Top Three Cloud Vulnerabilities with Digital Transformation

The advantages of using a security services provider

You are at risk

The increasingly distributed nature of data and the ever-changing data center landscape are significantly factoring in the growth of cyber risk to both on-prem and cloud environments. Together with BYOD rise on one hand, and the lack of security expertise on the other, these factors are posing new challenges for modern organizations to build a secure IT infrastructure, which is a pillar of any data protection strategy.

In virtualized environments, one of the dominant security challenges is the growing complexity of virtual machine (VM) architecture, which often spans across platforms and data center locations to support the increasingly dynamic application workloads. Managing such architectures ups the requirements for security, staff skill sets, and technology, ultimately leading to more complexity in the data center, which in turn increases the cost to manage, operate, and update your environment.

While virtualization provides the needed flexibility of implementation and protects data through isolation, the complexity of data center services and non-granular nature of physical security solutions require additional defense mechanisms to fight the evolving threats.

To maximize security of their virtualized environments, organizations need advanced solutions both on the level of infrastructure and on the level of strategy, systems, processes, and protocols. Here are some of the most important threats these solutions must address in order to keep your data safe.

1. Highly distributed nature of data and applications

The accelerated dynamics of data center deployments, which are increasingly hybrid, instant, and data-heavy, has greatly transformed data management practices. As opposed to more traditional approaches that rely on storing data on one centralized architecture, today's practises include more distributed, scalable, and robust platforms that allow for quicker deployments and improved resilience.

Such platforms may be fully or partially virtualized, with application workloads being distributed between multiple clouds and VMs. While this approach represents as an efficient way to bridge the gap between platform flexibility and performance, it has brought about new security risks. Data may travel unencrypted, requiring additional network solutions and applications to secure sensitive traffic. In addition to this, organizations often do not have a deep insight into their VMs and cannot promptly react to threats such as zero-day exploits or hyperjacking. This lack of visibility into data traffic is one of the key virtualization vulnerabilities as it expands the entry points for hackers.

One of the essential measures of protection against these attacks is improved visibility into east-west traffic through micro segmentation and enhanced monitoring systems. However, many organizations fail to implement such a comprehensive platform due to lack of expertise or resources, leaving their VMs largely unprotected.

> "Today's distributed datacenter landscape will likely develop into a more intelligent, highly interconnected network made up of new datacenter form factors. Compact, self-managing datacenter nodes and hubs (of data or connectivity, or both) will be embedded and pervasive, supported by and feeding into large datacenter campuses."
> – David Wood, Director of Power Business at Raritan[1]

2. Increasing attack surface with growing end points

We've been a mobile workforce for a while now, and it's still growing. The Ponemon Institute predicts a 50% increase in mobile access by end of 2018. The multiplying number of access pathways to your sensitive data is enough on its own to cause worry. But mobile brings its own set of vulnerabilities that many organizations have yet to overcome – mobile attacks are increasing, both in terms of number and pragmatism.[2]

The success of perimeter firewalls relies on perfect management of authorized devices and users, and what they have access to, which is a continuing challenge for IT. In other words, not only do businesses need to corral mobile device use, they also need to implement security measures within the firewall for when the inevitable breach takes place.

Let's face it, BYOD is no longer a trend we can ignore. Offering a VPN solution to the corporate network is accepting a BYOD strategy and introducing non-corporate equipment, or corporate equipment on unsecure networks, into the corporate environment. It is important to understand that every organization today has a BYOD strategy, one they are actively in charge of, or one that has been dictated to them by the users, that they are not in control of. Therefore, perimeter or North-South security strategies alone are no longer effective. East-West and micro-segmentation strategies are paramount to effective access control, and the containment of malicious activity.

> "Of the 53,844 mobile devices in the average Global 2000 enterprise, 1700 of those devices are infected by malware at any given time."
> – Ponemon Institute[3]

3. Missing internal security expertise

In the eye of the security storm sits the IT organization. They are never relieved of current duties, and must somehow not only keep the lights on for existing IT services, but also architect needed changes to make the company more agile - while keeping costs under control. A vast body of knowledge is required to do this, and adding security expertise to the list of requirements is beyond what many IT organizations can handle given their other expanding responsibilities.

