Getty Images

SECURITY > CLOUD SECURITY

One Company's Quest to Solve the Cloud Data Security Problem

GRA Quantum turns to Allure Security for help addressing the lack of governance, auditing and logging when it comes to cloud computing.

Karen D. Schwartz | Jul 16, 2019

With a focus on providing assessment, planning and managed security services to its customers, GRA Quantum puts a premium on keeping its clients' data safe. To accomplish this, it partners with world-class technology, security and cloud vendors.

enamored of Allure Security, which makes risk detection and response technology. GRA Quantum routinely recommends to its customers for tracking and analyzing cloud-based document access and sharing. The solution focuses solely on data, providing tools to detect and respond to incidents where data or files are inappropriately viewed, accessed or copied. It can flag potential risks, allowing validated users to drill down into each possible hazard directly from the dashboard to learn critical details needed to address those risks.

The technology addresses what many believe to be the greatest weakness in cloud computing: the lack of governance, auditing and logging. In essence, it provides more visibility into the access and control of protected documents by filtering and data cleansing events and then performing risk assessments on every event.

“One of the biggest challenges with cloud platforms and products is governance of those platforms—making sure that people are not accessing the platform if they aren’t supposed to be accessing it, and making sure users know how to properly share their documents without exposing them, even if it’s just out of ignorance,” said Jennifer Greulich, director of managed security services at GRA Quantum.

In addition, Greulich said, most cloud platforms have limited functionality for auditing and logging. “We realized that we had no way of seeing whether or not unauthorized access occurred on our sensitive documents because of the lack of logging and auditing within most cloud environments,” she said. “It’s actually quite shocking that cloud providers have gotten away with not providing logging and proper auditing of their systems for so long.”

Greulich said there have also been cases internally where employees were mishandling documents. For example, they might open a document, save it to their computer and then email it to themselves. “Without using a third-party tool, there is nothing that would tell our security operations center [SOC] that that happened.”

sharing properties. But this required performing permissions audits and, even then, it was difficult to determine if a document had been accessed, downloaded or emailed to an external source.

The GRA Quantum team then looked into APIs and other third-party tools but found mostly cloud access security brokers (CASB). While these tools are effective, they are overkill for what the company needed in terms of both functionality and cost. What GRA Quantum needed, Greulich decided, was a simpler solution that focused specifically on protecting data and notifying the SOC if data had been compromised.

Getting On Board

It didn’t take long for GRA Quantum to come to the conclusion that what was working for its customers would work for them. What’s more, Allure was already certified to work with Office 365, which GRA Quantum uses extensively. Allure covers files stored in Microsoft OneDrive, SharePoint, Teams and OneNote. According to Allure, its technology reads log information from Office 365, including user names, file names and paths, and IP addresses. It then filters the log information, adds geographic and organizational insights, and stores them for the long term.

Greulich’s team has spent the last few months implementing and fine-tuning the technology. It uses the risk scoring, for example, to evaluate departing employees and make sure they aren’t accessing proprietary data before leaving the company. It uses the geolocation technology to receive alerts about data access from other countries. For example, GRA Quantum was alerted that someone in Qatar opened a document, along with user information, the file and the file path. With that information, the company was able to determine that the behavior was acceptable and retune the alert. “But when we see a user in a place where we know we don’t have users, we know we will have an issue,” Greulich said.

environment. This includes decoy documents that can detect leaks and breaches.

“We’ll bury documents within file systems that no normal user will be searching for and know that if somebody hits a beaconized document, we’ve got something nefarious going on in our network, because it’s an automated tool finding that document,” Greulich said.

Eventually, Greulich hopes to take advantage of the technology’s data loss forensics technology, which helps prevent the sharing and exposure of data. “Right now we are in detect-only mode, but we’d like to extend this in a way that we can prevent, not just detect,” she said. “We want to use it as a way to prevent data from leaving our organization in the first place, across our entire organization.”

