# Beyond Perimeter Security:

## How to secure your public-sector network from the inside out

Perimeter Security Is Not Enough

Hackers Living Inside Your Network

The Software-Based Network

Making Networks More Manageable

Protection and Cost Savings

Why VMware?

# Perimeter Security Is Not Enough

Every school child is familiar with the story of the Trojan Horse. The ancient city of Troy is said to have had exceptional perimeter defenses. Legend says the walls of Troy kept the Greeks at bay for a full ten years. Then, Greek king Odysseus commissioned the giant wooden statue and presented it to Troy as a gift. Once the Trojans rolled the horse inside its gates, thirty soldiers snuck out of its hollow belly and proceeded to decimate the city.

The story of the Trojan Horse is one of mankind's earliest attempts to teach the lesson that perimeter security alone isn't enough. Unfortunately, as the centuries have rolled by, humans continue to count on walls, whether made of stone or digital technology, to protect them.

The mistake is assuming everything outside is bad and everything inside is good. Such is the lesson that America's Office of Personnel Management (OPM) learned the hard way. OPM was penetrated, not once, but twice. A Congressional investigation concluded that the penetrations themselves might have been prevented if the agency had employed multi-factor authentication.

However, once inside, hackers known as X1 and X2 spent more than a year within the OPM network. They were able to traverse many internal databases. They copied deeply personal information about American government employees, their personal habits, their relationships, their finances, and their weaknesses. Not content to simply visit text-only databases, the hackers also extracted 5.6 million sets of fingerprints.

OPM is just one of a rapidly growing number of government breaches. It is also an object example of what can happen when you put most of your faith into perimeter security, especially when that security is flawed or behind the times. Careers were destroyed when OPM's executives were forced out of their jobs. The compromise of America's national security was a far greater cost. The data stolen from OPM provides a foreign power with a complete and comprehensive kit for gaining access to other American systems, blackmailing federal employees, and even replacing existing data with false and misleading information.

What's so frustrating is that all of this could have been prevented with up-to-date, two-factor perimeter security matched with inside-the-network security designed to keep the hackers from jumping between systems. We'll discuss that next.

## RESOURCES

- Analysis: How one of the biggest data thefts in US history could have been stopped by basic security ›
- In-depth: Inside the cyberattack that shocked the US government ›
- News: Government is hit by 9,000 security breaches a year - but reporting them remains chaotic ›
- Analysis: US government weaker on cybersecurity than any other major industry ›

# Hackers Living Inside Your Network

Perimeters are porous. If nothing else, the OPM breach proved that, as did the break-in of the Democratic National Committee that saw John Podesta's emails splashed across the evening news. Breaches at the Department of Homeland Security and the FBI capped off a banner 2016. Governments outside the United States are also vulnerable to penetrations. In March, the Philippine Commission on Elections lost about 340 gigabytes of information to activist hackers.

As OPM and many other victims of advanced persistent threats have shown, hackers often spend years inside a compromised network before they're discovered. This happens because network managers put all their efforts into securing the perimeter. They assume that once properly authenticated, internal processes are legitimate and safe.

Nothing can be further from the truth. Internal networks have entered the era of Zero Trust. Every node and process inside a network must not be considered any more trustworthy than unknown nodes outside the firewall. Once a network has been penetrated, the perimeter defenses become more of a trap than a protection.

For years, IT professionals toyed with the idea of adding internal firewalls, creating micro-segments to separate different areas of the network from one another. Unfortunately, each change in configuration, each new server, app, or VM, required making changes in the firewalls, making the process cumbersome and inherently inflexible.

VMware's NSX changes all that.

## RESOURCES

- Analysis: Government slow to mount defense against APTs
- News: FBI Quietly Admits to Multi-Year APT Attack, Sensitive Data Stolen ›
- News: Chinese government suspected of hacking into FDIC computers
- News: Pakistan APT Group Targets Indian Government
- News: Canada Discovers It's Under Attack by Dozens of State-Sponsored Hackers
- Analysis: Network Micro-segmentation Could Be the Software Defined Answer to Security

