CrowdStrike Case Study

CROWDSTRIKE

CROWDSTRIKE AND AWS

OAK HILL ADVISORS CASE STUDY

ABOUT OAK HILL ADVISORS

Oak Hill Advisors is a global alternative investment firm that manages approximately $32 billion in performing and distressed credit related investments for institutional investors in North America, Europe and elsewhere. The company focuses on mortgages, collateralized loan obligations and high-yield active distress or performing credit loans.

Oak Hill Advisors is a global alternative investment firm that manages approximately $32 billion in performing and distressed credit related investments for institutional investors in North America, Europe and elsewhere.

THE CUSTOMER

CISO Sajawal Haider has a dual role at Oak Hill Advisors. In addition to managing security for the firm's global operations, he oversees infrastructure and infra-strategy and operations.

"For the past four years, we have been operating under a cloud-first strategy," he said. "That began with selective SaaS deployments and culminated in 2016 when we closed our data centers and moved everything to Amazon Web Services (AWS)."

Haider said the primary reason for moving the firm's infrastructure to the cloud was to leverage the platform's agility and unify the firm's operating framework.

"We needed to converge so that we could have the agility to more quickly innovate and develop applications," he said. "I also believe the cloud is more secure than on-prem data centers."

THE CHALLENGE

Despite being more secure, the cloud has "quite a few" security challenges that differ in nature from those of on-prem data centers, Haider said.

"One security challenge of the cloud is that your systems cannot sit behind a perimeter," he explained. "Another challenge is the dynamism of the infrastructure. We introduce changes daily, which in the past was not the case. And even if it were, because we were behind a firewall it took more time to discover and mitigate security issues. In the cloud, your vulnerability can be exposed within minutes or seconds."

Haider adopted four guiding principles to adapt the firm's security posture to the cloud's unique requirements: follow AWS best practices, assess infrastructure issues in real time, test more frequently during development, and automate incident response.

"These are the things we focus on to ensure we are secure in the cloud," he said.

Haider's guiding principles led him to the CrowdStrike® Falcon® platform, first to provide streaming protection and then expanding its deployment to eventually include Falcon Discover™ for AWS.

"The more we used CrowdStrike technology, the more we realized it truly was different than any of the other tools in our environment," he said. "Because the Falcon platform is focused on endpoints, based in the cloud and supported by managed services, it became a focal point of security for us."

In particular, Haider explained the importance of managed services to Oak Hill Advisors.

"We migrated to the cloud because we wanted to take advantage of the accelerated integration of cloud-based products," he said. "The problem is you can't find people who know how to manage the technology because it changes so quickly. We therefore now rely on vendors not only to own the technology but also to manage it. That's why CrowdStrike is truly differentiated: it has sophisticated technology and managed services, and they work hand in hand."

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered next-generation endpoint protection. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify next-generation antivirus, endpoint detection and response (EDR), IT hygiene and a 24/7 managed hunting service — all delivered via a single lightweight agent.

For more information visit:
www.crowdstrike.com/aws-and-crowdstrike

LESSONS LEARNED

There have been numerous advantages to extending CrowdStrike technology to the firm's AWS infrastructure, Haider said.

"Before deploying CrowdStrike, I didn't feel we had a very good platform and I thought we might not be able to investigate incidents properly," he said. "Now security incidents, whether high- or low-priority, are less a cause for alarm, because the Falcon platform has made us feel more secure."

The Falcon platform's single agent has been a boon in terms of both managing and updating the tools it offers.

"Having three to four things in one agent has truly helped," Haider said. "And CrowdStrike updates are usually a non-event for us. As a result, our teams can be more productive."

Haider also praised the in-context visibility Falcon Discover for AWS provides his security team, providing a comprehensive overview of AWS, VPC, security groups and EC2 instances.

"Those capabilities are indispensable, as it takes a lot of time for security teams to acclimate to and access in-depth knowledge of the complex AWS platform," he said.

"That's where CrowdStrike is truly valuable for us. Our security team can continue to work on what they need to work on."