The risks are in the IT staff's ability, or limitation, to adequately and efficiently manage security across your entire virtualized environment – including control over who has permission to access which resources. It also creates a conflict as IT resources take on dual roles of executing as well as auditing, which not only requires special training in security and risk management, but generates a significant gap in IT governance. In fact, this was identified by the Cloud Security Alliance (CSA) as a top security threat for 2018: "insufficient identity, credential, or key management can enable unauthorized access to data and potentially catastrophic damage to organizations or end users."[4]

The lack of expertise and ability to implement controls over access across your virtualized environment leaves a lot of opportunity for both human error, as well as malicious insider attacks.

> 60% of all attacks are carried out by insiders; of these, three-quarters involve malicious intent.
> – IBM Cyber Security Intelligence Index

Securing assets in the face of cloud and mobile

Who you choose as your cloud provider is clearly important, as is restricting who in your organization has the ability to create and deploy VMs. Security policies must be well defined and enforceable to ensure new images and instances are following the rules and minimizing your exposure.

Some sort of mobile management is also necessary to manage access from remote locations, as well as to control what happens to devices and their data, BYOD or not, when lost, stolen, or compromised. This can be with a tried and true Mobile Device Management (MDM) solution, or one of the more advanced Enterprise Mobile Management (EMM) solutions that extend into Mobile App Management (MAM), among other things.

Cloud and mobile are at the center of any IT strategy to create business agility, improve productivity, and enable the adoption of new technologies that help bring about digital transformation. But regardless of cloud provider and mobile management solution, you also need a foundational security layer that protects beyond your data center from these environments and access points that you can't fully control.

It's proving to be too large of a challenge for many resource-strapped IT organizations to effectively mitigate the growing security risks while controlling costs and keeping complexity to a minimum.

The good news is security solutions are evolving, as are security services.

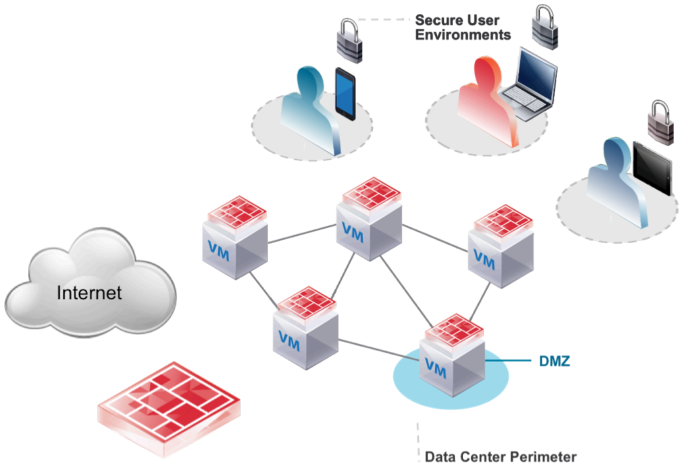
Let's take a look.

Technology-based security solutions

Hardening network and VM security

"Zero Trust" security allows you to adopt a stricter, micro-granular security model with the ability to tie security to individual workloads and provision policies automatically. With micro-segmentation, fine-grained network controls enable unit-level trust, and flexible security policies can be applied all the way down to a network interface – virtually firewalling every workload in the data center.