# The Software-Based Network

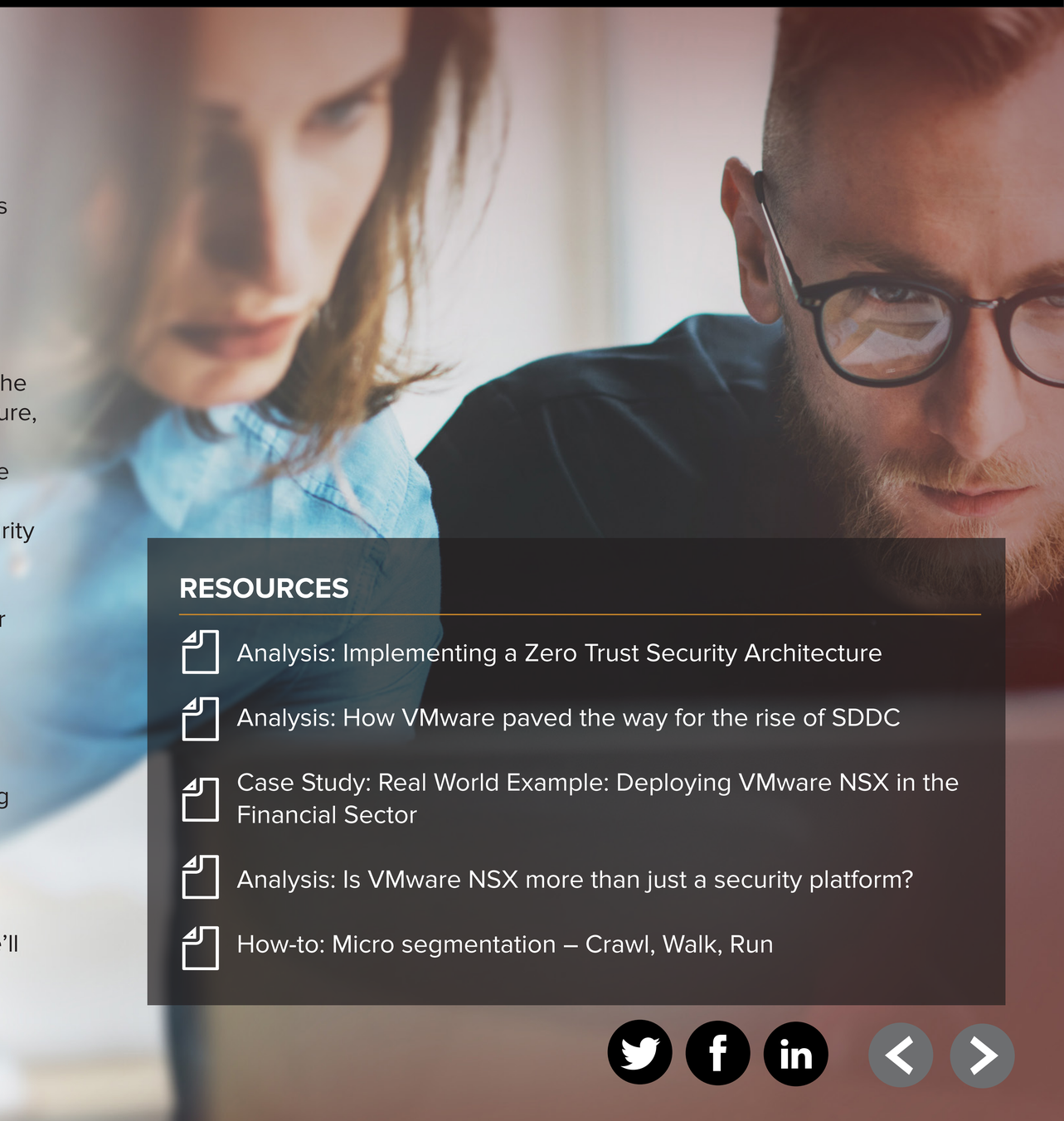
NSX abstracts network and security services into software, transforming what is normally a months-long infrastructure security project into a point-and-click on an interface. NSX allows you to create the virtual equivalent of a submarine's watertight doors across the network by defining security policies at the individual workload-level, creating micro-segments. This granular application of security policy prevents attackers from freely moving laterally from machine to machine within the data center.

Embedding security controls within the hypervisor affords NSX some distinct advantages. The first is context. From the hypervisor, NSX has critical insight into applications and infrastructure, resulting in more meaningful security policies based on workload attributes like machine name, operating system, and even regulatory compliance standards. The second advantage is ubiquity. Security policies are tied to workloads for their entire life cycle. If the workload moves, its security policies move with it. New workloads can automatically inherit their security policies when they are spun up to support existing applications.

NSX allows for the creation of entire virtual networks built in software. Virtual networks offer increased flexibility, agility, and control that is unattainable with physical hardware. Entire network topologies can be provisioned, copied, and stored as a template with the click of a button. Additionally, virtual networks can be stretched across multiple on-premises, private, and even public cloud environments.

The benefit for disaster recovery and failover is considerable, because your entire operating environment can be replicated in a new environment without needing to reconfigure all the VMs with new network addresses.

While the cost savings derived from virtualizing networking and security services can be considerable, the time and energy it frees up among your IT staff can be transformative. We'll discuss that next.



## RESOURCES

- Analysis: Implementing a Zero Trust Security Architecture
- Analysis: How VMware paved the way for the rise of SDDC
- Case Study: Real World Example: Deploying VMware NSX in the Financial Sector
- Analysis: Is VMware NSX more than just a security platform?
- How-to: Micro segmentation – Crawl, Walk, Run

# Making Networks More Manageable

Networks have transformed how people, processes, and systems communicate. As our level of interaction has gotten more complex, so have the networks. Creative and capable programming has created an explosion of applications and data, all riding on top of networks.

