



Strengthened protection against cyberattacks and data breaches by creating a more intrinsically secure environment



Streamlined security operations, facilitating collaboration and insights to better safeguard financial and personal data



Reduced data center costs by 70 percent, and improved flexibility with a software-only solution

United States Senate Federal Credit Union Makes Security Intrinsic with VMware



UNITED STATES SENATE FEDERAL CREDIT UNION

Like other well-established financial services providers, the United States Senate Federal Credit Union (USSFCU) is committed to keeping personal customer data and financial information secure. But with a customer base that includes high-profile U.S. Supreme Court and U.S. Senate members, USSFCU faces a unique challenge. Especially heading into the 2020 election year, the credit union is a target for hackers all over the world. Expecting the threat of serious infrastructure data breaches to increase, USSFCU needed to refresh its legacy IT environment to fortify security and simplify security operations.

Instead of investing further in expensive physical security appliances that would be time consuming for its five-person IT team to maintain, USSFCU decided to take a software-defined, intrinsic approach to infrastructure security, using VMware NSX Data Center for virtual firewalling and micro-segmentation. It also upgraded its environment based on VMware vSphere to include VMware AppDefense, which provides deep visibility into applications and their behavior. With VMware vSAN encrypting data at rest and VMware vRealize Network Insight delivering intelligent operations, plus VMware Carbon Black App Control to help lock down servers and critical systems, USSFCU is now well prepared to protect its members and their data.

The United States Senate Federal Credit Union provides banking and financial services to more than 32,000 federal employees. Founded in 1935, USSFCU now manages more than \$800 million in assets and works hard to meet customer expectations for quality services online and at its locations in Washington, D.C. and Virginia.

INDUSTRY

Financial Services

HEADQUARTERS

Alexandria, Virginia

VMWARE FOOTPRINT

VMware Carbon Black® App Control™
VMware NSX® Data Center
VMware AppDefense™
VMware vSphere®
VMware vRealize® Network Insight™
VMware vSAN™

RELATED CONTENT

[Customer Success Story](#)
[Blog](#)
[Video](#)



Keeping member data more secure

To keep its members' personal and financial data more secure from outside threats, USSFCU needed to improve infrastructure security, both at the network perimeter and internally. It also wanted to simplify IT management workloads so staff could better monitor the network and prevent data breaches.

"Given our membership, we have to assume we're always under attack," says Mark Fournier, director of IT infrastructure at USSFCU. "We want to constantly improve our effectiveness, agility and efficiency in protecting the financial and personal data of everyone from U.S. Senate administrative staff to senators and their families."

Historically, network security at the credit union had been siloed, with access limited to just a few administrators. Lacking centralized east-west visibility, engineers used open-source port scanning software and manual mapping to understand network communication flows and protocols. Security administration was split between different tools and management interfaces. Wanting to modernize, USSFCU sought a consolidated, intrinsic way to monitor infrastructure throughout its two data centers and three branch offices.

"We needed better visibility into what was happening on our network, as well as the ability to easily segment off virtual machines and applications to prevent the lateral spread of threats," says Corey Primrose, senior security administrator at USSFCU. "At the same time, we wanted to democratize networking and security by making it less arcane and more user-friendly to our entire team."

A flexible, intrinsic solution for security

To take security to the next level, USSFCU deployed NSX to provide network micro-segmentation and perimeter firewalling for its private cloud based on vSphere. When the credit union saw the flexibility that virtualized networking offered, it quickly upgraded to NSX Data Center, a complete L2-L7 networking and security virtualization platform. The solution includes VMware NSX Intelligence™, a native, distributed analytics engine, to provide continuous data center-wide visibility.

"We moved from the original NSX Data Center for vSphere to NSX Data Center because it gives us the ability to accommodate potential future use cases, such as edge services and multi-cloud," says Primrose. "We're in the process of building out a new headquarters and data center, and with virtualized networking and security, we can keep all our options open."

The credit union also upgraded its vSphere environment to include AppDefense, which delivers advanced threat detection and response capabilities fully integrated into VMware vSphere Hypervisor. Instead of trying to constantly watch for attacks, which regularly shift as hackers develop new strategies, AppDefense helps establish a zero-trust security model for applications. AppDefense understands the workloads and intended behavior of applications, so it can detect sudden or abnormal application behavior changes and keep USSFCU members safe by automatically locking down endpoints or blocking individual processes.

