Micro-Segmentation Builds Security Into Your K-12 Data Center's DNA

Secure Your Digital Learning Infrastructure from the Inside out with VMware NSX

TECHNICAL WHITE PAPER

vmware®

"It's bad if Personally Identifiable Information (PII) data is stolen from a corporation; it's crippling if you don't protect student data. That's why micro-segmentation, policy-based automation, and auditability with VMware NSX are critical to what we do."

— Jason Radford,
Head of Operations,
IliniCloud
(Bloomington School District)

Executive Summary

Most education IT professionals agree that securing the network only at the perimeter is inadequate for the demands put on today's district and school data centers. Once malware has managed to make its way behind the perimeter firewall by latching onto an authorized user (or other means), it can move easily from workload to workload. This lateral movement is possible due to a lack of sufficient internal network controls regulating server-to-server or east-west network traffic.

Micro-segmentation, enabled by E-Rate eligible VMware NSX™, is a breakthrough model for data center security. Network security policies are enforced by firewall controls integrated into hypervisors that are already distributed throughout the data center. This enables security that is both ubiquitous and granular, placing security policies close enough to workloads and applications to give them rich context while keeping them removed enough to have isolation from threats. Security policies also become more dynamic by being coupled directly to the workload, moving, changing, and being deleted as required.

A Bold New Approach: Security from the Inside Out

This approach to security, which is much better suited to support the dynamic nature of data center operations, has never been possible before. This model is more effective and dynamic for creating, maintaining, and improving security measures than attempting to simply plug gaps in perimeter defenses or manipulate the underlying physical network infrastructure. Ultimately it means that IT and instructional decision-makers can innovate with confidence, extending the reach of digital learning while safeguarding student information and privacy.

The Tortoise and the Hare: Security Isn't Keeping Up With Fast-Moving Workloads and Faster-Moving Threats

As virtualization and cloud technologies dominate both K-12 data centers (accelerating the speed at which servers, storage, and network resources are provisioned), administrators are under pressure to offer security that keeps pace with today's application and environment demands. This is especially critical as scrutiny around student privacy and safety grows—one breach can be devastating to both mission and reputation. The cost of recovery can be immense—but even with those risks, most decision-makers remain unsure.

Following are just some of the data points that tell us the current model for K-12 data center security is not keeping up with threats:

- 47 states now have data-breach laws that apply to public entities, including school districts.
- Nearly 800 educational institutions have experienced a data breach event since 2005 (about one educational institution per week). Nearly 1 in 3 were K-12 primary and secondary schools.
- 7 in 10 parents are comfortable with data-driven instructional tools, if the school can protect their data.

Network Virtualization Makes Micro-segmentation Possible

VMware NSX, the network virtualization platform for the Software-Defined Data Center (SDDC), creates a virtual network that is independent of the underlying physical network hardware, where IT can simply treat the physical network as a pool of transport capacity.

Much like the server virtualization model, a "network hypervisor" reproduces Layer 2 to Layer 7 networking services in software. These services can be assembled in any combination—in a matter of seconds—to produce a new network configuration.

You can programmatically create, provision, snapshot, delete, and restore complex networks all in software. New applications, new capacity demands, or the latest regulation—keeping your security environment dynamic and up to date is seamless and simple.

Because hypervisors are already distributed throughout the data center, with VMware NSX you can create network security policies enforced by firewall controls integrated into the hypervisors. These security policies are tied to your virtual network, virtual machine, and operating system, providing granularity down the virtual network interface card.

Fortunately, there is a smarter way to address these risks. By isolating workloads and regulating lateral movement, malware can be prevented from starting in one place and moving around until it achieves maximum damage or successfully downloads sensitive information. It's called micro-segmentation, and it helps set a whole new standard of information security.

