Customer E-book: How Companies Protect Their Apps and Data with NSX Service-defined Firewall
Stop the Lateral Spread of Threats and Eliminate Security Blind Spots

East-west firewalls are the new security battleground. The scale and distributed nature of networking today has expanded threat surfaces—making breaches all but inevitable. Organizations need to shift their focus to stopping the lateral movements of threats between devices, systems and environments. VMware Service-defined Firewall (SDFW), a stateful layer 7 firewall, gives organizations visibility into and control over east-west traffic—simply, at scale and without any network changes. This software-defined approach makes it practical to implement network segmentation and granular segmentation to achieve zero trust, prevent the spread of advanced threats and meet compliance requirements.

Read on to see how VMware customers are able to secure east-west traffic at scale with SDFW.
Company Background

Industry: Education

Location: Texas, USA

Global information, analytics and solutions company IHS Markit provides data-driven insight for more than 60,000 government and corporate customers across 120 countries.

Solution

IHS Markit deployed NSX Service-defined Firewall to better secure its hybrid cloud environment. A software-defined approach to securing workloads ensures that policies are extended out beyond the on-premise data center and are applied appropriately to workloads on any type of underlying infrastructure—whether it is on-premises, AWS, Google or Azure. This includes Layer 7 firewalls that ensure policy enforcement with intelligence closer to the source.

Challenges

Enable an agile development workforce that needs to iterate and push code to customers quickly with a high degree of automation

Move from a public cloud IT focus to a private cloud initiative to enable better business growth

Cut infrastructure costs without sacrificing governance and security requirements

Key Benefits

Reduces development cycles from one month to a single week - allowing the company to meet rising customer demands

Enables consistent security across infrastructures for deployment of flexible hybrid cloud environments

Reduces complexity while saving costs by replacing physical firewall appliances with a software-based approach
With VMware Service-defined Firewall, we can utilize segmentation across every environment—containers, to the public cloud environment with AWS and Azure, to on-prem—with a common security footprint. It makes operations’ life easier.

Andrew Hrycaj
Principal Network Engineer
IHS Markit
Company Background

Industry: Financial Services

Location: Virginia, USA

A financial cooperative designed to help its members achieve financial success, USSFCU serves more than 32,000 members, including high-profile U.S. Supreme Court and Senate members, and manages total assets in excess of $1 billion.

Challenges

Introduce new products and services to help meet its members’ evolving online banking needs and expectations

Large numbers of employees recently needed to work remotely in a secure way

Replace legacy hardware-based network infrastructure that was complex, expensive and hard to scale

Solution

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. USSFCU started with network segmentation and swiftly applied segmentation for policy-driven, application-level controls to isolate and secure workloads.

Key Benefits

Helps deliver innovative financial services to a growing customer base without increasing security risks

Provides segmentation, secure VDI and advanced threat protection via a single platform

Scales east-west protection faster and at lower cost than with traditional, hardware-based alternatives
With our NSX 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, USSFCU
Company Background

Industry: Insurance
Location: New York, USA

Preferred Mutual provides property and casualty insurance coverage to more than 232,000 individual and business customers through a network of more than 500 independent agents throughout New York, New Jersey, Massachusetts and New Hampshire.

Solution

Preferred Mutual uses NSX and Horizon to maximize remote employee and IT staff productivity while maintaining security of sensitive data. Preferred Mutual uses the Service-defined Firewall capability within NSX to segment its PCI network to meet security and compliance requirements. The company’s ultimate plan is to extend NSX firewalling to their entire environment.

Challenges

Enable a distributed workforce that needs to provide hyper-localized service to customers, without increasing security risks
Avoid the high costs and complexity typical of building out a physical network segment for PCI-DSS compliance
Meet data security requirements associated with HIPAA compliance

Key Benefits

Empowers a remote workforce with the fast, reliable application and data access needed to provide localized service to customers
Segments PCI network without costly purchases of traditional firewalls
Meets HIPAA compliance requirements in the data center
NSX makes it easy to operationalize segmentation, enabling us to work at a much faster pace than we could with other products.

Matthew Monahan Senior Systems Engineer, Preferred Mutual
Company Background

Industry: Media

Location: Milan, Italy

Sky Italia is part of Sky Group, Europe's leading entertainment company, which has recently become part of Comcast NBC Universal. As a separate entity, Sky Italia boasts a 4.82 million-subscriber base.

