enterprise might be affected by the following vulnerabilities, and to patch as soon as possible.

Exploitable vulnerabilities

Top 10 riskiest CVEs, most detected and unpatched

This list shows the vulnerabilities sorted by how widely they are detected in our customer environments, with the most detected on top.

Vulnerability ID	Summary	CVSS Severity
CVE-2024-30040	Windows MSHTML Platform Security Feature Bypass Vulnerability	8.8 High
CVE-2024-5274	Type Confusion in V8 in Google Chrome prior to 125.0.6422.112 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8 High
CVE-2024-30051	Windows DWM Core Library Elevation of Privilege Vulnerability	7.8 High
CVE-2024-4947	Type Confusion in V8 in Google Chrome prior to 125.0.6422.60 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8 High
CVE-2024-26169	Windows Error Reporting Service Elevation of Privilege Vulnerability	7.8 High

Vulnerability ID	Summary	CVSS Severity
CVE-2023-5217	Heap buffer overflow in vp8 encoding in libvpx in Google Chrome prior to 117.0.5938.132 and libvpx 1.13.1 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8 High
CVE-2023-4863	Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)	8.8 High
CVE-2023-4762	Type Confusion in V8 in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8 High
CVE-2023-6345	Integer overflow in Skia in Google Chrome prior to 119.0.6045.199 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a malicious file. (Chromium security severity: High)	9.6 Critical
CVE-2023-7024	Heap buffer overflow in WebRTC in Google Chrome prior to 120.0.6099.129 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8 High

Table 2. Top 10 riskiest and unpatched CVEs, listed by detection count (1H 2024)

Risk Incidents

CVE-2024-30051

This vulnerability has been observed to be used to deliver the previously notorious banking Trojan and now malware delivery service Qakbot, which throughout the years priori its takedown in 2023 served as an initial infection vector for various ransomware attacks.

CVE-2024-26169

It is believed that cybercriminals linked to the BlackBasta ransomware group have exploited this vulnerability. Investigations revealed that an exploit tool for this CVE was deployed in a ransomware attack attempt, following an initial infection by the DarkGate loader which BlackBasta has been observed to use since the QakBot takedown.

CVE-2023-30040

This vulnerability can be abused by first convincing a user into downloading a malicious file sent via email or instant messenger. When the malicious file is run, cybercriminals can exploit the vulnerability to bypass OLE mitigations in Microsoft 365 and Microsoft Office and then execute their code.

CVE-2023-6345

This vulnerability poses risks ranging from crashes to the execution of arbitrary code (the open source 2D graphics library Skia is also used as a graphics engine by other products like ChromeOS, Android, and Flutter)

CVE-2023-4762

This vulnerability has been observed to be abused to drop a spying tool called Predator on target Android devices in Egypt.

CVE-2023-4863

This vulnerability has been observed to be abused to drop notorious spyware Pegasus on target iPhones. The libwebp buffer overflow leaves all major browsers vulnerable, as libwebp is widely used from Chrome to Linux distributions, and even to applications such as Telegram and 1Password. Microsoft has also released an advisory alerting users that thius vulnerability also impacts Edge, Teams for Desktop, Skype for Desktop, and Webp Image Extensions.

Conclusion and Recommendations

A risk-based approach to cybersecurity will shift an enterprise’s strategy from being reactive to proactive. By recalibrating to be more proactive, an enterprise can make their time and resource allocation more efficient even as it expands and demands more security coverage. Based on our telemetry from for the first half of 2024, we recommend the following best practices to begin improving your enterprise’s risk score:

01

Optimize security settings to maximize product features and be alerted on misconfigurations.

02

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.

03

Disable risky accounts or reset them with a strong password and enable multi-factor authentication (MFA).

04

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

05

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