Improving Network Security with Arraya and VMware NSX

Your network is the backbone of your IT infrastructure. The connectivity between your systems, end users and the outside world must be highly-available or your services and users will suffer the consequences. Meanwhile, the perimeter of the traditional network is being redefined, with cloud-based applications, hosted disaster recovery, and remote and roaming end users. It's important that you constantly evaluate the state of your ecosystem and the current risk level of threats, and evolve your networks to address them.

VMware NSX for Network Virtualization

Networks as we know them are expanding to incorporate software-based solutions that promise interoperability, agility and centralized management. This includes the introduction of platforms like VMware NSX to manage network flow and segmentation. Networking, through the use of solutions like NSX, is becoming programmable, leading to new opportunities for orchestration and automated intelligence.

Abstracting your Network

NSX separates networking and security functions from the hardware that traditionally manages them. Networking and security policies are defined and managed centrally, then deployed at the workload, application or end user level. This changes the networking and security operational model to more closely resemble that of a virtual machine (VM), resulting in a more agile and secure data center.

Some of the most notable benefits of a virtualized network include:

Agility

The ability to implement network changes more quickly and accurately than can be done when provisioning physical networks

Flexibility

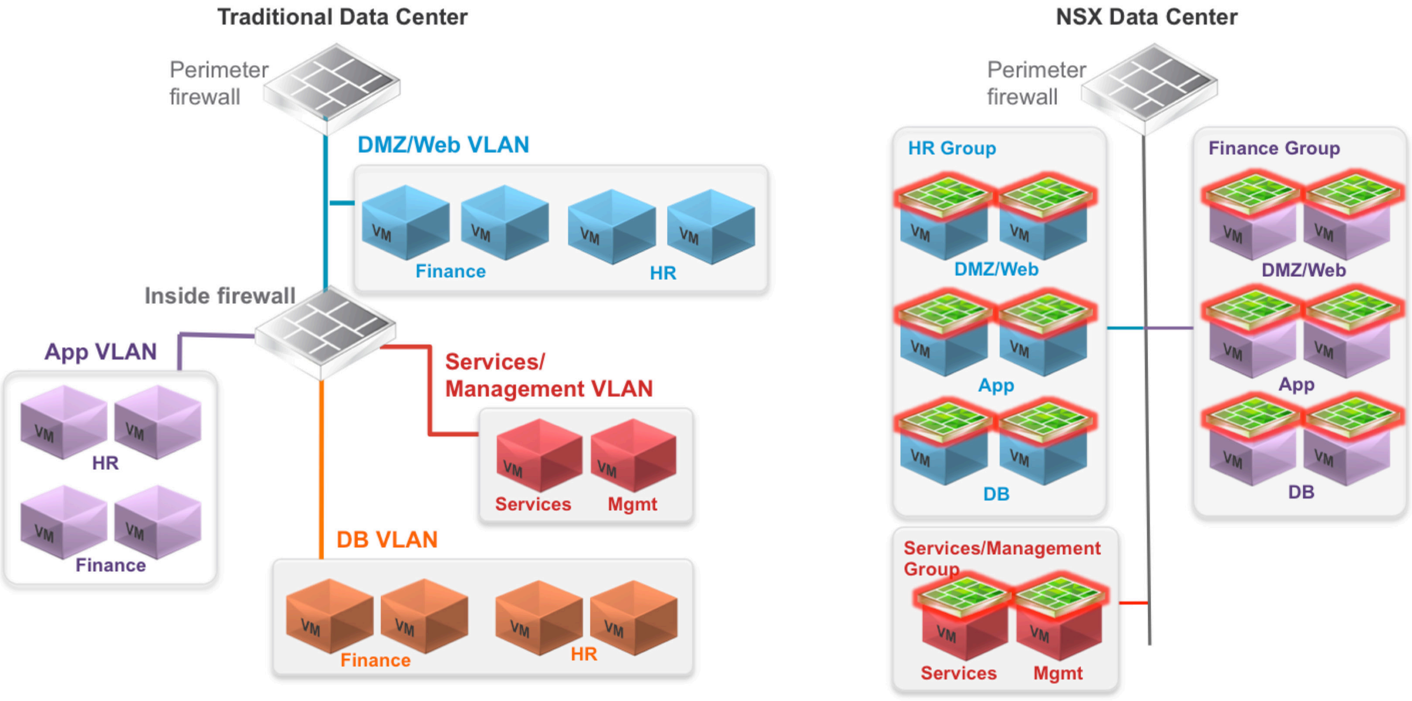
Because network and security parameters are handled at the workload level, applications can move across data centers and to the cloud, without requiring physical network changes

