Trend Micro Warns Devices and Accounts are Highest-Risk Assets

Cyber Risk Report highlights critical vulnerability, offers new ways to prioritize risk management

DALLAS, Sept. 25, 2024 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today urged network defenders to gain greater visibility into risk across their attack surface, after unveiling a new study* which provides granular metrics by region, company size, industry, asset type and more.

To read a full copy of the report, *Intercepting Impact: 2024 Trend Micro Cyber Risk Report*, please visit: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/intercepting-impact-2024-trend-micro-cyber-risk-report

Jon Clay, VP of threat intelligence at Trend Micro:"Trend's cyber risk report shares key insights on where risks are greatest within organizations such as weak security controls, misconfigurations, and unpatched actively exploited vulnerabilities. Shifting towards a more risk-based approach to cybersecurity—discovering the entire attack surface, using AI to calculate the actual risk, and providing mitigating controls advice—allows an organization to improve its cybersecurity posture like never before. This is a game changer for the industry."

The report also uncovered many weak configurations that could lead to compromise, especially around security controls.

Using a risk event catalog, the Trend Vision One™ platform calculates a risk score for each asset type and an index for organizations by multiplying an asset's attack, exposure, and security configuration by impact. An asset with low business impact and few privileges has a smaller attack surface, while higher-value assets with more privileges have a larger attack surface.

The following assets are the most at risk:

- **Devices:** 18 million total devices, with 620,610 classified as high-risk.
- **Accounts:** 44 million total accounts, with 17,065 classified as high-risk.
- **Cloud Assets:** 14.8 million total cloud assets, with 8,088 classified as high-risk.
- **Internet-Facing Assets:** 1 million total, with 1,141 classified as high-risk.
- **Applications:** 8 million total applications, with 565 classified as high-risk.

The number of high-risk devices is much higher than that of accounts, even though there are more accounts in total. Devices have a larger attack surface—i.e., they can be targeted with more threats. However, accounts are still valuable as they can grant threat actors access to various resources.

Elsewhere, the report also found:

- **Americas** has the highest average risk index among regions, with an average risk index rating of 43.4, driven by vulnerabilities in the banking sector and critical infrastructure and the region's attractiveness to profit-driven actors.
- **Europe** is the quickest region to patch vulnerabilities, indicating strong security practices.
- **Mining** has the highest risk score of any vertical due to its strategic position in global supply chains and large attack surface.
- **Pharmaceuticals** are the fastest sector to patch vulnerabilities by several days, reflecting the importance of protecting sensitive data.
- **The top detected risk event** is accessing cloud applications with a high risk level based on historical application data, known security features, and community knowledge.
- **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.

The report also uncovered many weak configurations that could lead to compromise, especially around security control settings.

As the threat landscape continues to evolve, organizations' ability to identify and manage risks is becoming increasingly crucial. The Trend Vision One™ platform, with its integrated Attack Surface Risk Management (ASRM), provides the necessary tools for comprehensive threat visibility and effective risk mitigation.

The following steps are recommended to help mitigate cyber risk:

- Optimize product security settings to get alerts on misconfigurations.
- When a risky event is detected, contact the device and/or account owner to verify the event. Investigate the event using the Trend Vision One™ Workbench search function to find more information about or check event details on the product management server.

management server.
- Disable risky accounts or reset them with a strong password and enable multi-factor authentication (MFA).
- Apply the latest patches or upgrade application and operation system versions regularly.

**The report is based on telemetry data from Trend Micro's Attack Surface Risk Management (ASRM) solution in its flagship cybersecurity platform, Trend Vision One™, plus the native eXtended Detection and Response (XDR) tools. It's divided into two sections: the user side covers risk in assets, processes, and vulnerabilities, while the adversary side maps adversary behaviors, MITRE, and TTPs. Data points are based on telemetry from December 25, 2023, to June 30, 2024.*

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's AI-powered cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, Trend's platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 70 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---

https://newsroom.trendmicro.com/2024-09-25-Trend-Micro-Warns-Devices-and-Accounts-are-Highest-Risk-Assets