AWS Security Visibility: Myths vs. Reality

By Bruce Sussman

Read more about the author

THU | AUG 29, 2019 | 10:55 AM PDT

Network security visibility is a challenge in any environment, even if your organization is completely on-prem.

But start moving your data to the cloud and you may wonder: are we losing the detailed control and response we had when it was in house?

AWS cloud visibility myths

SANS analyst Dave Shackleford says there are two really popular cloud security and visibility myths right now among IT and cybersecurity teams:

1. You lose the ability to get log monitoring in the cloud.
2. Network security visibility is less capable in the cloud.

He knows about these cloud visibility myths because he

Most Recent

CYBERSECURITY

They Made $30 Million Because Hackers Showed Them the Future

is constantly asked about them.

> "It's one of the most common questions I get, categorically, around operations and security in the cloud. How do I adapt some of the things I've been doing internally to try to gain visibility into the infrastructure, see what sorts of things are going on, and being able to build and piggyback things like detection and response capabilities around that."

And in a recent Amazon Web Service (AWS) training webcast, How to Build a Security Visibility Strategy in the Cloud, Shackleford busted those myths into a bunch of bits.

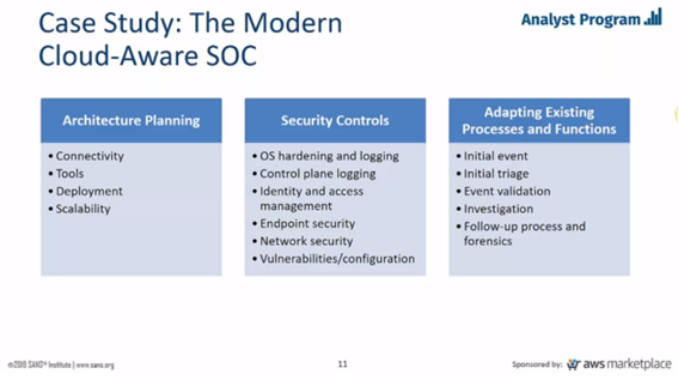
What does cloud security visibility look like now?

Let's take a look at the hybrid cloud model, which seems to be the front runner right now.

Organizations are building connectivity between cloud-based assets and on-prem assets. And the goal is implementing a model of deep, continuous visibility in the cloud.

For one thing, security teams can adapt many of their current methodologies and apply them to cloud visibility and security.

Take a look at this overview, which covers the cloud-aware SOC. It gives you an idea of the architecture planning, security controls, and adaptations of your current practices:



Shackleford says a key part of implementation is collaboration.

"The SOC team needs to align with cloud architecture and engineering teams that have built the hybrid architecture and maintain it. You need to do this more closely than before."

Cloud network visibility reduces asset management problems

You can't secure what you don't know you have, right? And asset management is a challenge for nearly every organization.

According to Shackleford, however, asset management in AWS can actually be easier:

> "It's all APIs. You turn this on and you know pretty much everything. Within AWS, there's no better description of this than their CloudTrail logging service; it's one of the most innovative things I've seen in recent memory."

Through CloudTrail, you will have access to a log of everything that happens and what was created.

New tool to put cloud network visibility, security, on a single pane

Visibility to everything that happens?

This raises an interesting question of its own. How do you easily sort through it all and find what's relevant?

That answer came from David Aiken of the AWS Marketplace Solutions Architect Team. He co-led the cloud security visibility web conference.

> "You move to the cloud and you ask for logs, and you get terabytes of log data to go through and figure out. What's noise, what's related, what's important, what should I prioritize? So we've got a new service in preview right now which brings

> together all these logs, security alerts, compliance status across all your AWS accounts as well as third-party services.
>
> This will make it easy to analyze what's happening across your accounts and give you a single pane of glass view across security compliance tools. It is going to be really, really helpful."

And he points out that because AWS is software- and API-driven, each action creates a complete audit trail of its own.

Which security vendors easily integrate with AWS?

We won't list them here, however, Aiken highlighted several security vendor partnerships that deploy easily into AWS, and we learned that vendors listed in the AWS Marketplace are screened for this ability.

The web conference unpacked everything we've covered here in more detail. And if you're a NIST CSF shop, you may be surprised to see how AWS security and visibility tools map back to the NIST Framework.

The speakers also covered that topic in the Amazon Web Service (AWS) training webcast, How to Build a Security Visibility Strategy in the Cloud.

It certainly offers visibility into this process.

Tags: Cloud Security, Amazon

Comments

First Name*

Last Name

Email*

Comment*

protected by reCAPTCHA
Privacy - Terms

Submit Comment

See what SecureWorld can do for you. Contact us today! CONTACT US

First name*

Email address*

SUBSCRIBE