Trend Micro Delivers the Industry's Most Complete Security Across Cloud and Container Workloads

Cloud-native security customized to the demand of DevOps to protect and scale environments

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced the availability of the industry's most complete security from a single solution protecting across cloud and container workloads. This leadership has been achieved through newly launched container security capabilities added to Trend Micro Deep Security to elevate protection across the entire DevOps lifecycle and runtime stack.

From virtual servers and data centers to public and private cloud workloads, containers are increasingly used and demand protection. Leading enterprises are bringing together their application development teams, IT operations and their security team to help the business deliver automated, secured applications to market quicker. Trend Micro connects teams with technology tools that bake security into the process while meeting compliance needs and reducing risk.

"While customers have been securing their containers with our technology for a couple of years now, we are proud to significantly expand our offering," said Steve Quane, Executive Vice President, Network Defense and Hybrid Cloud Security for Trend Micro. "Unlike many of the one-off point solutions crowding the market, our offering provides automated build-pipeline container image scanning, and extensive runtime protection providing full visibility and control. What is strikingly unique is our consolidated tool for container plus workload security in every environment."

Senior analyst and group director Doug Cahill at Enterprise Strategy Group believed, "Developers might be surprised by the scope of this new offering. The on-going deployment of application containers into production environments requires that the entire build-ship-run continuum be secured. As such, protection across the CI/CD pipeline for container environments must include the ability to the detect vulnerabilities, secrets, malware, and misconfigurations for early protection at build time, while delivering critical threat protection across on-prem and cloud host, orchestration and container layers at runtime."

The new features available now in Trend Micro's container security solution include:

Securing across the complete DevOps lifecycle

> Within the software build-pipeline, Trend Micro has extended its container image scanning to include pre-registry scanning, providing earlier detection of vulnerabilities and malware over and above scanning the trusted registry for any future threats. Deep Security will now also scan for embedded secrets such as passwords and private keys and provide compliance and configuration validation checks, along with image assertion for digitally signed images.

Securing across the entire stack

> At runtime of the container, Trend Micro has boosted container platform protection across Docker and Kubernetes. Deep Security has long ensured protection for the host and containers at runtime. This includes intrusion prevention system (IPS) rules, integrity monitoring to detect compromised instances of the platform, as well as log inspection.
>
> To ensure complete protection, Trend Micro inspects all lateral and horizontal traffic movement (east, west,

north, south) between containers and platform layers like Kubernetes and Docker.

Securing while granting full control

To increase automation and decrease manual tasks, security and operations teams using Trend Micro can now use any command shell to execute the application program interfaces (APIs). This additional option ensures full control of deploying policies, automation of monitoring, reporting and more. This completely new set of representational state transfer APIs have been written to automate security for application development and operations teams across the container orchestration tools and runtime environments.

A customer currently evaluating the container security from Trend Micro is DealerSocket's Director of Network and Security Operations, Greg Tatum. He said, "DevOps presents unique security challenges. The move to DevOps requires security tools that our engineers and infrastructure teams can easily embed, in real time as they are built."

To learn more on the Trend Micro container security solution, visit https://www.trendmicro.com/containers.

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 workloads, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and investigation, enabling better, faster protection. With more than 6,000 employees in 50 countries and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. For more information, visit www.trendmicro.com.

Contact:

Kateri Daniels
817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY
