CASE STUDIES: SECURING APPLICATION INFRASTRUCTURE

Why Organizations Are Leveraging Micro-segmentation for Better Protection

vmware®

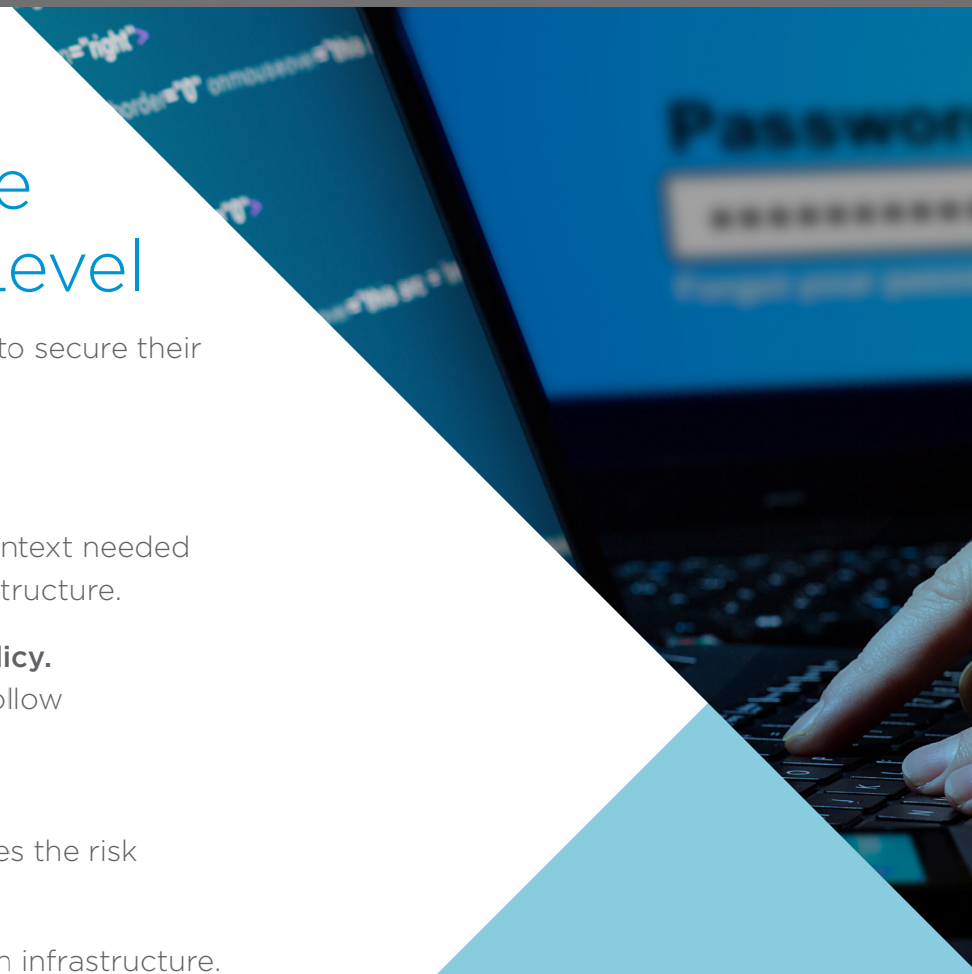
Data Center Threats Are Evolving Fast

As technology continues to advance, so do security threats. Modern-day attacks are not only smart and sophisticated, they're also able to breach the perimeter firewalls that traditional data centers rely on. As a result, organizations of all sizes are racing to protect sensitive information that affects both users and the business. And the expenses are adding up.

The high cost of cybercrime includes data center outages, security breaches, and reputation damage. According to the Ponemon Institute, the average cost of a data breach rose to $4M in 2016. That's $158 per stolen record[1]—far beyond what the average IT budget can accommodate.

As IT devotes more time and energy to fighting back against malicious threats, it leaves little left over for innovation. Combined with the pressure to get products and services to market faster than competitors, organizations are expending more resources than ever to keep up. Agility is a must in the fast-paced digital economy—but without the right security solution, data will continue to be at risk, and organizations will continue to fall behind.

1. 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute, June 2016



Better Security Starts at the Application Infrastructure Level

To protect against these fast-evolving threats, organizations need to secure their application infrastructure.

A secure application infrastructure has three main components:

1. **Virtualization: Abstraction of applications from infrastructure.**
   Virtualization enables full visibility into the data path, and the context needed to understand applications and the way they interact with infrastructure.

2. **Micro-segmentation: Granular application-aligned security policy.**
   The creation and automation of granular security policies that follow applications and workloads across public and private clouds.

3. **Encryption: Hypervisor-based infrastructure protection.**
   Workload-level encryption on individual hypervisor hosts reduces the risk of compromised networking components.

