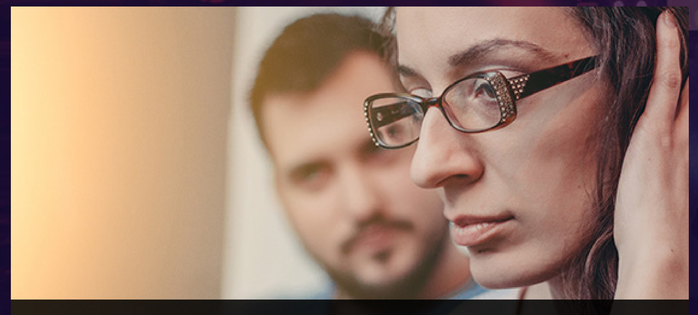
Beyond Perimeter Security:

How to secure your education network from the inside out

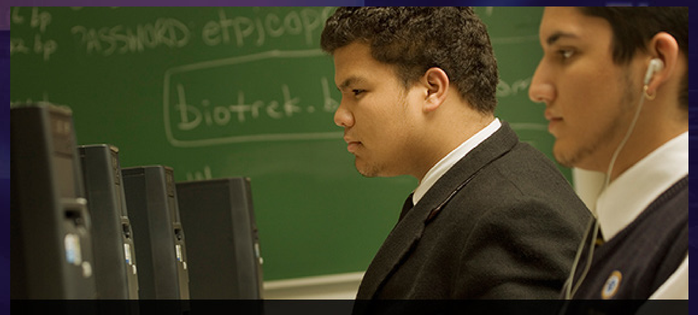
Perimeter Security Is Not Enough

Threats Living Inside Your Network

The Software-Based Network



Making Networks More Manageable



Hutto Independent School District

Why VMware?

Perimeter Security Is Not Enough

There are bad days and then there are very bad day.[1] On March 17, 2016, school superintendent Ken Scarbrough was having a very bad day. After a ransomware attack "corrupted and encrypted most of the district's servers," Scarbrough had to cancel classes for the 2,400 students[2] of the Cloquet Public Schools district in eastern Minnesota.

Rather than paying the ransomware demand of $6,000 in bitcoin, the school district shut down its systems and rebuilt them from scratch. The district's email, learning management system, phones, school bells, and even food service systems were hit.

While technology coordinator Yvette Maijala wasn't "100 percent sure what triggered the attack," her belief is that someone within the school district's firewalls opened an attachment, which triggered the spread of the malware.

Cloquet, of course, is not alone. Ransomware attacks have been spreading at a disturbing rate across educational districts nationwide. In 2016, the cost of ransomware exceeded $1 billion.[3]

Unfortunately, some schools are caving into the ransom demands, even though payment doesn't always yield a decryption key[4] (and may let hackers know they have a live target to hit up for another round). In South Carolina, Horry County School District had to shut down more than 100 servers after ransomware corrupted data.[5] The district paid nearly $10,000 to hackers, with the result that "most systems are back to normal."

Just recently, the Los Angeles Valley College was hit by malware,[6] shutting down systems for thousands of students. In response, officials of the Los Angeles Valley Community College District chose to pay the $28,000 fee in bitcoin in return for a decryption key. The college's computer systems were eventually restored.

Ransomware is far from the only malware category to impact schools. Hacking of all types, including from those physically inside the network, has added to the problem. That's next.

RESOURCES

- News: Cloquet schools suffer 'ransomware' attack
- News: Internal documents restored after ransomware attack
- News: LA college caves in, pays $28,000 ransomware demand
- News: Horry County pays nearly $10k to 'ransomware' hackers
- Analysis: Two-thirds of companies pay ransomware demands: But not everyone gets their data back
- Analysis: The cost of ransomware attacks: $1 billion this year

Threats Living Inside Your Network

Many of the districts hit by ransomware demands believed they had properly protected their networks by using firewalls to separate their internal networks from the Internet. Unfortunately, malware often passes through firewalls in the form of email attachments opened by less-than-diligent users. Other malware is personally carried inside the perimeter on laptops and mobile devices.

