Zero Trust Comes to Industry's Broadest Cybersecurity Platform

Trend Micro Zero Trust Risk Insights continuously reveals and prioritizes risks for better decision making

DALLAS, Sept. 27, 2021 /PRNewswire/ -- Zero Trust is a term frequently touted but rarely implemented authentically by cybersecurity providers. Trend Micro Incorporated (TYO: 4704; TSE: 4704) is changing that with the full release of its risk insights capability following a beta test with 3,500 enterprises. The industry's broadest Zero Trust risk assessment solution now forms a critical component of Trend Micro's unified cybersecurity platform.

A comprehensive understanding of risk is the foundation for effective security prioritization and automatic access control decision making with Zero Trust. Many other vendors that claim to employ Zero Trust overlook this vital component in their own security philosophy. Trend Micro gives customers a complete understanding of their risk so security teams can make informed decisions and implement effective solutions rather than simply exchanging one piece of cybersecurity infrastructure for another.

"Some of the downsides of digital transformation projects are legacy security systems causing issues and an almost unmanageable expansion of complexity," said Joel Stradling, Research Director European Security & Privacy, IDC. "To compound this, the threat landscape is increasingly sophisticated making defense strategies similarly complex. Information is king, and Trend Micro's Zero Trust Risk Insights gives CISOs better visibility into an organization's security risk, which in turn helps organizations shed several layers of management complexity and achieve a stronger security posture."

Built on Trend Micro's complete cybersecurity platform, the service is designed to continually assess the risk of identities, devices, and cloud applications using telemetry across endpoint, email, cloud, networks, and SaaS applications. That risk insight is used to automatically detect, block, or remediate issues before a connection is completed. Customers also benefit from continuous security posture assessment and complete insights without requiring additional apps or agents.

"This new solution adds further telemetry and visibility of connections across the entire IT environment to truly inform SOC teams," said Wendy Moore, vice president of product marketing at Trend Micro. "The risk and security of users, devices, and apps can be easily seen, issues prioritized in a way unique to Trend Micro's platform capabilities. This is true Zero Trust theory put into product form."

As the evolving threat landscape continues to garner attention amidst high profile security incidents, decision makers at enterprises worldwide are beginning to realize the benefits of a broad Zero Trust solution.

"The challenges we face in securing our infrastructure are only growing more complex," said Chase Renes, System Administrator, Vision Bank. "Understanding our risks and potential vulnerabilities and how attackers will try to exploit them is the foundation of good cybersecurity. Trend Micro provides a complete picture of our security posture and allows us to eliminate or prevent threats before they surface."

Unique benefits of Trend Micro's Zero Trust solution focus on:

- Identity risks: Identifying compromised user accounts and suspicious user activity, such as accessing risky cloud applications or unusual login activity. These might indicate a user account is being abused by an attacker. For example, phishing emails being sent from an internal user is a notable indicator of malicious account abuse.
- Device risks: Identifying suspicious processes, unpatched vulnerabilities, attack techniques and tactics, and misconfigured applications or operating systems. For example, the use of many legitimate tools can be an indicator of an ongoing ransomware attack.

Zero Trust Risk Insights provides a spectrum of overlapping services to ensure a comprehensive understanding of organizational security.

- The vulnerability prioritization takes advantage of Trend Micro's leadership in vulnerability research, including insights from the Zero Day Initiative. It uses global and local threat intelligence on exploit attempts plus vulnerability severity to prioritize which vulnerabilities are critical to apply a prevention rule or patch.
- Visibility into email usage is particularly important for security teams, as phishing activity could indicate that user identities have been compromised.
- Cloud applications visited by users may be unsanctioned or have data sovereignty and privacy concerns. Using a SaaS-based app reputation database, Trend Micro tracks access to risky applications.

To find out more about Trend Micro Zero Trust Risk Insights, please visit:
https://www.trendmicro.com/en_us/business/products/detection-response/zero-trust.html

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 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, the 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 65 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/2021-09-27-Zero-Trust-Comes-to-Industrys-Broadest-Cybersecurity-Platform