Establishing "Zero Trust" security

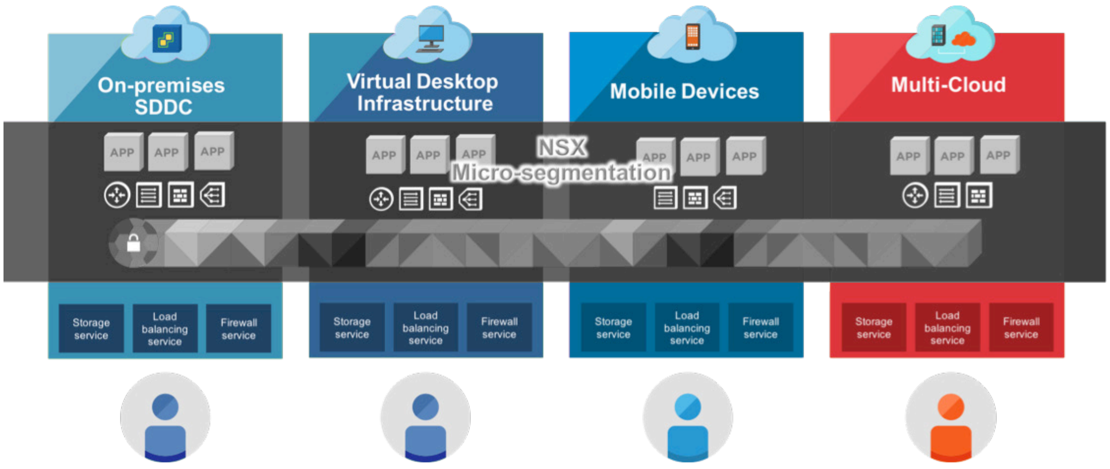


Benefits of a Zero Trust security environment

More secure data center while providing Capex savings	+70% Capex savings with micro-segmentation
Server utilization Capex savings	+80% five year Capex savings
IT automation Opex reductions	+87% Opex savings for networking tasks

* Based savings realized after VMware NSX deployment; results will vary based on data center size and complexity

VMware NSX provides micro-segmentation and virtualized firewalls to help reduce operational costs, improve network performance, and secure East-West (lateral) traffic within the data center.



Addressing today’s risks with VMware NSX	
Storing data within a VM in a hybrid cloud environment	• NSX is an important element in locking down your virtualized environment, regardless of where VMs run. • NSX can quickly identify and isolate problems before they spread.
Increasing attack surface with growing end points (mobility)	• NSX policies follow loads no matter where they reside and control access to images and production VMs. • Lateral traffic is continually monitored to prevent unauthorized access from any user, any device.
Missing internal security expertise	• Create security profiles that can be attached automatically to workloads as well as classifications of users.
Lack of insight into VM activity	• VMware vRealize Network Insight and NSX can quickly identify and isolate problems.

Performance acceleration technology

Hardware-enhanced security with Intel® Xeon® Scalable processors
It’s common for certain security technologies to potentially impact performance, but by deploying hardware with built-in security features you can eliminate the negative impact on your systems.

The revolutionary architecture of Intel’s Xeon Scalable processors enables advanced security capabilities that help optimize infrastructure for fast and secure data processing in both traditional data centers and cloud environments. Key features like performance increases, higher availability, enriched management options for the virtualization of network functions (NFV) – and Intel’s QuickAssist Technology (QAT) – complement any security solution approach while ensuring the needed performance for your applications. Intel QAT increases hardware-accelerated encryption and drives large gains in virtual networking and security appliance throughput.

Approaches to security

The challenges of creating a secure virtualized environment

Go it alone - Every business endeavors to improve their IT security and a natural first step is to consider what you can do yourself. Given the technologies available, like VMware NSX, and the capabilities of your IT organization, can you properly assess, plan, roadmap, execute, and manage ongoing security solutions across your environment, across devices and users, and into the cloud?

If you intend to handle security services in-house, it’s imperative to be proactive. Have a plan. Practice your plan over and over until it becomes “muscle memory” for your organization. Then, when an incident happens, everybody knows what to do and what is expected, and can focus on the specific attack and any unique needs or mitigation it requires.

Leverage cloud services - Another approach is to use cloud services. Most cloud service providers offer a basic level of security and will enforce good security practices such as minimum password rules and forced password changes. Cloud providers also typically provide automated data backup and recovery to allow you to focus on building your business rather than on IT and information security.

But the reality is, the operational tax, the acquisition of talent, and staying current with technology and ever-morphing threats, create a high price tag that only the largest enterprises can afford due to the economies of scale they can achieve. Smaller organizations will struggle to create the efficiencies and effectiveness needed without being exorbitantly expensive.

Augmenting your IT - As we mentioned, security solutions, and services, have evolved. An alternative approach is to engage a managed security services provider, which can handle all of the above, and depending on the size and complexity of your network, is often more affordable than you'd expect.

Utilizing a managed security services provider

phoenixNAP cloud and security services

Working with a security services provider, like phoenixNAP, is a smart and cost-effective alternative to attempting to manage security yourself. It allows you to leverage an existing secure environment while augmenting your IT staff with the needed expertise. Technology alone does not create an ongoing, secure environment for your business; it's about approach, execution, and management based on a deep understanding of best practices that ensure protection against the latest threats.

