MAKING YOUR WAY THROUGH THE CLOUD

Who's in control of your cloud security—you or your service provider?

BY ANNE SAITA

IN 2012, a Fortune 500 oil and gas company joined the early adopters migrating assets and business processes to "the cloud." Corporate executives' biggest security concern then was the potential for a rogue administrator from a chosen cloud service provider to pilfer all of its data.

"That was the big fear at the time," explained Jon-Michael C. Brook, CISSP, CCSK, a principal at Guide Holdings who consulted with the company during its initial cloud migration. "They weren't as worried about errors that they might make; they were more worried about the trusted insider within the cloud service provider."

Those concerns haven't gone away, but eight years later a different insider threat is forcing companies to step up their cloud security posture. Today, a cloud-based breach is much more likely to come from an honest mistake rather than malicious attack.

ILLUSTRATION BY TAYLOR CALLERY

This commonplace lapse in configurations, combined with a growing global reliance on cloud services and increasing complexity of cloud infrastructures, is expanding risks and challenging vendor relationships. It's also requiring cloud consumers to "own" their security, rather than rely on providers to carry a greater load.

CLOUD-BASED APPS AND DATA

Commercial cloud usage in recent years has moved up the technology stack, from an early reliance on renting virtual machines and storage space with infrastructure as a service (IaaS) and platform as a service (PaaS), to widespread use of highly scalable software as a service (SaaS). With the new focus on SaaS, application developers are becoming far more removed from default or designed protections.

"If you start doing stupid things, or your supply chain does stupid things, you are at risk. As far as the third- and fourth-party vendors are concerned, you need to have vendor management. That's tough to do."

—JON-MICHAEL C. BROOK, CISSP, CCSK, principal, Guide Holdings

At the same time, organizations are moving from monolithic public and private cloud usage to multi-cloud programs that offer different types of virtual services from a multitude of vendors. The result: serious cloud sprawl, more complex cloud infrastructures and a complicated supply chain—all of which hinder visibility at a time it's most needed.

In FireMon's most recent report on the State of Hybrid Cloud Security, the cloud services industry is expected to grow at three times the pace of overall IT services by the end of 2022. A major driver: digital transformations that promise to improve productivity and drive down operational costs. But the majority (60%) of IT participants in the study admit deployments are outpacing security's ability to place controls around these cloud services.

Then there are data breaches that send shockwaves, like the 2019 Capital One breach that compromised sensitive data on some 100 million customers. Authorities said an apprehended former system engineer at a major cloud computing company was able to gain access by exploiting a misconfigured web firewall application.

That's not to say trust in the cloud hasn't improved. "The cloud's become trusted," Brook said, "to the point that if you haven't made that digital transformation yet, your board is probably asking, 'Why not'?"

He notes that even the U.S. intelligence community now has a cloud. The challenge today is how to handle third- and fourth-party risks as CSPs broaden their offerings through partnerships to meet customer demands.

"If you start doing stupid things, or your supply chain does stupid things, you are at risk," he said. "As far as the third- and fourth-party vendors are concerned, you need to have vendor management. That's tough to do."

Such a program requires data flows to track where all information and particularly sensitive data goes, even to the point of planting fake data to see if it ends up on the dark web. It also requires close scrutiny of service level agreements to make sure they remain realistic and compensate fairly for any losses due to a breach. And, of course, there needs to be a solid incident response plan for if or when there's a service failure.

"With people going into the cloud, the biggest thing as a consultant that I keep seeing is this 'good enough' mentality," said Brook, who also serves as a research fellow for the Cloud Security Alliance. "They take a monolithic VM that they put together 10 years ago and just stuff it directly into the cloud. … It ends up costing more money to not use any of those cloud-native, auto-scale options and it's less resilient."

SHARED RESPONSIBILITY MODELS

Cloud providers have long touted a shared responsibility model when it comes to securing their infrastructure, platform and services.

"Statements pertaining to shared responsibility models that all the major CSPs have published have become a lot more concise and focused on what they provide and what the limitations are in securing services," explained cloud security architect Richard Tychansky, CISSP-ISSEP, CSSLP, CCSP, CAP, CIPP/US and CIPP/G. "They are actually putting in writing what they expect customers to do to secure their environments and protect their data."

This includes where service providers' responsibilities end. "I know the CSP is protecting its physical assets, the servers and network infrastructure, for free. But what they've now made clear is if my organization is offering a multi-tenant application environment [multiple customers using the same application], then I'm responsible for making sure every one of my clients has their data logically

"We need to see more CSPs putting the encryption keys in the customers' hands by default. If that can happen, then I think we'll have better cloud security in the future because customers won't have that question: 'Well who at the cloud service has access to my data?'"