Today's Security Normal: Good but Not Good Enough

The issue isn't that the current physical security appliances used by education IT organizations use aren't sophisticated. Given the purpose for which they were designed, today's adaptive firewalls and intrusion prevention systems are intelligent and formidable. But statistics show that they aren't sufficient to protect the data center. Some challenges include:

- Complex security mechanisms like physical firewalls are administratively intensive to maintain and update. District CIOs are having a tough time justifying this rising overhead when they're under constant pressure to expand access to teaching and learning resources without increasing costs.
- Physical devices cannot be everywhere at once, or even too many places at once. It's simply too complicated and expensive to locate firewalls pervasively throughout the data center. Even if the devices could be adequately deployed, it would be impossible to keep them constantly updated and protected against evolving threats.
- The perimeter-centric security model is designed to work from north to south, which means from the client to the server. It's not designed to handle east-west traffic, which is how communication between servers travels, and how many threats propagate inside the data center.

Most IT professionals agree that securing the network only at the perimeter with physical firewalls is inadequate for today's data centers. While perimeter defense is strong, it isn't impregnable.

Among the many ways that intruders can make their way into the data center is by creating malware that latches onto an authorized user to get behind the physical firewalls. This is especially risky for education IT, where users aren't always educated on security best practices and nearly all data is potentially sensitive.

The World is More than "Trusted" and "Untrusted"

Historically, using traditional network firewalls, similar compute systems are grouped into security or trust zones. Firewall policies can then be used to create a comfortable envelope around these siloed zones. To contain complexity and cost, larger zones are easier to set up than smaller ones—the most immediate example being the practice of creating a "trusted" zone, separated from an "untrusted" zone.

Large envelopes with more compute systems inside them are better for economics and ease of administration—but not, as it turns out, better for security. Once inside a security or trust zone, access is completely unrestricted between systems—because

[1] Global State of Information Security Survey 2015, PriceWaterhouseCooper, 2014

anything in the zone is assumed to be trustworthy by everything else in that zone. The bigger the zone, the more havoc a single piece of malware can wreak. The malware can travel around unchallenged, disrupting operations or stealing sensitive data for days, weeks, or even months.

The Traditional Choice: Performance or Security?

The typical data center might have a pair of firewalls at the perimeter and maybe a handful inside the data center, compared to several hundred workloads. To protect all of this east-west traffic would not be feasible even for the most skilled and well-funded IT team.

Given the infeasibility of this strategy, you still have the problem of directing all VM-to-VM traffic through a large chokepoint firewall, and the negative performance impact would be frightening.

Since physical security is optimized in one direction, a better model requires an entirely different approach: micro-segmentation enabled by network virtualization. Micro-segmentation can help your organization address all of these issues:

1. Stopping the spread of malware within the data center
2. Enabling faster delivery of networking and security services
3. Creating more flexible and even automated adaption to changing demands and security conditions

Until network virtualization with VMware NSX, a micro-segmentation model for data center security was not possible. Now it is not only feasible, but also streamlined and cost-effective to deploy and administer.

If Threats Can Start Anywhere, You Have to be Everywhere

In a sense, physical security is like using gloves to guard against germs. It is external, limited protection. If someone sneezes in your face, you're probably going to end up with a cold or flu. Micro-segmentation is like fortifying the immune system of the data center: so germs (or malware) can't get in. Or, if something does, the system can shut it down (or limit its spread) so it can't do any more damage.

Micro-segmentation is based on the assumption that threats can come from anywhere within the data center, so the micro-segmentation model makes security ubiquitous throughout the data center. This model not only provides pervasive coverage, but also the ability to create and change security policies with agility and speed that matches the dynamic workloads they must protect.

The DNA of Better Security is not unlike how biotechnology is used to change plants at the molecular or cellular levels to be pest and disease resistant. That's what micro-segmentation can do to secure all of your data center resources. It allows security to become both pervasive and extremely granular, eliminating gaps and vulnerabilities throughout the data center; this is how NSX builds security right into your K-12 network's DNA.

Seamless, Secure K-12 Services

Fulton County IT Director, realizing he was serving a generation of users who "were born with iPads in their hands," realized they needed to get more serious about how they protected critical applications and information from a broad range of internal and external threats. To ensure quality of services and solutions didn't suffer, the technology needed to integrate easily into the existing environment.