Challenges

Increase the service’s on-demand streaming capabilities for users without compromising security

Deliver content from local, remote and public cloud data centers and always in a secure environment

Replace expensive legacy network architecture that couldn’t provide the necessary scalability and flexibility to meet business goals

Solution

Sky Italia adopted the entire VMware Software Defined Data Center stack, including VMware NSX. The company outlined the profile of application flows, using vRealize Network Insight (vRNI), and implemented the correct and necessary firewall rules for each individual flow, using the NSX Service-defined Firewall, to achieve granular segmentation. Once the rules for a specific application have been defined, the operational commitment is completely automated and, importantly, the rules applied to the application are always "clean". This allowed Sky Italia to eliminate spend on dedicated firewalls for on-premises to public cloud secure interconnections by using the NSX firewall and seamlessly moved workloads between environments.

Key Benefits

Enables the creation of a secure, flexible and scalable streaming architecture for business applications

Displaces dedicated firewall appliances, leading to cost savings and simpler security architecture

Increases operational agility through automation of deploying security policies and elastic scalability of firewall capacity
VMware Service-defined Firewall allows us to reduce operational overhead and operational effort, which is present in legacy and more traditional solutions. Again, there is a big benefit in terms of flexibility and time to market—those are the two main reasons that facilitate this adoption.

Angelo Scano
Senior Research Engineer, Sky Italia
Company Background

Industry: Education
Location: Texas, USA

ESC Region 100 provides professional development, technical assistance and management of educational programs to 77 public school districts and 66 charter campuses—serving 70,000 educators and 578,000 students across 10 counties.

Challenges

- Protect school infrastructure and personal data in line with compliance requirements
- Level the field so smaller, rural schools can access resources on par with larger, more urban schools
- Enable more efficient remote access to apps and desktops

Solution

After a costly and disruptive recovery from a ransomware attack that crippled its infrastructure for several days, ESC Region 11 implemented VMware Service-defined Firewall to prevent the lateral spread of future threats. Deployed alongside NSX Data Center as part of a layered approach to help prevent and mitigate damage from future attacks, VMware Service-defined Firewall allows Region11 to implement granular firewalling and security policy enforcement for every workload in the data center.

Key Benefits

- Enhances security of school data and infrastructure to help prevent attacks and mitigate damage
- Improves access to curriculum and programs for schools, even those that are smaller or more rural
- Boosts productivity with digital workspaces for access to apps from any device, anywhere
NSX just stood out head and shoulders above the rest with its price point for value, the ability to extend to the cloud [and] the ease of use. Since NSX we’ve been attacked the same way as years before, and it didn’t take us down. Quite honestly, nobody even knew we were attacked.

Rory Peacock
Deputy Executive Director of Technology, Region 11
Company Background

Industry: Education

Location: Preston, England

The University of Central Lancashire (UCLAN), based in North West England, is one of the UK’s largest universities with a student and staff community approaching 38,000. The institution is dedicated to creating real-world learning experiences for its students and embracing a broad pool of academic talent.

Challenges

Create a "learning without barriers" environment that would allow students to study any way they wish, securely, from anywhere on or off campus

Empower this open learning environment without adding IT complexity

Ensure the university complies with stricter General Data Protection Regulations (GDPR)

Solution

UCLAN deployed NSX Service-defined Firewall (SDFW) to implement a multi-layered, Zero-Trust approach to its security posture, moving to a place where all traffic is treated as "untrusted" and in need of protection. NSX attaches policies to each workload and automates policy creation and management. Once a network security policy is defined for one server, all subsequent web servers will adhere to the same policy without new rules needing to be added each time one is provisioned—eliminating the need to manually configure each new environment.

Key Benefits

Ensures all systems and web servers are secure and compliant, no matter where students need to browse

Decreases reliance on manual workflows through automation, reducing IT complexity and overhead

Keeps the university in compliance with new GDPR regulations—eliminating the chance UCLAN could be hit with heavy fines
VMware NSX is a breath of fresh air. Obviously, our students don’t know their seamless technology access is enabled through security at the network level, but they are very appreciative of the frictionless IT and free environment it’s helped us create.

Frank Wadmore
IT Networks and Security Manager
UCLAN
Company Background

Industry: Financial Services
Location: Prague, Czech Republic

Prague Stock Exchange is the largest and oldest securities market organizer in the Czech Republic. PSE group manages highly sensitive data, similar in nature to banking information and accordingly subject to security requirements.

Solution

The Prague Stock Exchange deployed NSX Service-defined Firewall (SDFW) to achieve granular policy management through segmentation. This enables the creation of two separate working environments for each internal user—one protected and fully virtualized with output only to a display, and another unprotected, in the form of a standard desktop, potentially also virtualized. Users can use a single computer for both workplaces.