Greulich also hopes to persuade Allure to broaden the appeal of its cloud data security product, both for its own company and for its customers. For example, it has asked Allure to consider supporting not only Office 365 but Google Drive, Dropbox and Box. The company also has requested a way to track documents on users’ laptops.

“There are countless times where users will open a cloud document and save or download or something because they need to edit it or maybe aren’t familiar with really how to use cloud technology,” she explained. “That means we have documents all over endpoints and there is no way to track that.

“At the end of the day, I want to see where is our sensitive data, who is using it and how can we protect it,” she added. “We think that this can go a long way for us to do that.”

0 COMMENTS

Symantec Bolsters Cloud Access Security Solution

JUL 19, 2019

At the AWS Security Conference, Experts Address Cloud Concerns

JUL 04, 2019

Broadcom Is in Advanced Talks to Acquire Symantec

JUL 03, 2019

Net Defender CloudFlare Goes Down, Taking Many Websites With It

JUL 02, 2019

Getty Images

SECURITY > CLOUD SECURITY

Symantec Bolsters Cloud Access Security Solution

Symantec makes improvements to its Cloud Access Security Solution to better secure access in the cloud.

Karen D. Schwartz | Jul 19, 2019

bolstering its approach to secure access in the cloud.

The Cloud Access Security Solution, part of the company's Integrated Cyber Defense Platform, is designed to address security issues in the cloud, on the web and in email. The goal, according to Symantec, is to offer customers an integrated suite of solutions that enforce zero trust security policies across all cloud-based environments.

The combined solution, which integrates products from a host of acquisitions, is extremely comprehensive, said Rob Westervelt, a research director at IDC.

"They are combining technologies they acquired from Bluecoat, Illuminate and Fireglass with the rest of their portfolio: DLP, rights management, automation encryption and endpoint protection," he said.

One of the most significant parts of the announcement is designed to improve application security in the cloud. It combines the CloudSOC Mirror Gateway with web isolation capabilities from Fireglass to create a set of cloud access security broker (CASB) security controls for applications in the cloud, accessed by any device. It also allows organizations to apply and enforce granular policy controls.

"If you have an application that is extremely critical, you can use the Mirror Gateway to basically create a mirrored copy in an isolation portal," Westervelt explained. "Because they are working on a mirrored copy of the application in isolation, nothing can really break, and it's much more difficult for an attack to be carried out."

Westervelt said the solution has a lot of promise and solves important security issues, but Symantec has yet to prove that the solution scales.

Another important part of Symantec's Cloud Access Security Solution protects data antivirus and sandboxing technologies.

The Luminate acquisition, a huge enabler of the infrastructure-as-a-service (IaaS) solution, was a critical one for Symantec, Westervelt said.

“CISOs—even those who work in Symantec shops—often tell me they are using Zscaler’s remote access solution to access cloud resources as an alternative to VPN because it’s easier and solves the issue of bring your own device [BYOD],” he said. “And that’s all they were using Zscaler for. Symantec’s solution in this area now does almost the exact same thing.”

In addition to the software-as-a-service (SaaS) and IaaS parts of the Cloud Access Security Solution, Symantec announced more minor advances in the web and internet security arena and the email security arena.

Westervelt said this announcement is an important one, both for Symantec and its customers. Not only does it bring critical components together under the same umbrella, but it does so in a way that can reduce complexity and cost for customers.

“The cool thing is that they aren’t just announcing that they have integrated new technology with what they already have,” he said. “They have built on top of it. The Secure Access Cloud piece itself is an integration coupled with Symantec’s VIP Secure Access, which means that if there is a perceived issue, you can step up the authentication and push out a challenge.”

RELATED

One Company’s Quest to Solve the Cloud Data Security Problem

At the AWS Security Conference, Experts Address Cloud Concerns

JUL 03, 2019

JUL 02, 2019

Next Article

ITPro Today™

an informa business