By choosing VMware NSX, the district got next generation information security that actually simplified how IT resources were planned, stood up, and managed. Rock-solid security never meant the district couldn't help teachers and administrators get the job done. New environments can be built quickly and controlled carefully, helping teachers and staff focus on teaching, not technology.

- Carefully managed access across diverse devices, operating systems, and connections
- Security policy that follows workloads and updates easily
- Performance stays nimble across applications and user experiences

Figure 2: Micro-segmentation allows you to secure traffic between virtual machines, as well as between VMs and physical hosts. You can create and apply security policies down to the virtual network interface card level. Policies will automatically move with the workload, even if the physical IP address changes. Micro-segmentation makes it even easier than with physical security alone to integrate other types of security products into the data center.

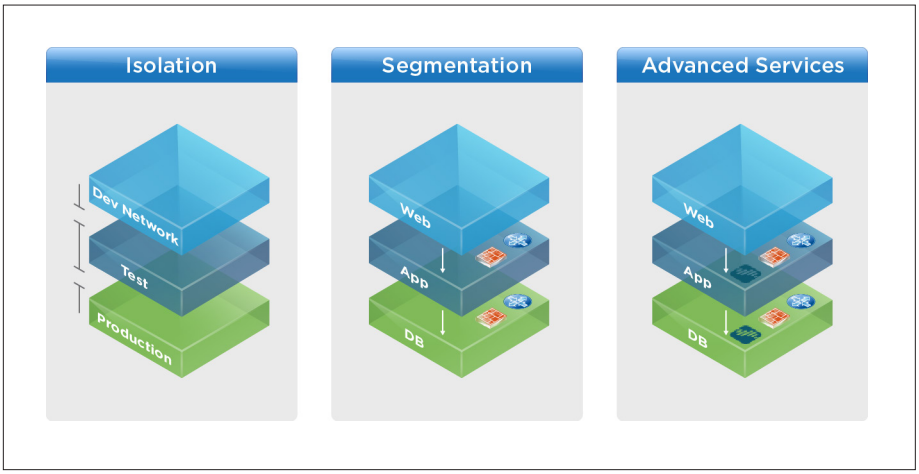

Figure 2: Micro-segmentation allows you to secure traffic between virtual machines, as well as between VMs and physical hosts. You can create and apply security policies down to the virtual network interface card level. And policies will automatically move with the workload, even if the physical IP address changes. Micro-segmentation makes it even easier than it is with physical security to integrate other types of security products into the data center.

Create More Flexible and Realistic Security Policies

As shown in Figure 3, rather than using the VM's IP address or VLAN, you can apply a flexible combination of attributes to describe each workload and create the appropriate security policy for that workload, e.g., by groups, such as all assessment platforms, by operating system, or perhaps "all VMs handling student information" (a "sensitive data" type).

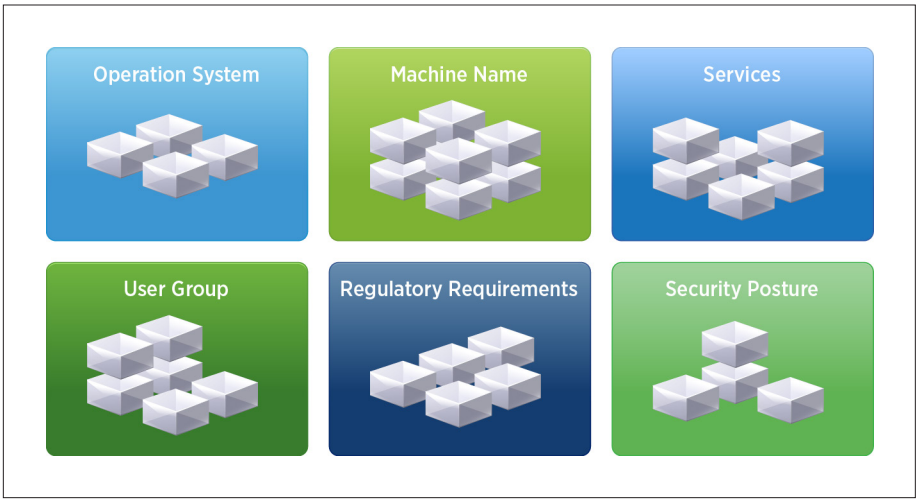

Figure 3. Because VMware NSX understands workloads, you can define groups in a way that actually reflects the function of the workload. These are just some examples of the logical ways you can define groups.