With simplified and reliable IT infrastructure management and a monitoring portal, phoenixNAP helps you streamline all your IT infrastructure tasks - from billing to firewall setup and storage management.

- Single pane of glass to manage your infrastructure
- Streamlined payments and billing
- Simple firewall, storage, and server setup
- Instant load balancer health checks

phoenixNAP security pillars

People	Security, cloud, and network expertise	Expertise to manage the environment; 24 hour monitoring; deep knowledge of the latest standards around threat assessment and operational support
Process & Policy	Threat Management Platform	Streamlined processes that ensure compliance with carefully defined policies
Technology	Data Security Cloud	Combination of best-of-breed technologies (including VMware NSX); hardware, data centers, performance

Security at the core	
Confidentiality	Micro-segmentation and encrypted drives within VMware
Integrity	System is monitored, managing threat factors, maintaining latest technology
Availability	Multi data center capability, hosted cloud infrastructure - better than someone can build in-house

phoenixNAP Data Security Cloud

The world's most secure cloud from a partner you trust

phoenixNAP's Data Security Cloud is a battle-tested, scalable, and globally available platform. Secure by design, your data is fully protected - not only at the perimeter, but on the application level as well. Provisioning is automated and network virtualization easier and more agile than ever before. Take total control of your IT infrastructure, cost, and security - all through a single pane of glass.

phoenixNAP's Data Security Cloud protects your data on a hardware and software level. Moving away from bottlenecks created by manual provisioning of network resources and reactionary security practices, it provides cloud infrastructure with zero trust policies to help you handle security challenges at scale, while enabling automated and easy management for compliant deployments.

Add-on service packages include:

Basic Log Monitoring

Threat Detect & Notify

Advanced Threat Detect & Respond

Threat Management Platform

The Threat Management Platform offering ingests Syslog, WMI, and agent based logs from different sources (such as firewalls, switches, and servers) and correlates those logs with industry threat data signatures to identify behaviors that signal the indicators of a potential threat event, such as someone trying to log into multiple computers in a short period of time, submitting multiple incorrect user ID and passwords in rapid succession, or the rapid connections to multiple machines via commonly known windows service ports. These threat behavior patterns are gathered from, and updated, based on subscribed industry threat data feeds, keeping current with up-to-date data of potential malicious activities.

Additional phoenixNAP services

Patch Management	This automated Patch Management system ensures that available patches for security vulnerabilities are applied in a timely manner and through a proper change control process.
Critical Environment Recovery (7 Day Encrypted Backup)	Critical Environment Recovery services allow clients to recover if a serious security event happens, such as a crypto-virus, by rolling back to a known good state following a malicious attack or malware event.
Firewall/Switch Management	Firewall/Switch Management allows an organization to access skilled and certified individuals using a fractional contracted services model, resulting in considerable cost savings over hiring an in-house administrator with the same level of expertise. Our experts configure and manage firewalls and switches based on industry best practices in addition to monitoring performance and maintaining patching protocols.
Configuration Management	Our integrated tools and SOC analysts review backup data against authorized change data and alert on anomalies, identifying changes quickly that could have adverse impact to security.
Vulnerability Assessment	phoenixNAP provides clients with business-friendly reports that show valuable KPIs and performance of those KPIs over time. These proactive reports are also useful within audit frameworks required for various compliance and business needs.
Performance Monitoring	Our performance monitoring allows you to gauge over what periods of time a system is performing well and when it's overloaded. Once a system is identified as overloaded, it becomes a trigger for upgrades or other actions, such as running parallel servers during certain times.
End Point Security	Using AI, behavior analysis, and signature-based models, pNAP's End Point Security offering helps prevent crypto-viruses and malware from infecting end-user devices, initiating recovery procedures natively included in the operating system or via recovery from backup.

Want to learn more about phoenixNAP's Data Security Cloud solution and security services offerings?

Please visit www.phoenixnap.com/data-security-cloud

phoenixNAP GLOBAL IT SERVICES

intel

vmware

1: datacenterfrontier.com/a-look-at-data-center-of-the-future
2: Gartner, 2016, "Predicts 2017: Endpoint and Mobile Security"
3: Ponemon Institute, 2016, blog.lookout.com/gartner-mobile-security-predictions
4: CSA, 2017, downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf