Trend Micro Research Finds Misconfiguration as Number One Risk to Cloud Environments

Cybersecurity must be considered at all points of a cloud migration

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), the global leader in cloud security, today released the findings from research into cloud security, which highlights human error and complex deployments open the door to a wide range of cyber threats.

Gartner predicts that by 2021, over 75% of midsize and large organizations will have adopted multi-cloud or hybrid IT strategy.1 As cloud platforms become more prevalent, IT and DevOps teams face additional concerns and uncertainties related to securing their cloud instances.

This newly released report reaffirms that misconfigurations are the primary cause of cloud security issues. In fact, Trend Micro Cloud One – Conformity identifies 230 million misconfigurations on average each day, proving this risk is prevalent and widespread.

“Cloud-based operations have become the rule rather than the exception, and cybercriminals have adapted to capitalize on misconfigured or mismanaged cloud environments,” said Greg Young, vice president of cybersecurity for Trend Micro. “We believe migrating to the cloud can be the best way to fix security problems by redefining the corporate IT perimeter and endpoints. However, that can only happen if organizations follow the shared responsibility model for cloud security. Taking ownership of cloud data is paramount to its protection, and we’re here to help businesses succeed in that process.”

The research found threats and security weaknesses in several key areas of cloud-based computing, which can put credentials and company secrets at risk. Criminals capitalizing on misconfigurations have targeted companies with ransomware, cryptomining, e-skimming and data exfiltration.

Misleading online tutorials compounded the risk for some businesses leading to mismanaged cloud credentials and certificates. IT teams can take advantage of cloud native tools to help mitigate these risks, but they should not rely solely on these tools, the report concludes.

Trend Micro recommends several best practices to help secure cloud deployments:

- **Employ least privilege controls:** Restricting access to only those who need it.
- **Understand the Shared Responsibility Model**: Although cloud providers have built-in security, customers are responsible for securing their own data.
- **Monitor for misconfigured and exposed systems:** Tools like Conformity can quickly and easily identify misconfigurations in your cloud environments.
- **Integrate security into DevOps culture:** Security should be built into the DevOps process from the start.

For more information and to read the full report, please visit: https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/exploring-common-threats-to-cloud-security.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and

control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro secures your connected world. For more information, visit www.trendmicro.com.

---

1 Smarter With Gartner, 5 Approaches to Cloud Applications Integration, May 14, 2019

Contact:

Erin Johnson
817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
OTC Pink:
TMICY

---

https://newsroom.trendmicro.com/2020-04-08-Trend-Micro-Research-Finds-Misconfiguration-as-Number-One-Risk-to-Cloud-Environments