Security

Network virtualization enables micro-segmentation – a more effective approach to security that monitors traffic as it flows between systems and workloads

Improved Security through Virtualization

While network security has traditionally done most of its work at the perimeter firewall, network virtualization enables the concept of micro-segmentation. This allows network administrators to apply security policies to workloads, applications, systems and users, essentially creating firewall type protection throughout your network. This lateral protection, until now, hasn't been operationally (or financially) feasible.



Core capabilities of micro-segmentation

Visibility

East-west traffic typically does not go through a firewall, making it invisible to security teams. Through virtual networks, hypervisors running on your systems are in a position to see all traffic in a data center, giving your security team unprecedented control at the workload level.

Isolation

Isolation is important for compliance, containment, and separating dev environments from production. Virtual networks are inherently isolated from other virtual networks as well as from the underlying physical network. No physical subnets, VLANs, ACLs, or firewall rules are required.

Segmentation

Traditionally, a physical firewall or router controls traffic between network segments. Unfortunately, network segments are often too large to be effective and time consuming to configure. In a virtual network, services are programmatically created, deployed to virtual switches, and enforced at the virtual interface – eliminating the need to be configured in the physical network.

Automation

Automated provisioning enables the correct firewalling policies to be used when a workload is created. If the application is deleted, its security policies are automatically removed from the system. This eliminates "firewall rule sprawl" which can result in hundreds, even thousands of floating, outdated firewall rules that can cause performance and security issues.

Key Benefits of Micro-Segmentation

1. Minimize Risk and Impact of Data Center Breaches

If a threat infiltrates the data center, micro-segmentation contains and blocks its lateral (east-west) movement to other servers, preventing attackers from exploiting other systems and dramatically reducing the risk to the business. This cuts down on the financial impact by avoiding legal expenses, customer turnover, time spent on investigations, and lost productivity.

2. Accelerate Time to Market with Automated IT Service Delivery

Enterprises can use micro-segmentation to provision security services with the same agility, speed, and control as virtual machines (VMs) for cloud-native and traditional applications and computing. App teams can have access to self-service provisioning, bringing new applications and services online in seconds or minutes, not days or weeks.

3. Protect Existing Network Investments

Because virtual networks require little to no configuration changes to the underlying physical network, they can transparently coexist on the physical network with as much micro-segmentation as needed for workloads. With micro-segmentation, businesses can leverage physical network and security equipment already in place and, in many cases, extend the life of the existing infrastructure.

4. Lower Operating Expenses

Micro-segmentation dramatically reduces the effort and time required to execute security tasks like provisioning, changes, scaling, and troubleshooting – reducing turn around times from weeks or days, to hours or minutes, with some no longer requiring human intervention at all.

5. Achieve Both Speed and Business Agility

Businesses are often forced to choose between speed and security. Safety restrictions can get in the way of business agility, often times inspiring rogue shadow IT projects designed to circumvent these "barriers". Network virtualization and micro-segmentation enable businesses to rapidly — and securely — innovate to create a competitive advantage while maintaining persistent security throughout the data center and beyond.

