Symantec Brings Remediation and Threat Intelligence Automation Capabilities to Cloud Security with New Service for Amazon GuardDuty
Tuesday, June 25, 2019 01:00:00 PM (GMT)

New service with AWS, full-stack container security and DLP protection for Amazon S3 buckets announced at AWS re:Inforce 2019

Symantec Corp. (NASDAQ: SYMC), a global cyber security leader and an Advanced Technology Partner in the Amazon Web Services (AWS) Partner Network (APN), today announced a new service for Symantec's Cloud Workload Protection (CWP) solution and Amazon GuardDuty to provide automated remediation and enhanced threat intelligence for AWS workloads and storage. Announced at AWS re:Inforce 2019, this new service will help enterprises navigate the complex security landscape, allowing AWS customers to automate and streamline key components of cloud security.

Modern enterprises have been transformed by the cloud, creating a new reality for security teams tasked with protecting critical workloads and information. While operating in the cloud has unleashed a number of benefits for businesses, new research from Symantec reveals that it has left IT departments scrambling to keep up. According to a [recent survey](#) from Symantec, nearly 70 percent of companies fear the risk of data breaches in the cloud, and an alarming 83 percent of IT personnel believe they do not have processes in place to effectively take action on cloud security incidents.

Automation is critical to solve cloud-scale challenges and supplement the cyber security intel gap. The Symantec Cloud Workload Protection new service with Amazon GuardDuty addresses both those challenges through continuous assessment, automated remediation and enhanced threat intelligence. CWP works closely with Amazon GuardDuty to automatically detect security threats and infrastructure misconfigurations in AWS workloads and storage, recommend necessary changes and automate workflow to remediate security gaps. The service also delivers automatic protection mode, which invokes cloud APIs for automated response to policy violations.

"As our enterprise customers move more workloads and data onto our cloud services, they need the right tools to help them navigate and enhance their security, privacy and compliance posture," said Dan Plastina, vice president, Security Services, Amazon Web Services, Inc. "With APN Partners such as Symantec, we are able to extend enhanced cloud security to our customers, ensuring that they can expand their cloud footprint while maintaining the highest standards of cyber security."

In addition to the new service with Amazon GuardDuty, Symantec also unveiled cloud security innovations as part of its [Integrated Cyber Defense Platform](#), including full-stack container security, Data Loss Prevention, cloud forensics and incident response technology to AWS customers.

Key updates include:

- **Full-stack container security:** Through the Symantec Cloud Workload Protection Suite, customers can gain deep visibility and full-stack protection of the entire container environment – host, runtime and Kubernetes orchestration layers. As containers are steadily more important in hybrid environments, it is critical for security teams to have increased visibility, detection and remediation capabilities.
- **DLP protection for Amazon Simple Storage Service (Amazon S3) buckets:** Symantec has extended its DLP solution to scanning of Amazon S3 buckets. This new enhancement automatically discovers and classifies sensitive data stored in the cloud, offers near real-time and scheduled scanning options for round-the-clock visibility and protection, and can be managed through a single, intuitive dashboard.
- **Simplified management across the security suite:** The entire CWP Suite can now be centrally managed through the Symantec Integrated Cyber Defense Management console, giving users total control over their entire security footprint while driving down the cost and complexity of managing it.
- **Full cloud visibility and forensics for swift incident response:** Deployed in AWS or on-premises, Symantec Security Analytics exposes the full source and scope of all threats and attacks no matter where they originate—across your own network or in AWS cloud workloads—to effectively arm incident response teams and threat hunters against even the most sophisticated threats.

"The explosive growth of cloud workloads and storage has expanded the threat vector at a time when enterprise security teams are already overwhelmed," said Art Gilliland, EVP and GM Enterprise Products, Symantec. "Smart automation, management innovations and integration through our Integrated Cyber Defense Platform give security teams the tools they need to take control of the complex, shifting threat landscape."

For more information, please visit: https://www.symantec.com/blogs/feature-stories/three-ways-get-handle-cloud-security.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to help protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

View source version on businesswire.com: https://www.businesswire.com/news/home/20190625005385/en/

--30-- MM/SF

Contact:

Nicole Murphy
Symantec
650-527-8000
Nicole_murphy@symantec.com

Industries: Data Management, Security, Technology, Software, Internet
Languages: English
Primary Identifiers: NLOK-US
Related Identifiers: NLOK-US, US871503108
Source: Symantec Corporation
Subjects: Contract/Agreement, Trade Show, Product/Service