CUSTOMERONE

Symantec

How We Secure Our Workloads in the Public Cloud

Venturing into the public cloud is the liberating experience that all developers dream of, with the freedom and flexibility to innovate and accelerate testing cycles for increased business productivity. However, public cloud best practices dictate that security responsibilities must be satisfied before these benefits can be fully unlocked.

As customer utilization of our cloud-delivered products and services continued to explode, Symantec recognized that security needed to keep up with the velocity and frequency of our public cloud workload deployments. “We want our developers to be as productive as possible while still adhering to our strict security policies,” said Igor Bolotin, Senior Technical Director of Symantec Cloud Platform Engineering (CPE). Bolotin continued “We recognized that security measures must be integrated seamlessly into the DevOps workflows that our developers rely on for rapid testing and deployment of our cloud-first security offerings.”

Public cloud networks can be built and configured on-demand by any developer. This is a big transformation from traditional data center operation. The challenge is to ensure that network controls are properly applied, and that workloads are appropriately isolated from one another. Additionally, automatic enforcement of security policies on new servers wasn’t possible, leaving many cloud servers exposed. “While a new server could be spun up at the click of a button, agents and security policies would have to be installed and applied manually.” Bolotin added.

To address the problem directly, Symantec developed Symantec Cloud Workload Protection (CWP), a cloud-delivered service that automates security for public cloud workloads. Symantec desired a service that applies security in a seamless fashion so that developers could still complete their work in an efficient manner.

Regarding today’s threat and vulnerability landscape, Bolotin commented, “CWP provides a view into application and operating system (OS) vulnerabilities while discovering threats and exploits that we weren’t able to see before. CWP’s Threat and Vulnerability Map provides our CPE team with visibility into vulnerable versions of OS’s and applications deployed by our product teams. We use this information to update CPE base images with the latest versions so that product teams don’t have to worry about patching their workloads. CWP also provides information on older versions of base images still in use, enabling DevOps engineers to immediately update and deploy new images. And finally, CWP has access to the Symantec Global Intelligence Network, which provides up-to-date information on the latest global attacks and vulnerabilities.” Bolotin summarized, “Cloud security used to be a checklist…an afterthought. Now, it’s automated.”

customer_one@symantec.com

CustomerONE Team
350 Ellis Street
Mountain View, CA 94043
800-745-6054

Symantec’s CustomerONE team can facilitate discussions between you and our IT security practitioners to help you address your security questions and concerns. Please contact us directly or through your Symantec sales team.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.