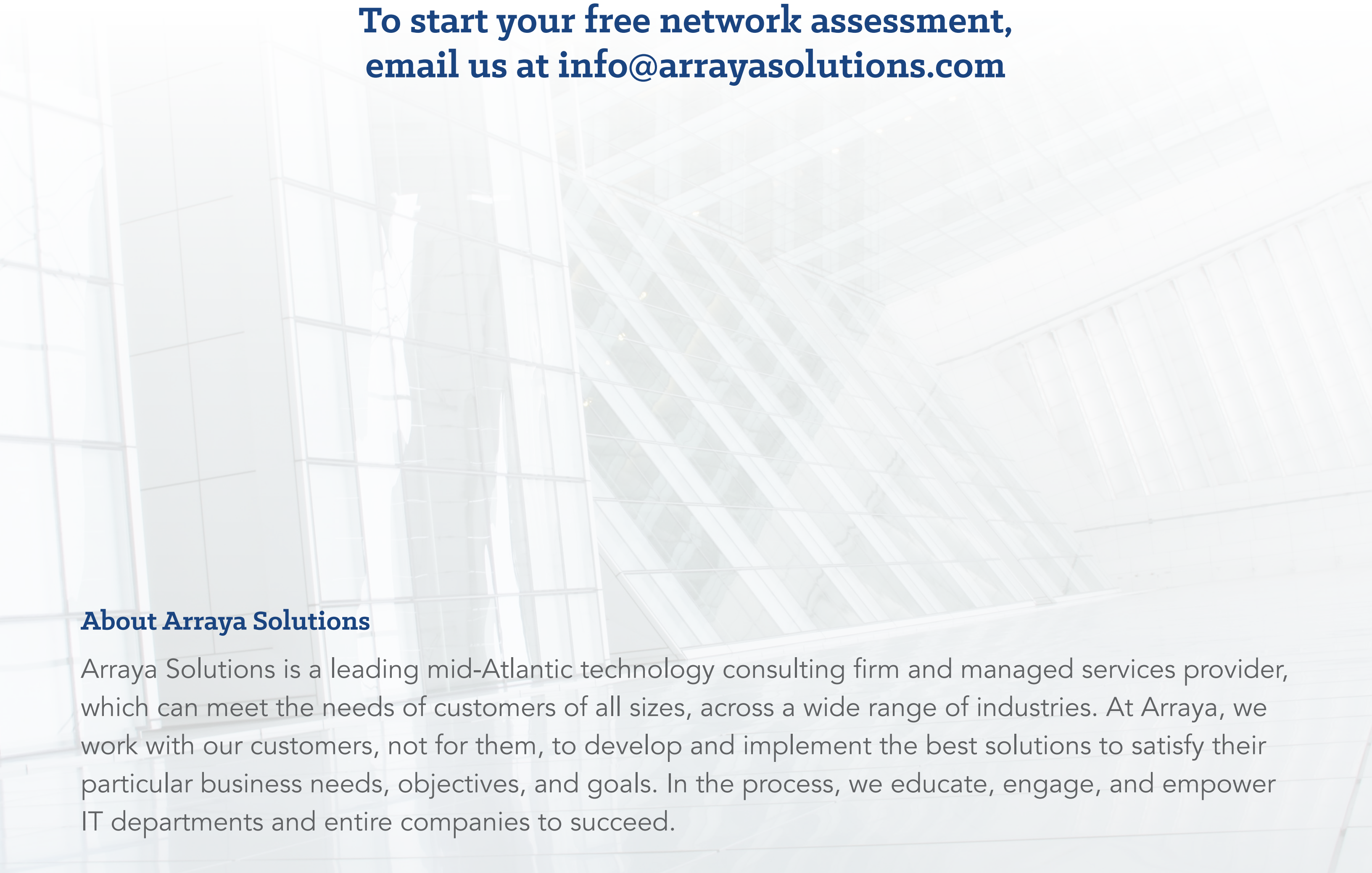
Getting to your Ideal Data Center End State

The Arraya Solutions Virtualization team can help your business determine if you can benefit from a network virtualization solution, making your networks application aware and directing resources where needed most. Experience all the benefits of a virtualized network, including more control over your security, through a partner with broad and deep experience planning, implementing and growing virtual networks. Micro-segmentation is the number one reason companies are interested in VMware NSX, and Arraya can handle your deployments start to finish.

Free Network Assessment

Sprawling networks and unclear perimeters can make it challenging to know everything that's in your environment. The structure and layout of your network must be evaluated to ensure availability, validate security and guarantee performance. Arraya is offering a FREE network assessment that will give you a holistic view of your network ecosystem and security gaps. We use an application-focused tool that provides deep insights into network infrastructures, reducing the time required to plan and configure application security by up to 70%.

**To start your free network assessment,
email us at info@arrayasolutions.com**



About Arraya Solutions

Arraya Solutions is a leading mid-Atlantic technology consulting firm and managed services provider, which can meet the needs of customers of all sizes, across a wide range of industries. At Arraya, we work with our customers, not for them, to develop and implement the best solutions to satisfy their particular business needs, objectives, and goals. In the process, we educate, engage, and empower IT departments and entire companies to succeed.