CUSTOMER SUCCESS STORY

Strengthens security of customer information, reducing the likelihood of a data breach

Provides granular, software-defined network security across data centers and clouds

Enables more proactive security management while reducing operational costs

Ceridian Improves Application and Network Security with VMware

Given the nature of Ceridian's business as a leading HCM provider, it handles personal identifiable information (PII) about its customers' employees. Ceridian maintains a high level of trust with its customers and is liable for the personal information it processes. To improve and evolve its security posture, Ceridian deployed VMware AppDefense to protect applications running on VMware vSphere virtual machines and adopted network virtualization supported by VMware NSX.

Improving application security for HCM solutions

Ceridian's most important asset is customer trust. Faced with rapidly evolving threats and a shifting security landscape, the company wanted to add more layers of security solutions to protect the personal information of its customers' employees.

"As an end-to-end human capital management provider, we help our customers manage the hire-to-retire lifecycle," says Warren Perlman, CIO at Ceridian. "That's a big responsibility, and quite honestly, it will always make us a target. To avoid a data breach and all the reputational and financial damage that comes with it, we're continually investing in security solutions that will keep us a few steps ahead."

CERIDIAN

Ceridian is a leading provider of human capital management (HCM) software, transforming the employee experience with Dayforce—a single solution that combines payroll, human resources (HR), benefits, workforce management and talent management. Its cloud-based HCM applications help companies attract and hire the best employees, access real-time payroll and give employees the information they need to make faster, better decisions.

INDUSTRY

Business Services (HCM)

HEADQUARTERS

Minneapolis, Minnesota

VMWARE FOOTPRINT

VMware vSphere® 6.7
VMware AppDefense™
VMware NSX®
VMware vRealize® Network Insight™
VMware vRealize Automation™
VMware vRealize Operations™
VMware vSAN™

RELATED CONTENT

CIO video
Video

vmware®

LEARN ABOUT CERIDIAN'S DIGITAL TRANSFORMATION

SEE HOW CERIDIAN IMPROVED TIME TO MARKET, SECURITY

With a heterogeneous technology infrastructure and multiple vSphere deployments across the U.S., the U.K. and Canada, Ceridian needed a way to protect its HCM solutions at the hypervisor layer to immediately block any suspicious application behavior. It also wanted to enable more proactive security management with notifications and by increasing visibility into network and application traffic. In addition, as Ceridian modernizes its data centers and integrates with public cloud technologies, it wanted to simplify network security and improve disaster recovery (DR).

Fortifying while streamlining

To bolster application security, Ceridian deployed AppDefense in a U.S.-based trial. AppDefense leverages the vSphere hypervisor to provide visibility into behavior and build a least-privilege security model for Ceridian's customer-facing HCM applications. AppDefense manages the intended state of an application, then uses vSphere to detect and control deviations from that intended state. When a threat is detected, AppDefense can respond automatically, if necessary.

"What AppDefense brings to the table is the ability to block processes from running on the fly, and immediately lock down and protect our applications to prevent customer data from being compromised," says Kevin Young, senior systems engineer at Ceridian. "It also gives us greater insight into what's happening, so we can make the best judgments on how to further secure our environment."

The trial proved the value of AppDefense, and Ceridian soon began rolling it out globally. The company also changed its approach to network security, replacing physical security solutions with network virtualization using NSX. AppDefense integrates with NSX to provide adaptive micro-segmentation and a comprehensive, zero-trust model to secure applications and networks deployed in private or public cloud environments.

"We've always done network segmentation, but scaling and maintaining it was becoming a VLAN nightmare, creating issues with change management and control," says Perlman. "NSX simplifies all that. It also allows us to recover applications without changing the IP address of the server, which has a massive impact on our recovery objectives."

> "The data security track record of any SaaS provider is critical to prospective customers. With VMware solutions, Ceridian can continue to use its security leadership as a selling point to win new business."
>
> WARREN PERLMAN
> CIO, CERIDIAN

To gain additional visibility into network behavior, Ceridian deployed VMware vRealize Network Insight for intelligent operations.

"vRealize Network Insight gives me network visibility that previously would have taken multiple people and multiple sessions to gather," says Young. "Having that information directly visible and available is hugely beneficial to a systems engineer."

More proactive security management and increased visibility

With AppDefense, NSX and vRealize Network Insight, Ceridian makes its applications and network even more secure, keeping customers' data protected and their trust intact. "The data security track record of any SaaS provider is critical to prospective customers," explains Perlman. "With VMware solutions, Ceridian can continue to use its security leadership as a selling point to win new business."

Adds Young, "AppDefense provides a real-time map of what's happening in our environment. We can see the services that are running, the inbound and outbound connections, and how those evolve and change over time. We can see if someone is using a system in a way that it wasn't designed to be used, and provide education on how to better use the system to reduce business risk."

The VMware solution enables more proactive security management while reducing operational costs, allowing infrastructure and operations teams to be more proactive.

"Getting real-time access to application and network security information without spinning up a team of people on the network side to help diagnose a potential issue is a beautiful thing," says Perlman. "It's not costing us hundreds or thousands of dollars an hour as we troubleshoot, so there's significant cost savings from an operations standpoint."

NSX improves security and consistency by allowing Ceridian to specify granular, software-defined network security policies across data centers and clouds. And by maintaining the same IP address scheme for application servers during failover, it enables near-instant application recovery, accelerating Ceridian's formal recovery time objective (RTO) sixfold and recovery point objective (RPO) fourfold.

"NSX makes it so that we're all looking underneath the same curtain, which has enabled the trust and validation we need to meet the requirements we've put forth for our security posture," says Perlman. "It also brings us much closer to true disaster recovery failover with no impact to end users."

Looking ahead

As Ceridian retires legacy data center architectures and integrates more public and private cloud technologies, it will use VMware NSX-T™ to extend network virtualization and security beyond vSphere environments.

"At the end of the day, avoiding any impact to the people who use our product is our biggest concern," says Perlman. "We never want a person to go unpaid, and we never want a person to have their information stolen and used against them in any way whatsoever. VMware helps us prevent data breaches by securing critical workloads."

@Ceridian addressed its security needs by protecting its human capital management applications with VMware AppDefense and micro-segmenting its network using VMware NSX. #VMware

---