Challenges

Secure dematerialized securities information—extremely sensitive data on par with bank account information
Reduce operational costs required to monitor, manage and secure IT infrastructure through system consolidation and optimization
Maintain compliance with government regulations when handling sensitive customer data

Key Benefits

Improves east-west security inside the data center to help stop the lateral spread of threats and protect sensitive data
Saves operational costs through the simplification and consolidation of IT infrastructure and systems via software-defined firewalling
Meets compliance requirements for sensitive customer data
The implementation of the NSX platform delivers unprecedented possibilities for micro-granulation of security settings, and hence more selective and improved protection of individual applications.

Miroslav Prokes
Director of ICT development and operations, Prague Stock Exchange
Company Background

Industry: Technology

Location: Brno, Czech Republic

RWS Moravia helps companies reach more customers around the world through software localization—the process of providing high quality, specialized translations tailored to target customers and local conditions. Moravia has translated software into 330 languages for more than two billion users.

Challenges

Provide its globally-distributed employees and freelance translators with fast, reliable and secure access to applications in the company’s private cloud

Reduce the attack surface inside the data center to stop the lateral spread of threats

Ensure IT infrastructure and strategy can be scaled to support planned business innovation and growth

Solution

RWS Moravia deployed NSX Service-defined Firewall to automate segmentation of its data center environments. The implementation and automation of object- and policy-based administration allows RWS Moravia to deploy security groups based on user and application type. Dynamic rules-based management makes it easy to create, update and scale the network based on current needs without adding risk.

Key Benefits

Ensures fast, reliable and secure application access for more than 10,000 distributed users

Provides unprecedented visibility and protection for applications, data and users from endpoint to cloud for improved security posture

Automates security policy management for improved operations and reduced complexity and costs
The main advantage of NSX Service-defined Firewall is meeting the high demands on data center security without compromising performance. With a virtualized network we have also set the foundation for fully automated infrastructure and we can respond quickly to the needs of our customers and software development teams.

Přemek Vala
CIO, RWS Moravia
Company Background

Industry: Law Enforcement

Location: Florida, USA

Osceola County Sheriff’s Office serves 360,000 residents of Osceola County, Fla. Its 500 officers and 300 civilian support staff work with the community to provide a safe and secure environment to live, work and visit.

Solution

Osceola County Sheriff’s Office uses NSX Service-defined Firewall for segmentation and securing east-west traffic inside the data center. The agency is able to separate criminal justice data from data not covered by CJIS standards and gains eye-opening insights into traffic moving through the network, allowing IT staff to create appropriate port rules and better lock down traffic.

Challenges

Provide security for sophisticated, modern technology used for law enforcement activities

Meet compliance requirements mandated by state and federal standards for data and application security

Simplify security operations across an evolving network architecture

Key Benefits

Hardens security with improved visibility and control of internal traffic

Adheres to Florida Department of Law Enforcement (FDLE) and FBI Criminal Justice Information Services (CJIS) standards

Simplifies operations through end-to-end security controls from the end point to the data center
VMware does so much for security, virtualization and endpoint management that it seemed like a smart move to switch to VMware.

Daniel Caban
CIO, Osceola County Sheriff’s Office
Company Background

Industry: Financial Services

Location: Myanmar

Established in 1993, Yoma Bank was one of the first private banks in Myanmar. Today, it is the fifth biggest bank in Myanmar, with 80 branches throughout the country.

Solution

Yoma Bank worked with VMware to build a software-defined data center that could extend banking services online and to mobile devices and would be simple to monitor, manage and secure. The Bank uses NSX Service-defined Firewall to enable a Zero Trust security model through segmentation. In turn, this allows the bank to implement granular firewalls and security policy enforcement down to the virtual machine—isolating the systems that store, process or transmit sensitive data.

Challenges

Provide 24x7 online and mobile banking services to meet rising customer expectations in a developing country

Build a modern, flexible and scalable IT infrastructure capable of meeting that challenge without adding complexity

Ensure data security and compliance for these innovative banking services

Key Benefits

Enables the first mobile financial service in the country, bringing financial inclusion to the unbanked without putting data at risk

Increases operational efficiency, which has resulted in a 30 percent reduction in opex

Meets compliance requirements—previously an inhibitor to business growth
We depend on NSX to ensure the security of sensitive customer data and provide services we couldn’t before. It makes network segmentation possible for the first time.

— Kyaw Soe Lin
CTO, Yoma Bank
Get Out of the Way of Your Developers

Development velocity and business agility require flexibility up and down the network stack. Our software-defined approach to distributed firewalling allows organizations to secure all traffic from the edge to the data center in a simple, cost-efficient manner. NSX SDFW eliminates security blind spots by making east-west firewalling practical at scale, so you can stop the lateral movement of threats inside the data center and meet compliance requirements. It’s time to empower your developers and protect modern applications.

See the product demos

Try it for yourself with a Hands-on Lab

Get a free trial of VMware NSX-T

Talk to your VMware sales representative or partner to dive deeper