Customer
Case Study

Modern Woodmen Enables Segmentation, Network Detection and Response

Industry
Financial services and insurance

Location
Rock Island, Illinois

VMware footprint
VMware NSX-T™

VMware partner
27 Virtual

Key challenges
- Implementing micro-segmentation policies was challenging
- Heterogeneous infrastructure was hard to manage across dashboards
- Network complexity contributed to an expanded threat surface

Solution
Migrated from VMware NSX® Data Center for vSphere® to NSX-T.

Business benefits
The modern network infrastructure meets the company's networking and security needs. Internal users and members have secure anytime, anywhere access to the apps they need.

Modern Woodmen of America is a fraternal financial services organization offering life insurance, retirement planning, and fraternal benefits to more than 740,000 members nationwide. A lean organization with less than 500 employees, Modern Woodmen relies on a robust self-service website where members can access accounts, manage their portfolio, and pay their bills on their terms whenever and wherever they want. Reliable connectivity and security of the applications—regardless of where users log in—is a critical factor in delivering positive and convenient experiences to members.

An expanding threat vector in a modern world

According to Modern Woodmen's senior network engineer, Zach Lotz, the company was using VMware NSX Data Center for vSphere to manage its network backbone across their data centers. However, NSX Data Center for vSphere could only manage traffic flowing across virtual infrastructure, leaving about 20 percent of traffic that was running on physical devices unmanaged. The inability to manage and monitor 100 percent of east-west traffic at scale prevented Lotz from setting up micro-segmentation policies across multiple environments, creating a security gap.

"The inability to set up segmentation policies and east-west firewalling across dev, stage and prod environments created a security gap that could be exploited by sophisticated threat actors," Lotz said. "Once an attacker gained access, they'd have free reign to spread throughout the network."

"[The migration to NSX-T] allows us to lock down our network to the point where only known traffic can communicate while everything else is blocked."

Zach Lotz, Senior Network Engineer, Modern Woodmen

---

vmware®

A seamless migration managed by experts

Modern Woodmen worked with VMware to modernize its network infrastructure across virtual and physical hardware by upgrading to VMware NSX-T. Built for modern networks, NSX-T is uniquely designed to go across virtual, cloud and data center environments with an API-driven architecture, built-in distributed security, and streamlined operations.

VMware introduced Modern Woodmen to 27 Virtual, a progressive cloud infrastructure solutions provider with specific expertise in VMware products and support services.

"27 Virtual was great. They helped us set up a plan and timeline and walked us through every step of the process," Lotz said. "However, most importantly, 27 Virtual let us drive the migration internally, which gave us the opportunity to get hands-on training and learn the software by working with it ourselves. It wasn't a 'here, we'll do it for you and then drop it in your lap' type of engagement. We were put in a position to continue to manage the environment on day two and optimize our investment."
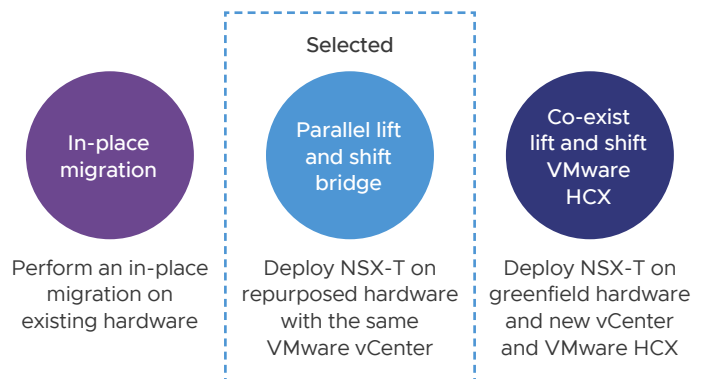
Migration with no disruption

According to Lotz, the entire migration took less than 40 hours over the course of four weeks, and the only reason it took that long was because Lotz made the decision to only work on the migration during off-hours in the evening or on the weekend.

Once the infrastructure was in place, the actual migration was pretty seamless, resulting in just a few seconds of downtime. Lotz actually used two methods to do the migration: a bridge and a hard cutover. Most environments were simply shut off on NSX Data Center for vSphere and then turned back on with NSX-T. For more critical network segments, such as SQL databases with member information, Lotz used a bridge to connect NSX Data Center for vSphere to NSX-T.

"The downtime was less than two seconds in most cases—a very manageable disruption for our business," Lotz said. "You'd have to be at the perfect place, the perfect time, clicking the button at the exact time to realize that the application wasn't available. No one, not a single internal user or member, was impacted."

Reduced threat surface and a single pane of glass

Migrating to NSX-T allowed Modern Woodmen to modernize its network backbone across virtual and physical infrastructures across distributed data centers. This allows the company to implement segmentation policies and advanced threat prevention capabilities inside and across segments, preventing potential threat actors from traversing the network. Lotz uses VMware vRealize® Network Insight™ to analyze traffic flows within the network and apply the appropriate tags in real time. NSX-T then segments the traffic based on these tags.

Selected

In-place migration

Perform an in-place migration on existing hardware

Parallel lift and shift bridge

Deploy NSX-T on repurposed hardware with the same VMware vCenter

Co-exist lift and shift VMware HCX

Deploy NSX-T on greenfield hardware and new vCenter and VMware HCX

vmware®

Enabling a future in the cloud

Modernizing the network through NSX-T will allow Modern Woodmen to continue to evolve its IT operations to better support business objectives. A move to the cloud is inevitable, Lotz admits, but already having NSX-T will streamline the process of moving workloads into a cloud environment without losing the ability to implement segmentation, east-west firewalling at scale, and network detection and response.

Learn more

For more information about how migrating to VMware NSX-T meets the needs of a modern network infrastructure, visit vmware.com/go/v2t.

For more help on migrations

Assess your environment for migration using the migration assessment tool. For any additional help, contact VMware migration specialists.

"The best part of segmentation with NSX-T is the ability to start broad—development versus production—and then go more granular as needed, even down to the application level," he said. "This allows us to lock down our network to the point where only known traffic can communicate while everything else is blocked. Any anomaly is quickly identified and dropped."

On an operational level, the migration from NSX Data Center for vSphere to NSX-T consolidated network traffic management to a single pane of glass. It doesn't matter if a workflow is running on a virtual machine or physical appliance, network administrators have complete visibility and control over that packet from a single GUI, greatly simplifying network management.

vmware®