DataCenter Knowledge™

MANAGE > SECURITY

Micro-Segmentation Is Complicated, So Vonage Turned to Machine Learning for Help

Machine learning goes hand-in-hand with the new essential network security strategy.

Maria Korolov | Sep 23, 2019

Vonage, a telecom with more than $1 billion in revenues last year, has data centers around the world to help it handle voice-over-IP traffic for both businesses and consumers.

The company had all the traditional network protections in place, but recent headlines about cybersecurity breaches were unsettling.

Related: Investors Pour Money into Startups Killing the Data Center Firewall

"If you look at the media reports, bad actors that are able to penetrate are going horizontally across organizations and looking for vulnerabilities and soft spots," said Steve Strout, the company's global head of technical operations.

About a year ago, Vonage started to look at ways to protect its data centers against this kind of lateral movement. One solution was to increase the number of segments its networks were divided into.

Related: Latest Data Center Network Security Strategies Revolve Around Intelligence

"Having a lot of segmentation is becoming an industry standard," said Strout.

Unfortunately, with the technology Vonage had in place increasing the number of segments wasn't practical.

"When you increase segments, the complexity becomes tremendous," he said. "The management overhead of making changes, of ensuring that routes are open, becomes a real problem."

To stay ahead of attackers, Vonage began to look for ways to automate microsegmentation, improve its network security without having to add a lot of staff. Late last year, it decided to go with Edgewise.

The new system was up and running this January. At first, out of caution, it was configured to run in recommendation mode, so human operators still carried out any changes instead of letting the system handle all the microsegments automatically.

By the end of April Vonage switched to automated mode. "When we went automated, we [didn’t] undo anything, and I haven't found anyone complaining about false positives or false negatives," Strout said.

And no new employees were required. "Actually, it freed up time for people to do other things," he said.

The initial setup of the micro-segmentation system was automatic as well, because it used machine learning to figure out what the segments should be. First, the micro-segmentation agents were installed and allowed to run for a while to give the system a good idea of what normal traffic looks like.

Once in place, switching on the platform was not difficult, Strout said. "It took somebody without any real network knowledge a couple of minutes to get this to work and work the way we wanted it to work. I hate to say it, but it was absolutely simple."

He said the entire network environment was mapped in about 20 minutes. "In Vizio, it would have taken us two months." Vonage currently has between 25,000 and 35,000 rules in place for its micro-segmented network.

And if the network changes, there's no need to manually make the configuration for each of the company's locations around the world, he said, or to write scripts for each change.

"We're at a point now where I only look at it once or twice a month," he said.

Edgewise isn't the only company offering micro-segmentation technology. In addition to the large players, like VMware and Cisco, there are specialsts including Guardicore, Illumio, and ShieldX.

It's the right time for an automated, AI-powered approach to micro-segmentation, said Kris Lahiri, chief security officer at Egnyte, a content security company.

"Not to say that such an approach didn't exist in the past," he added. But today's networks are very diverse, with physical servers and cloud environments, virtual machines and containers, office LANs and on-premise data centers. "There is a need for tooling that decreases the complexity of keeping such complicated networks on high level of security."

Last year, Gartner named micro-segmentation one of its top ten security projects . And, in a report published this spring, the market research firm called micro-segmentation "a key requirement of solid workload security."

The market has acknowledged that micro-segmentation is necessary, and it's not just because attackers are getting smarter, said Tom Hickman, VP of engineering at Edgewise Networks. Enterprise networks are changing at a faster rate than ever before.

"Doing traditional network management techniques with static firewall segmentation, you need a team of network administrators just to keep up with the change rate," he said. "And you're not actually securing what you thought you were securing, or you'd break your business apps. The environment would change, and you'd break access to your finance database or your payroll."

Some companies are taking a more manual approach to micro-segmentation. Cloud security vendor Caveonix, for example, needed state-of-the-art security in its own data center.

"We employ micro-segmentation, and it's greatly successful in reducing our attack surface and the number of ways attackers have to access our system," said Chris Davis, the company's VP of product management.

As a technology company with plenty in-house cybersecurity expertise, Caveonix built its own micro-segmentation system to use with both its own data center and its AWS deployments.

"It's been done incrementally over time," he said. "But if we were to start from scratch and have a focused project team on it, we can maybe do it in two to four weeks, depending on how aggressive we want to be."

Now that the system is set up, upkeep doesn't take too much time, he said. "It's baked into how we deploy things now and happens in the process of setting up new systems."

There are approximately 200 segments on Caveonix’s network now, according to Davis.

Caveonix does also use AI and machine learning as part of its micro-segmentation efforts, identifying network anomalies in connections, sockets, network addresses, "anything related to the metadata of network communication," he said.

Once a micro-segmentation system, the next step is to automate responses to violations.

"Seeing what you have is important," said Ratinder Paul Singh Ahuja, chief R&D officer at ShieldX Networks, another micro-segmentation vendor. "But data center managers need to be able to block malicious activity if they see it."

He suggested that companies looking to roll out this kind of security pick a direction that allows for full automation.

"Data center managers need to be wary of tools that keep one foot in the past and one in the future," he said. "Like cars – go electric and don’t waste time with something hybrid.

Source URL: https://www.datacenterknowledge.com/security/micro-segmentation-complicated-so-vonage-turned-machine-learning-help