Case Study

BINARY DEFENSE™

Global retail technology provider finds true partnership with Binary Defense

Business

National Cash Register (NCR) is the world's enterprise technology leader for restaurants, retailers and banks

Challenges

Global customer base with complex systems and processes

A cyberattack could have devastating effects on NCR and its customers

Results

A true cybersecurity partner with open lines of communication

Proactive measures prevented malicious activity from doing damage

"NCR wanted somebody who put the customer first, where we didn't feel like a number or just another contact from a third-party provider." -Paul Farley, Deputy Chief Information Security Officer, NCR

Point-of-service technology provider with global reach

National Cash Register (NCR) is the world's enterprise technology leader for restaurants, retailers, and banks. As the #1 global point-of-service software provider for retail and hospitality, and the #1 provider of multi-vendor ATM software, NCR creates software, hardware and services that run the enterprise from the back office to the front end and everything in between.

NCR's customers have very complex businesses, and they trust that NCR's systems and processes run efficiently. If a cybersecurity event were to interfere or interrupt their customers' service, it would obviously have a huge impact on trust—not only between NCR and their customers, but also between their customers and their end users. Not surprisingly, an organization like NCR is very appealing to a cybercriminal—a successful breach would yield a payload of financial data and customer information. Sophisticated, multi-layered cybersecurity protection is a necessity for NCR to keep cybercriminals at bay.

Putting the customer first

Unsatisfied with NCR's current cybersecurity solutions provider, Paul Farley, Deputy Chief Information Security Officer, knew he needed a partner that could ensure that NCR's global business customers would run smoothly and without interruption of service. Finding a partner that would engage with his team on a high level was critical for Farley, as well. "Security never sleeps and neither can our security provider," he said. "NCR wanted somebody who put the customer first, where we didn't feel like a number or just another contract from a third-party provider. Binary Defense has lived up to that and exceeded that goal."

Binary Defense was a great fit for NCR, as it is staffed 24/7/365 by a team of security experts who act as an extension of NCR's in-house team. The Binary Defense Security Operations Center (SOC) monitors the entire NCR environment, including log data from network infrastructure, as well as on 34,000 endpoints (employee workstations), for suspicious activity and works with NCR to remediate any issues that arise.

Farley saw value in the relationship with Binary Defense from day one. "It's not just about opening tickets and acting on a transactional basis. As soon as we engaged with Binary Defense, we heard feedback on what we're watching, how we're alerting … so that together we could do a better job," he said. "The staff at Binary Defense are accessible. They are on a first-name basis with our security team inside NCR. Everyone from the analysts to senior management."

Binary Defense SIEM

Helps businesses turn mountains of log data into actionable information

24/7 Around the Clock event monitoring

Your resource for monitoring, tuning and deploying of SIEMs

No need to hire additional staff as we monitor 24/7/365

Filter the noise and save time from combing through alarms

“Binary Defense is good at what they do. They get results.”
-Paul Farley

Proactive hunting uncovered malware threat

In addition, Binary Defense provides proactive threat hunting services to NCR. Threat hunting is a service wherein a security expert looks for attacks that have evaded other methods. Through threat hunting, the team discovered a malicious script an employee had unknowingly downloaded that had the potential to have done damage. The threat hunting team alerted Farley to the situation and worked with him to determine the scope of the threat. Without this service in place, NCR may not have detected any suspicious activity.

The Binary Defense threat hunting team also shares research with its customers. When the team uncovered a new malware variant, they reached out to NCR proactively to inform them of their findings, which helped NCR develop preventative measures to protect against the malware.

Sharing core organizational values

“Binary Defense is good at what they do. They get results. They have the technical expertise and the depth that they can support me if I need to ask for help with a hard problem. When you combine that with the communication with the team and the seamlessness with which we deployed, it really felt very natural working with them,” Farley said. “And I think that’s important because this is hard. Security is hard. There’s a lot of pressure and you have to have solid relationships and foundational practices or you’re not going to succeed.”

He truly thinks of Binary Defense as a partner and an extension of the NCR team, as the two organizations share core values. “Our founder says to ‘treat every customer as though they’re your only customer,’” said Paul. “That’s what we feel like we get from Binary Defense. Binary Defense is very customer-focused and proactive.”

To see how Binary Defense can help protect your organization from cyberattacks, visit BinaryDefense.com/Cybersecurity-Solutions.