Keep Security in Synch with Dynamic Workflows

Keeping firewall rules in synch with actual workloads is virtually impossible with today's physical firewalls, whether they're outside or inside the data center. And an out-of-date policy is a vulnerability waiting to be exploited.

With the micro-segmentation model, security policies can be created in seconds. They are even automated—applied when a VM spins up, moved when a VM is migrated or changes IP addresses, and removed when a VM is deleted.

Eliminate Inefficient Traffic Patterns that Lead to Overprovisioning

Figures 4 and 5. Enforcing security using VMware NSX and micro-segmentation eliminates some of the inefficient traffic patterns that are inevitable with physical security, such as hair-pinning, which results in core link oversubscription.

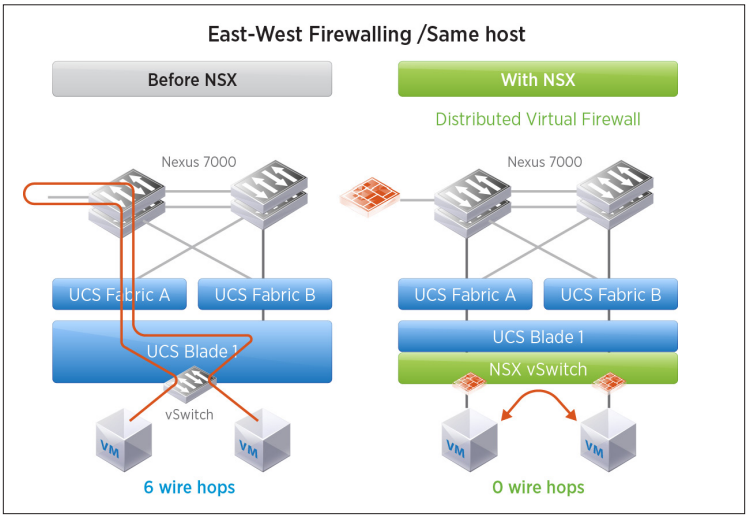

Figure 4: East-west firewalling on the same host using micro-segmentation with VMware NSX shows how you can create more efficient traffic patterns (in this case, reducing the number of hops from 6 to 0).

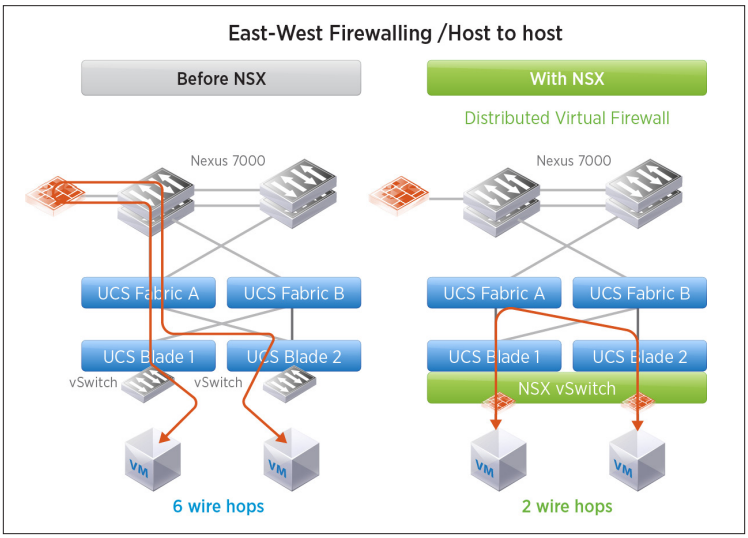

Figure 5: East-west firewalling from host to host using micro-segmentation with VMware NSX shows how you can create more efficient traffic patterns (in this case, reducing the number of hops from 6 to 2).