The key take-away from all of this is that each of these institutions thought they were reasonably protected because they trusted that their perimeter was secure. As we've seen, perimeter security is not enough.

Schools aren't just subject to attack by outside hackers. Schools are populated by swarms of digital natives called "teenagers," a designation for some of the most terrifying humans on the planet. At the Hillard Bradley High School, two students "hacked into a school computer and stole other students' login information," according to a report on WCMH TV in Columbus, Ohio[7] Another student broke into Panther Creek High School's internal systems. He changed the grades and GPA scores of six students. The result? Transcripts of those students sent to colleges had to be recalled. The 17-year-old Ferris Bueller wannabe was eventually arrested.[8]

Another hack was perpetrated from inside the Sachem School District, which manages 18 schools and provides education for about 15,000 students on Long Island. Information about students' ID numbers, school lunch records, information about medical records, report cards, district records, and personal identifying information were all posted on an online forum.[9]

According to James J. Nolan, Sachem Superintendent of Schools, "the District has a high degree of confidence that its data systems were not breached from the outside." In other words, someone inside the perimeter accessed and posted the information.[10]

While some of these hacks may have a teen movie feel to them, someare deadly serious. In 2015, the University of Virginia was penetrated by an attack "originating in China." The attack stole personal information about the university's East Asia experts, as well as dug into work being done on contract for the US Department of Defense by university faculty researchers.[11]

Internal networks have entered the era of Zero Trust. 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: The real LA schools iPad scandal
- News: Hilliard Bradley High School hacked, students' information exposed
- News: Data breach of Long Island school district affects thousands of students
- 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

Hutto Independent School District

The Hutto Independent School District is a fast-growing publicly-funded school district located in Hutto, Texas, about 30 minutes outside of Austin. Hutto's three IT administrators manage a network supporting 8,000 students and educational staff. According to Network Administrator Chris Harding, "We're a very small team of admins for what's otherwise a large enterprise, and we need everything to just be flexible and agile."

Hutto Director of Technology Travis Brown explained that his team delivers virtual desktops to its students through a network of both virtual and physical desktops, and a software-based network infrastructure based on NSX.

Harding reports that NSX substantially increases security and flexibility. "With NSX...there is a drastic increase of security. We don't have to worry about putting a specific firewall appliance between the virtual desktop users and the regular desktop users, and the remainder of the data center. We can be hands off and not have to worry about [an] attack because, literally, the traffic will not flow if it's not allowed. It just doesn't traverse the system. It's not about breaking past the security. It [NSX] just literally closes it off."

Because of the added security NSX provides Hutto, Harding added, "We feel comfortable opening our VDI environment to the student at home, the student who is home-bound." Because students access virtual desktops rather than running their own desktops at home, they have access to any school-licensed software, without the challenges and hassles of VPN access.

Like most educational institutions, Hutto has to manage operational costs. Both Brown and Harding report that NSX drastically increased their utilization of their network, leading to consolidation. According to Brown, "We've been removing a lot of physical equipment out, physical equipment that we didn't have to replace. We've reduced our rack sizes by 33 percent so far and we're still working on consolidating even further."

Describing NSX, Brown said, "You've got the product that will allow you to function as if you're a Fortune 500 without having to purchase all of the high-end hardware."

Brown advised, "As you build this environment, if you build it correctly, then it can make you very agile. Grow into the environment, do not attempt a rip-and-replace."

As a final thought, Harding recommended, "Sitting down and taking the time to design what you want to see the network be... that's really going to be the majority of the time. Implementing is actually really fast."

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 school and university 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 school districts and universities 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 their students 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 staff, faculty, and students will thank you.

To learn more about VMware solutions for education, please visit www.vmware.com/industry/education.