Micro-segmentation plays a critical role in securing your application infrastructure.

Let's take a closer look at how it works.

Stop Security Threats in Their Tracks with Micro-segmentation

Perimeter firewalls provide only one layer of threat protection. Micro-segmentation protects the data center from the inside out. It provides distributed firewalling that secures all workloads and east-west traffic across the data center—without the use of additional physical firewall appliances. That means individual workloads and applications are safe, no matter where they are in the data center.

With micro-segmentation, you can:

- Stop the lateral spread of threats
- Reduce the manual effort and cycle time for security tasks
- Enable attribute-defined security policies

In the pages that follow, we'll look at how organizations around the world are using micro-segmentation to enhance security, increase agility, and gain a more solid foothold in today's highly competitive business landscape.

WHAT IS MICRO-SEGMENTATION?

Micro-segmentation is an approach that enables organizations to build security into the DNA of the data center. Distributed firewalling protects individual workloads, while networks are isolated to create a Zero Trust environment.

This ensures that all traffic inside the data center is legitimate—so even if a threat slips past perimeter security, it can't go far. With micro-segmentation, you can achieve granular security that sticks with your applications, no matter where they are.

Case Studies

Americas

- Armor
- Vallejo Sanitation

Europe, the Middle East, and Africa

- Herning Kommune
- Prague Stock Exchange

Asia-Pacific Region

- Zettagrid
- Japan Advanced Institute of Science and Technology (JAIST)

Armor

As a data security company, Armor protects its clients' critical data workloads with robust security and infrastructure. That means it needs a solution it can trust to keep user and business information safe for industries like healthcare, government, and more. It chose VMware NSX® because it gives Armor the ability to keep all of its customers' data secure with micro-segmentation in a multi-tenant environment.

CHALLENGES	SUCCESSES
Modern attacks are so sophisticated, they can even shut down a hospital ICU	Micro-segmentation gives each customer a tight security wrapper from day one
Multi-tenant nature of the cloud makes it difficult to orchestrate security	The highly programmable NSX platform protects individual servers with unique security needs
Creating complex, cloud-based networks with high security requirements is a difficult, time-consuming task	NSX enables the customization of complex networks on the fly

WATCH THE CASE STUDY >

"We have over 1,400 customers that have 1,400 different problems [and] 1,400 different security settings. Having the ability to orchestrate all of those needs of our customers—and to do that on the fly—I don't think anyone else has that capability."

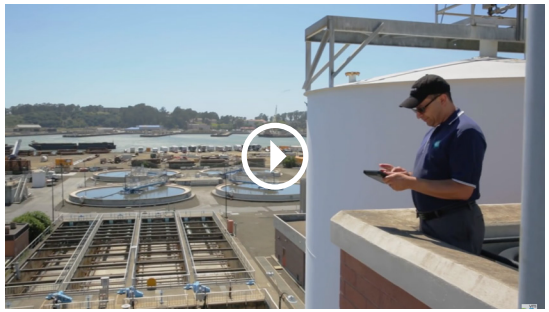
JEFF SCHILLING
CHIEF SECURITY OFFICER
ARMOR

Vallejo Sanitation

Vallejo Sanitation and Flood Control District (VSFCD) collects and treats wastewater to keep the Vallejo, California community healthy and free from flooding. It is imperative that the operations staff is free to serve customers—without compromising network security. VSFCD chose NSX because it allows the district to easily manage its network while leveraging the benefits of micro-segmentation to keep workloads and users safe.

CHALLENGES	SUCCESSES
Needed to keep wastewater treatment plant running 24/7, 365 with no shutdowns	Two VSFCD administrators can now run their entire system 24/7 with 99.992% uptime
Field workers needed secure access to sensitive data on personal mobile devices	Workers can securely access encrypted data in the field with a secure "tunnel" in NSX
Network was inefficient and difficult to maintain, requiring complex physical equipment and numerous VLANS	Micro-segmentation allows all VDI to be in one pool, eliminating 5–6 VLANS and easing complexity

WATCH THE CASE STUDY >



"VMware NSX is providing something that hasn't really been seen before in the networking world. We're able to set up micro-segmentation on the network to provide enhanced security, set up groups and policies based on virtualized content, and configuration is way easier."

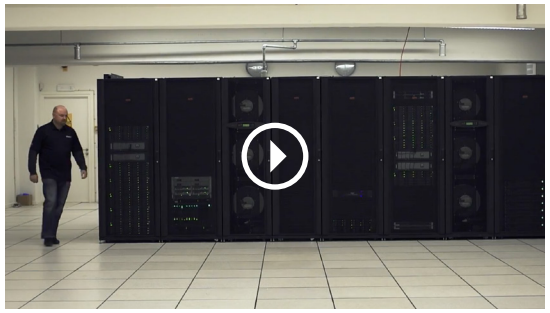
TERRY CHATMAN
INFORMATION SYSTEMS SPECIALIST
VSFCD

Herning Kommune

As one of Denmark's largest municipalities, Herning Kommune has a broad range of critical public service responsibilities. Not only is it vital to keep its network secure, it also needs to stay conscious of cost, ease of use, and efficiency. It chose NSX because it enables exceptional security and efficiency at a low cost.

