CUSTOMER SUCCESS STORY

Protecting the USSFCU brand and customer data with a Zero Trust strategy to mitigate security risk

Providing micro-segmentation, secure VDI and advanced threat protection via a single platform

Simplifying operations and automating policy management

Scaling east-west protection faster and at lower cost than with traditional, hardware-based alternatives

Protecting Customers and Staff with VMware Service-defined Firewall

The United States Senate Federal Credit Union (USSFCU) serves high-visibility clients, including U.S. senators, making the protection of sensitive data a top priority. The organization had already empowered employees with secure, digital workspaces with VMware Horizon and VMware Workspace ONE. As part of its continuous improvement strategy for infrastructure security, USSFCU turned to VMware for a unified solution that stretches from the perimeter to the data center, across its network and virtual desktop infrastructure (VDI), with granular policy controls to protect applications, services and workloads.

Accelerating security transformation

The more USSFCU's acting CIO learned about the security capabilities inherent to VMware solutions starting at the hypervisor level, the more excited he was to leverage those more fully to enable a Zero Trust architecture and better protect USSFCU's customers and employees from data breaches. "We had to overcome silos to address a convergence of risk management imperatives, from endpoint hazards to the potential for threats moving laterally through the data center," says Mark Fournier, interim CIO for USSFCU.

UNITED STATES SENATE FEDERAL CREDIT UNION

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 $1 billion 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 NSX® Data Center
VMware Carbon Black® App Control™
VMware vRealize® Network Insight™
VMware vSphere®
VMware vSAN™
VMware Horizon®
VMware Workspace ONE®
VMware Professional Services

RELATED CONTENT

Video and Success Stories

To prepare for its deployment of VMware NSX Data Center, Fournier and his team ran VMware vRealize Network Insight, which quickly helped them gain visibility into the kinds of network traffic, while discovering issues they might want to address with NSX micro-segmentation policies. With a good plan in place and VMware Professional Services support, USSFCU was able to go from design to production with NSX in just one week.

Intrinsic security with deep visibility

The team moved quickly to extend VMware Service-defined Firewall capabilities, further bolstered by VMware Carbon Black App Control. USSFCU started with network segmentation and swiftly applied micro-segmentation for policy-driven, application-level controls to isolate and secure workloads. The IT team uses stateful Layer 7 controls with applications such as Microsoft SQL Server to inspect patterns, and either allow or disallow particular protocols and ports. With the distributed intrusion detection and prevention system (IDS/IPS) that is part of the Service-defined Firewall functionality, USSFCU can detect lateral threats more efficiently than discrete appliances.

"With our VMware Service-defined Firewall, we fortified our environment with streamlined east-west monitoring, remediation and blocking capabilities that deliver impressive visibility and granular control," Fournier says.

> "With our VMware Service-defined Firewall, we fortified our environment with streamlined east-west monitoring, remediation and blocking capabilities that deliver impressive visibility and granular control."
>
> MARK FOURNIER
> INTERIM CIO,
> UNITED STATES SENATE FEDERAL CREDIT UNION

Protecting digital workspaces

USSFCU protects Horizon virtual desktops by using NSX to segment the digital workspaces and inspect their traffic flows for any threats trying to move laterally. Firewall policies are applied to VDI workloads to mitigate threats from otherwise vulnerable users and desktops. When larger numbers of USSFCU employees recently needed to work from home, policies could automatically be applied to the expanding VDI pools for faster and safer scaling of digital workspaces. Identity-based firewalling allows USSFCU to better protect against threats while taking into account user roles and providing more customized experiences regardless of the end user's location or device.

"VMware delivers simplicity combined with a measure of efficiency. VMware's consistent standards intelligently leverage a common underlying platform to provide value. For us, it means flattening the learning curve even as we expand our capabilities, while helping our team collaborate with greater agility," says Fournier.

U.S. Senate Federal Credit Union #USSFCU mitigates risk with VMware Service-defined Firewall built on #VMware NSX.