VMware NSX Brings Realization of Software Defined Data Center Closer

The Software Defined Data Center (SDDC) is a data center model that enables administrators to bring up new applications in a matter of minutes, rather than weeks, and that includes compute, storage, network, and security provisioning. The SDDC model is also easy to change, simpler to manage, and more responsive to evolving IT and instructional challenges.

A significant and non-disruptive step toward creating real SDDC innovation is adopting the VMware NSX network virtualization platform. While the ability to inject robust security directly into your network DNA is huge, there are other significant benefits it brings to your infrastructure:

- Accelerate network provisioning and streamline operations.
- Facilitate an even greater degree of data center consolidation.
- Enable unencumbered workload mobility and placement.
- Enable push-button, zero-compromise disaster recovery.
- Save on hardware acquisition and ongoing operation.

Enhance Security through VMware's Ecosystem of Technology Partners

NSX is designed as a platform that integrates easily with key technology partner solutions. These tools ensure that you can continue to enhance your security capabilities to respond to constantly changing conditions in the data center. For example, Palo Alto Networks is a partner in the VMware ecosystem. Palo Alto Networks' integration with VMware NSX adds the ability to:

- Efficiently add advanced, next-gen firewalling and IPS security to workloads inside the data center.
- Share intelligence with other security products in the VMware NSX ecosystem to adapt to emerging security conditions in the data center.

Ease of Implementation

If you have VMware NSX, you've got everything you need to deploy micro-segmentation. Because hypervisors are already distributed throughout the data center, it's easy to implement, manage, and monitor.

NSX runs on top of any network hardware, so you don't have to buy or replace any appliances to get big security gains. Additionally, there's minimal disruption to the physical security infrastructure you already have in place.

Simplifying Complexity and Adapting Faster to Change

Following are two examples of how micro-segmentation can make even the most complex or fast-changing security scenarios easy to implement.

Figure 6 illustrates how easily micro-segmentation can make security more granular without adding complexity.

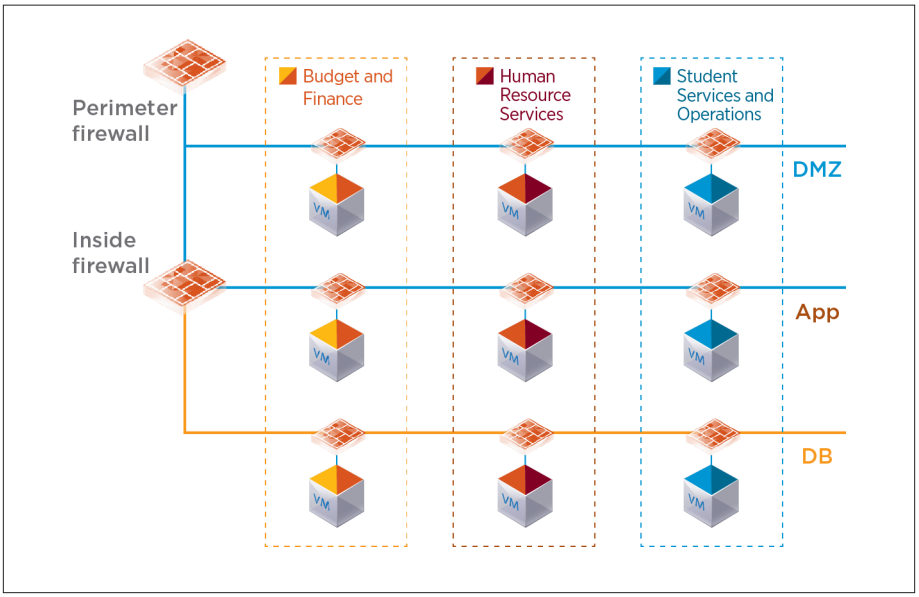

Figure 6. As shown here, micro-segmentation allows you to protect each VM with its own perimeter security (granularity that would not be practical with a physical firewall). With this granularity, it becomes easy to align policies with logical groups. It also prevents malware from spreading, as it is more likely to do in the old trust zone model.

Maximum Multitenant Performance

Bloomington, Illinois School District decision-makers were stuck. A rapid rise in demand for cloud and other computing services was driving up cost and complexity as technology became more and more critical to teaching and learning. Stakeholders looked to IT for leadership, demanding a solution that met diverse demands on reduced dollars.