—RICHARD TYCHANSKY, CISSP-ISSEP, CSSLP, CCSP, CAP, CIPP/US, CIPP/G, cloud security architect

separated," and that is a big responsibility, he said.

Tychansky sees more attention now on cloud-based data processing and data storage—and the role of encryption in reducing data exposure. Expect cloud customers to request management of their own encryption keys to minimize risks of data loss, data sharing and subpoena requests.

"We need to see more CSPs putting the encryption keys in the customers' hands by default. If that can happen, then I think we'll have better cloud security in the future because customers won't have that question: 'Well, who at the cloud service has access to my data?'"

CLOUD SECURITY POSTURE MANAGEMENT

Just as cloud usage has exploded, so have security tools to reduce the risks from faulty cloud configuration and administration.

In 2019, Gartner coined the term cloud security posture management (CSPM) to describe a new category of cybersecurity solutions that find and resolve customer-driven cloud misconfigurations. Analysts claim such errors are responsible for almost every attack on cloud services. And, they predict that within the next four years, those that adopt these products will see up to an 80% reduction in cloud security incidents due to misconfigurations.

Gartner analysts also warn that CSPM requires continuous assessments as both cloud infrastructures and applications continually evolve.

In a January 2019 Gartner white paper, *Innovation Insight for Cloud Security Posture Management*, author and analyst Neil MacDonald writes: "As enterprises place more services in public cloud and as the public cloud providers introduce more infrastructure and platform services directly into the hands of developers, it is becoming increasingly complex and time-consuming to answer the seemingly straightforward question: 'Are we using these services securely?' and 'Does the configuration of my cloud services represent excessive risk?'"

Among the paper's recommendations:

- Consider short-term contracts with CSPM vendors until the market is more mature.
- Take advantage of a CSP's internal CSPM capabilities if that cloud use is limited in scope and usage.
- Look to see what CSPM capabilities a cloud security access broker (CASB) might provide.
- Include everyone within a cloud operations team, so everyone has a firm handle on everything being accessed, stored or processed within a cloud management platform.
- Make sure any CSPM strategy includes locating all sensitive data stored in a cloud repository.

While the term may be relatively new, the concept of creating checks on configuration and compliance best practices and industry standards is not. But what a CSPM solution can do is provide that nudge to beef up requirements and elevate individual accountability.

"I think it's got potential," Brook said. "It's something where I expect the AWSes, Microsofts and Googles will come out with their '80% is good' version. They're already doing it from the perspective that they're already telling you, 'You have auditing capabilities out there.' AWS has their inspector products, and Microsoft and Google offer something similar that tells you what the found issues are, but they don't yet clean them up.

"I think we may get to that point where they do provide this by buying a CSPM provider. Or maybe they don't because it's too complicated, or they don't want to go down that multi-cloud route and just leave it to other people," he continued. "I don't think the big guys are going to get to the point of not allowing the company to have the machete on the table and if you hack your fingers off, it's your fault. At some point they will make you put the machete in the closet and lock the door."

Tychansky's view of the CSPM term is that it is more "fast fashion" and in response to a marketing trend than anything, but the concept—to instrument security controls into cloud-native applications in order to better measure cloud security posture over time—is important and will persist in one form or another based upon demand.

"If we have instrumentation built into applications and [micro]services, then we can better manage and monitor

application security controls in the cloud. Security instrumentation is where I'm predicting the technology will evolve," he said.

He likens these instruments to nano agents built into applications that then act as sensors. "In the future, when organizations deploy to the cloud, security architects will specify the placement of sensors throughout the environment, including within cloud-native applications and storage. Everyone from system reliability engineers, to auditors, to incident responders will have the telemetry data that they need to measure the security posture of the cloud configuration and the health of the services. Sensors will facilitate alerting in real time based upon anomalous behavior and well-understood application threat models defined in code."

"Cars and airplanes are built to safety standards, but we haven't built the cloud to a single safety standard that we all agree on despite the work of several standards-setting organizations," he continued. "Right now it's a shared responsibility model, and CSPs have limited their liability." For small, medium and large organizations that means they need qualified security personnel even more than they did for their on-premises solutions.

He continued: "We don't do a good enough job of creating security architectures with this notion of building in by default sensor instrumentation into cloud deployments. Many years ago we started to do with that with intrusion detection and prevention systems, but many cloud-native services today lack any form of automated instrumentation. And that's something we can do at very low cost. We can re-architect to build in these sensors into cloud-native applications…that's where hopefully we can see some change."

And for those very early in their digital transformation? Brook recommends starting small. That oil and gas company mentioned earlier first moved a lunchtime application into the cloud. It let employees know what was being served in the cafeteria that day. "It's low risk, so they had time to get it right," he said. "These are still greenfield opportunities." ■

ANNE SAITA *is editor-in-chief of* InfoSecurity Professional.