CROWDSTRIKE

CROWDSTRIKE AND AWS
POKÉMON COMPANY INTERNATIONAL CASE STUDY

Pokémon Company International is responsible for the brand management, licensing and marketing of Pokémon products to a global audience numbering in the hundreds of millions. In 2017, the company expanded its online business, due in part to the success of PokemonGo.

At the time, Pokémon hired CISO John Visneski to build and run the online security program. One of the first things he did, he said, was broaden a long-standing company tenet — ensuring children's safety — to encompass the safety and trust of all customers.

"When a parent lets their child download PokemonGo, they are placing their trust in us as a brand that we are a safe place for children to play," Visneski explained.

That broadening of focus reflected a key belief Visneski has about the role his team fills.

"At the end of the day, whatever organization you are in, your job as a security professional is to align with the business and be a business enabler," he said.

THE CHALLENGE

For a company the size of Pokémon, availability and security are vital to doing business.

"We may need to scale up quickly and scale back just as quickly, and then scale up again," Visneski explained. "Whenever that happens, it's crucial that security and operations are not affected."

The ramifications of downtime are swift and serious.

"If Pokémon goes down for five minutes, we make a few people mad," Visneski said. "If it goes down for a half hour, Reddit lights up on fire. If it goes down much longer than that, gaming pubs start writing articles about us. Going offline deteriorates our brand and the promise we make to our users."

Visneski's team's ability to discover abnormal activity and act quickly is a business enabler in an industry where it's survival of the fastest — yet survival takes more than applying products to problems in hopes of finding a solution, he explained.

"Every organization's biggest problem is visibility into its environment," Visneski said. "Many folks get ahead of their skis and try to get 'wonder products' that will solve all their problems, without first doing due diligence to establish a baseline, basic hygiene and that crucial visibility."

WHY AMAZON WEB SERVICES

Like many companies, Visneski said, the corporate side of Pokémon is a hybrid of on-premises and cloud-based systems.

"But our customer-facing platform is almost entirely on Amazon Web Services (AWS)," he said, noting that they take full advantage of EC2 instances in production and DevOps environments.

At first, cost savings were the motivation behind building an online business with AWS, Visneski said. Then scalability came into play.

"For a brand like ours with hundreds of millions of customers spread globally, AWS provides an excellent environment," he said. "Our developers can work as fast as they want to scale to meet the demands of PokemonGO or other apps released in the future."

"That speed of scale and business enablement is what we have leveraged through AWS in a pretty big way," Visneski continued. "AWS has been an excellent partner."

When Visneski did his due diligence to gain visibility into and establish baselines for Pokémon's AWS platform, he found an ideal partner in CrowdStrike and the CrowdStrike® Falcon® platform — technology that, like AWS, is cloud based and highly scalable.

Specifically, Visneski's team uses Falcon Discover™ for AWS to identify all Amazon Elastic Compute Cloud (EC2) instances that do not have the CrowdStrike Falcon platform installed.

Falcon Discover for AWS also provides additional details about each EC2 instance where the CrowdStrike Falcon platform is installed.

"For a brand like ours with hundreds of millions of customers spread globally, AWS provides an excellent environment. Our developers can work as fast as they want to scale to meet the demands of PokemonGO or other apps released in the future".

John Visneski
CISO
Pokémon Company International

THE BENEFITS

Visneski was pleased with the speed and scope of the visibility his team was able to achieve.

"The visibility into EC2 instances is pretty awesome," he said. "Not exciting just in security, but also in DevOps. The beauty of DevOps is that it moves fast, but the risk that comes with that is that DevOps engineers can lose sight of the tools they deploy, so visibility into EC2 instances has been one of the best features for us."

In addition to that visibility, Visneski said the other big successes of the integration of AWS and CrowdStrike has been how quickly the security posture responds to spinning up and taking down EC2 instances and other aspects of Pokémon's environment.

"The on-demand platform and services of AWS and CrowdStrike products has been huge for us in this regard," he said.

So has the integration of systems.

"One of the foremost challenges was finding a platform that could allow our analysts to pivot seamlessly between on-prem systems and AWS," Visneski said. "Going back to survival of the fastest, it's really hard if your analysts have to flip between multiple screens, multiple tools and authentications. CrowdStrike allows us to integrate a whole bunch of different activities. As a result, it serves as a good foundation for everything else that we do."

The solution's success so far, especially its integration of different systems and activities, has Vineski eagerly looking ahead.

"The panacea we in security drive towards is as close to a single pane of glass as possible so that we can reduce the time it takes to respond to an event, reduce the amount of blowback that happens when an architect makes a change that changes the stack that may affect another part of the stack. The CrowdStrike Falcon platform's ability to integrate with our environment made it an easy choice."

"We are excited about the future, especially around Falcon Discover for AWS," Vineski said.

"One thing we appreciated with CrowdStrike is a transparent flow of data back and forth; we don't feel we are alone. We have folks we can call if we get in trouble. We cannot be everywhere at all times and see everything, so having a business partner like CrowdStrike help us through this stuff is incredibly important".

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