Working with the statewide district cloud provider IlliniCloud, Bloomington IT selected VMware NSX to help manage and secure the day-to-day delivery of applications and information to diverse users and devices. Through virtualization, access to important resources gets simpler, while micro-segmentation strengthens the data center from the inside out.

- Leveraging existing hardware to accelerate time to value
- Simplified management of both performance and security
- Shared, multitenant services model transforms IT delivery

Figure 7 illustrates how micro-segmentation also simplifies the security for virtual desktop deployments. Consider an example in which a district IT department has decided to virtualize the desktops across the Finance department. With traditional hardware-based perimeter security, securing virtual desktops in the data center would add yet another level of complexity to the matrix of security policies, since the policies would have to be mapped back to the network position of the virtual desktops.

With micro-segmentation, however, creating and applying security policies is possible based on the flexible attributes of the desktops themselves: for instance, the type of operating system, the names of the machines, or in this case, the user group (Finance). Deploying security for the virtual desktops for Finance takes a matter of minutes. It is also not disruptive to the security policies that are already in place for the other departments and applications, and there are no additional costs required for new appliances.

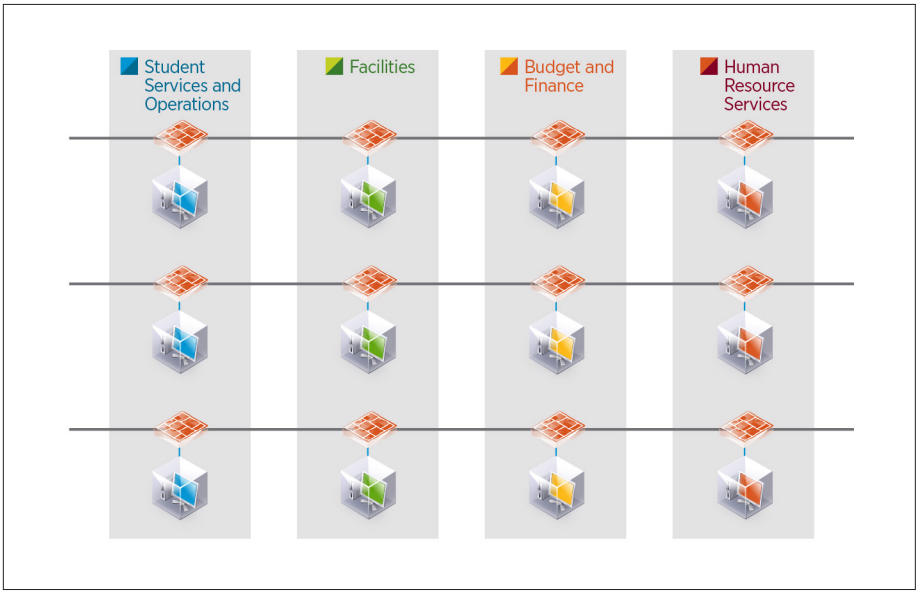

Figure 7. With micro-segmentation, creating a new policy based on VDI takes minutes and does not involve changing other policies already in place.

Conclusion

Thanks to the innovation and efficiency made possible by network virtualization, micro-segmentation has become a practical and powerful reality for K-12 decision-makers worried about securing their district's information and infrastructure. Data center administrators no longer have to predetermine where security needs to be located, because it's available anywhere.

This means policies can be created to match workloads and change as readily as workloads change. Security is pervasive, but not rigid. It's revolutionary, but not disruptive to your existing infrastructure.

Micro-segmentation enabled by VMware NSX blankets the data center itself with complete, adaptive protection. In short, your data center now has security infused into its operational DNA. New applications, new users, new demands—your digital learning infrastructure is now ready for anything, thanks to micro-segmentation.

Learn more about micro-segmentation and VMware NSX in education at: http://www.vmware.com/go/NSXK12.

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

 Item No: VMW10258-WP-MICRO-SGMNTN-DATA-CTNR-K-12-USLET-102 05/16