CHALLENGES	SUCCESSES
Physically moving switches and reconfiguring networks during machine relocation was a time-consuming, complex process	Migrated administrator tasks from hardware to software, eliminating the physical work of reconfiguring networks
Municipalities struggled to communicate and collaborate securely	Achieved improved, secure communication with other municipalities
Hundreds of servers were difficult and expensive to maintain and operate	Reduced physical servers from 200 to 15

WATCH THE CASE STUDY >



"Since we have an increasing number of assignments and fewer hands, it is imperative that the amount of administration is as limited as it is the case with virtualization. It is difficult to quantify the gain from less administration, greater flexibility and higher reliability, but the benefits are substantial."

MIKAEL KORSGAARD JENSEN
SERVER MANAGER
HERNING MUNICIPALITY

Prague Stock Exchange

PRAGUE STOCK EXCHANGE
BURZA CENNÝCH PAPÍRŮ PRAHA

As a financial services institution, Prague Stock Exchange is particularly vulnerable to cybersecurity threats. It is imperative to its success that it find and implement a robust solution that keeps sensitive data safe without compromising on efficiency. It chose NSX for its ease of use, low cost, and micro-segmentation capabilities.

CHALLENGES	SUCCESSES
Security of operations and stored data needed to be more robust	Enabled granular security for individual applications with micro-segmentation
Network operations weren't optimized	Reduced the number of computer rooms from three to one with 90% server virtualization
Day-to-day management was complex	Simplified IT management by reducing physical nodes from three to two

READ THE CASE STUDY >

"Ensuring the reliable and lasting security of sensitive information is one of the main tasks of the IT department. The implementation of the NSX platform will bring us unprecedented possibilities for micro-granulation of security settings, and hence more selective and improved protection of individual applications."

MIROSLAV PROKEŠ
DIRECTOR OF ICT DEVELOPMENT AND OPERATIONS
PRAGUE STOCK EXCHANGE

Zettagrid

As an operator of Infrastructure-as-a-Service, Zettagrid runs one of the fastest, most highly available public clouds in its market. Its customers rely on it for secure, efficient, and agile solutions. Zettagrid chose NSX because it is a cost-effective, efficient, and future-proof way to secure the data center.

CHALLENGES	SUCCESSES
The network was complex and costly	Removed reliance on project services and implementation services
Educating customers on how to use network services was inefficient and frustrating	Allowed customers to securely consume NSX from the Zettagrid portal
Provisioning took days or weeks to complete	Achieved networking elements in seconds rather than days or weeks

WATCH THE CASE STUDY >

"Zettagrid has always been an enthusiastic adopter of new technology and we are thrilled to be the first in Australia to automate NSX into the public cloud space."

NICHOLAS POWER
COO
ZETTAGRID

Japan Advanced Institute of Science and Technology (JAIST)

JAIST is Japan's first independent national graduate school, known for providing high-quality IT services from the start. It needed to continue to deliver outstanding IT resources without compromising on cost, security, or agility. It chose NSX because it offered protection and speed, yet stayed within its budget parameters.

CHALLENGES	SUCCESSES
Large volume of research and personal information needed better security	Automated security policies provides granular protection for sensitive data
Virtual machines weren't individually protected	Micro-segmentation enables firewalls for individual virtual machines
Remote desktops needed secure access to applications and resources	Users can securely access applications from virtual desktops whenever it's convenient for them

READ THE CASE STUDY >

"VMware solutions include the functions and technologies that are needed to provide ICT as a public infrastructure, with a limited staff and budget. In addition, synergistic effects can be achieved through the combination of different VMware products, making this an excellent solution for achieving the required return on investment."

SHUICHI KOSAKA
TECHNICAL SPECIALIST AT RESEARCH CENTER FOR ADVANCED COMPUTING
JAIST

Secure Your Application Infrastructure to Move Your Business Forward

The digital economy is moving fast, but with the right tools, you can keep up with, and even outpace, your competitors. NSX provides the security and agility you need to enable a more efficient network, freeing up IT to do what it does best: innovate.

By stopping the lateral spread of threats in the data center, securing end users, and enabling DMZ anywhere, NSX enhances your existing virtualization efforts for a complete solution to today's security challenges.

Join other companies around the world in transforming your security with proven solutions that move your business forward.

TAKE THE NEXT STEP

Learn more about VMware security solutions >

Join Us Online:

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com