"The internal firewall and micro-segmentation capabilities of NSX Data Center enabled us to rapidly deliver on our CIO's zero-trust initiative. Combined with VMware Carbon Black and vSphere with AppDefense, we've simplified our environment while making our security posture much stronger."

MARK FOURNIER
DIRECTOR OF IT INFRASTRUCTURE,
UNITED STATES SENATE FEDERAL CREDIT UNION



“VMware solutions help us solve different security challenges in parallel,” says Fournier. “We can use NSX Data Center for perimeter security and micro-segmentation, AppDefense for detecting unusual behavior and vSAN to encrypt data at rest. Together, they help us seamlessly provide robust protection for our IT infrastructure and our members’ data.”

To further fortify its infrastructure, USSFCU deployed VMware Carbon Black App Control to help secure servers and key systems, prevent unwanted changes and support regulatory compliance. The solution combines application allowlisting, file integrity monitoring, robust device control and memory/tamper protection into a single agent, so only trusted and approved software is allowed to execute on USSFCU’s critical systems and endpoints. By watching for behavioral indicators of malicious activity and conducting continuous recording of attack details, Carbon Black App Control provides USSFCU with rich visibility into suspicious activities.

“VMware Carbon Black gives us peace of mind when it comes to the ever-present and evolving threats of ransomware. Having personally been involved with a number of organizations impacted by ransomware activities, I’ve seen that the resulting costs and damages can be immeasurable. At USSFCU, it’s crucial for us to be able to confidently lock in systems to a known, good state at the time of deployment. This goes a long way to prevent, if not eliminate, the threat of an errant malware process making entry into a protected system. Complementary solutions from VMware, such as AppDefense, bolster our overall level of protection even further,” Fournier says.

Avoiding disruptions and damage

Deploying NSX Data Center has had a transformative effect on how USSFCU protects its infrastructure, enabling the credit union to quickly provision the networking and security services it needs to counter threats and keep members’ data safe. Even if an attacker manages to get through the perimeter, micro-segmentation will protect critical applications and data as automated remediation goes to work.

“NSX Data Center lets us easily run discoveries over groups of VMs and see exactly what’s going on with our network,” says Primrose. “It gives us more proactive security, and when we do need to react, we can do so much faster and with much more granular control.”

Standardizing on VMware security solutions allowed USSFCU to remove multiple legacy toolsets, giving the credit union single-pane-of-glass security management. As a result, the IT staff no longer needs to manage multiple firewalls or antivirus solutions to keep ahead of potential attacks. Tight integration between NSX Data Center and AppDefense also improves operational effectiveness and saves time by automating previously manual tasks.

“The ability to directly see how systems interact with each other enables more people to engage in security conversations. We’re improving our understanding of data flows and network structure, which results in a stronger data protection strategy,” Fournier says.

With Carbon Black App Control, USSFCU has the control it needs over its environment to prevent unauthorized changes to applications and files. The solution streamlines the USSFCU IT team’s work by automating approvals of trusted software and eliminating the burden of allowlist management.

“We operate in a ‘default deny’ state, which means that all newly discovered applications or vendors must go through a review and approval process,” Fournier says. “Certainly, we want to empower our colleagues to have the right tools, but we have to do it within the confines of a safe and stable environment. VMware Carbon Black bolsters our outreach efforts with the rest of the organization, giving people an extremely clear indicator when an application doesn’t meet approval, combined with an easy path to kick-start the process. It helps keep us all on the same page and reduces the operational IT deficit when it comes to catching up on the things we didn’t know about.”

USSFCU’s approach has delivered greater IT efficiency along with a 70 percent reduction in data center costs. “The internal firewall and micro-segmentation capabilities of NSX Data Center enabled us to rapidly deliver on our CIO’s zero-trust initiative. Combined with VMware Carbon Black and vSphere with AppDefense, we’ve simplified our environment while making our security posture much stronger,” says Fournier.



Looking ahead

As USSFCU prepares to bring its new data center online, VMware solutions will enable the credit union to provide world-class financial services security from day one, without expanding its IT team.

“Our new headquarters’ data center will be our technology crown jewel,” says Fournier. “VMware solutions with intrinsic security will allow us to deploy faster, reduce costs, use less space and better protect our members’ personal and financial information.”



Learn how @USSFCU continually improves networking and security with #VMware to intrinsically protect its members’ data.