Unfortunately, while applications and data have the design flexibility of software, networks have always been tied intimately to the hardware. A need to link a few applications and databases together has often resulted in a network configuration workload that could require months to requisition and install the hardware, then weeks to make the necessary configuration changes, usually entirely by hand.

Those configurations required a mix of hardware, scripting, and conf file tweaks, all prone to error. As networks grow, more configurations have to interact, and the complexity increases exponentially. Because it's almost impossible to see the entire architecture of the network, there is a huge potential for even greater errors.

Networking is often the last part of data center operations to be virtualized. Hardware-centric networks tend to be characterized by both inflexibility and lots of indecipherable patchwork, leading to maintenance and management nightmares.

NSX changes all that. It seems odd to say that a network hypervisor is capable of providing sanity, but because NSX is able to rationalize, automate, clarify, and monitor network configuration at a level above the hardware, your IT folks are more able to focus on advancing the mission of your agency and less likely to be spending time putting out fires.

Because NSX abstracts the network from the hardware, it's also possible to regularly upgrade the underlying hardware without having to reconfigure every application and server running in that environment. The added flexibility provided by NSX, with its built-in automation capabilities, is a force multiplier that can help your IT team get more done, and perhaps even give them the occasional weekend off from work.

## RESOURCES

- How-to: Automating Security Group and Policy Creation with NSX REST API and Python
- How-to: NSX - Network-as-a-Service with vRO
- How-to: vRealize Automation and NSX – Better Together
- Tutorial: The Beginner's Guide to integration between vRealize Automation & NSX

# Protection and Cost Savings

CODE – the Central Office Division of Everything – is a fictional agency that hunts for priceless historical artifacts, rescues citizens in distress, fights terrorists, regulates the use of color in big box store branding, and does it all with panache. CODE's director is Major General Nathan Steelman. Steelman's favorite saying is, "Panache doesn't come cheap, so we need to save money on everything else."

It's with that in mind that CODE's intrepid IT manager, Jo Danger, set out to improve the agency's IT infrastructure. The organization was launching application after application, and it was very important that the various tenant organizations she had to manage on her network were kept isolated from one another.

During her planning process, she opened up the VMware NSX Business Case Economics Calculator and punched in some numbers. Her team comprises ten full-time engineers who manage 400 physical servers hosting 6,000 virtual machines. Over the course of the next five years, she expects to increase the number of VMs she has to manage by 20 percent per year.

Jo was impressed with the results. Without NSX, she would have had to hit up General Steelman for $71 million over the course of five years. With NSX, that number was cut to $30 million, with the biggest savings in CAPEX. The calculator predicted $50 million of savings in hardware. The NSX licenses themselves would only eat up a little of the budget.

More to the point, NSX's automation capabilities would save her overworked team 14,580 hours of work. About 73 percent of their grunt work would evaporate, giving the team more time to innovate and improve service delivery.

CODE would also get the benefits of NSX's micro-segmentation and disaster recovery flexibility, not only resulting in impressive time-to-recovery benefits, but also tangible CAPEX savings nearing $6 million. She pitched the plan to General Steelman. He approved it. A year later, her entire network was up and running on NSX.

(Meanwhile, on the other side of the world...)

"Boss, we're in." The hacker had finally constructed an email message with a shortened URL spearphished right at General Steelman. Steelman opened the link. The foreign hacker had managed to get inside the General's virtual desktop instance and was about to dig around the network, looking for data and more credentials.

But... there was nothing there. Just one measly server. The only thing the hacker was able find was a folder full of puppy pictures. Because the General's desktop instance was firewalled in a micro-segment by NSX, there was no place for the hacker to go inside the network. Another infiltration foiled by virtual networking.

## RESOURCES

- Analysis: Two Great Security Features of VMware's NSX Network Virtualization Platform
- Analysis: VMware NSX – Common use cases

# Why VMware

VMware is often associated with server virtualization. But server virtualization is only one step in the triad of servers, storage, and networks. As you've seen in this eGuide, abstracting the network from hardware can provide unprecedented flexibility, cost savings, and a powerful layer of security.

VMware's offerings help customers build software-defined data centers (SDDC). The power of the SDDC concept is that it enables agency IT teams to build in consistency, reproducibility, and compliance, as well as flexibility and rapid response.

It also allows agencies to expand their infrastructure and their offerings beyond on-premises connections. IT environments can transition seamlessly to and from the cloud, on-demand. User access and network management can be available from any Web browser, as well as mobile devices. An entire network may be managed from a smartphone in any part of the world, while maintaining network security and integrity.

Fundamentally, VMware offers the ability for organizations and agencies to respond with agility, saves IT teams from the tyranny of hand-configuring everything (along with the inevitable errors and their desperate fixes), and provides more value to the taxpayers at a lower cost.

NSX is a critical piece of the puzzle, but only a piece. Feel free to reach out to VMware to explore the full depth of their offerings. Your customers, clients, and constituents will thank you.

To learn more about VMware solutions for the public sector, please visit www.vmware.com/industry/government.