Exceptional Attack Protection Proven in Rigorous MITRE Engenuity ATT&CK® Evaluations

Trend Micro's flagship threat detection and response platform proves its advantages in sophisticated simulations

DALLAS, April 20, 2021 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, excelled in the latest ATT&CK Evaluation performed by MITRE Engenuity. The Trend Micro Vision One™ platform quickly detected 96% of attack steps from the simulation that mimicked the behavior of two infamous APT groups.

Unlike other industry organizations that test a product's ability to detect and prevent various malware samples, MITRE Engenuity's ATT&CK Evaluations appraise a solutions' ability to detect targeted attacks leveraging known adversary behavior. This approach more closely mirrors real-world attacks that are most critical. MITRE Engenuity focused on techniques associated with notorious threat groups Carbanak and FIN7 in this year's simulations.

Click here to read the full MITRE Engenuity ATT&CK Evaluation for Trend Micro Vision One: https://resources.trendmicro.com/MITRE-Attack-Evaluations.html.

"Security has been about spotting the tools used in an attack: MITRE Engenuity adds the dimension of recognizing rather the patterns of an attacker, no matter when different tools are used," said Greg Young, vice president of cybersecurity for Trend Micro. "MITRE ATT&CK is, like the attacks it models, complex. Doing well on a third-party test like this is satisfying – and with 96% visibility, we did very well here – especially considering it models techniques used by two of the world's most capable threat groups. An even bigger success is helping educate organizations that ATT&CK isn't just about the test but that ATT&CK can be a part of the everyday playbook for SOCs, which is reflected in our solutions."

This year's test included two simulated breaches, one at a hotel and one at a bank, using typical APT tactics such as elevation of privileges, credential theft, lateral movement and data exfiltration.

Trend Micro Vision One recorded the following impressive results:

- Delivered 96% of attack coverage to provide visibility of 167 out of 174 simulated steps across the evaluations. This broad visibility allows customers to have a clear picture of the attack and respond faster.
- 100% of attacks against the Linux host were detected, capturing 14/14 attacker steps, which is especially important considering its huge increase in use by many organizations.
- 139 pieces of telemetry were enriched by the Trend Micro Vision One platform to provide extremely effective threat visibility to better understand and investigate attacks. This is critical for SOC analysts.
- 90% of attack simulations were prevented through automated detection and response very early on in each test. Deflecting risk early on frees up investigation resources, allowing teams to focus on the harder security problems to solve.

Trend Micro Vision One allows customers to see more and respond faster — collecting and automatically correlating telemetry across email, endpoints, servers, cloud workloads and networks to speed up detections and investigations.

Its performance against techniques used by two of the world's most formidable cybercrime enterprises proves its value in threat detection and response, and ability to optimize cyber-risk reduction for customers.

The MITRE ATT&CK framework helps industry define and standardize how to describe cyber-attack techniques — offering organizations a common and regularly updated language to triage detection and response as efficiently as possible.

This year's strong performance in MITRE Engenuity's ATT&CK Evaluation is the second in a row for Trend Micro, whose capabilities also impressed in the 2020 tests.

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. TrendMicro.com.

About MITRE Engenuity ATT&CK Evaluations
MITRE Engenuity ATT&CK Evaluations are paid for by vendors and are intended to help vendors and end-users better understand their product's capabilities in relation to MITRE's publicly accessible ATT&CK® framework. MITRE developed and maintains the ATT&CK knowledge base, which is based on real world reporting of adversary tactics and techniques. ATT&CK is freely available, and is widely used by defenders in industry and government to find gaps in visibility, defensive tools, and

freely available, and is widely used by defenders in industry and government to find gaps in visibility, defensive tools, and processes as they evaluate and select options to improve their network defense. MITRE Engenuity makes the methodology and resulting data publicly available so other organizations may benefit and conduct their own analysis and interpretation. The evaluations do not provide scores, ranks, or endorsements.

SOURCE Trend Micro Incorporated

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

---