SUCCESS STORY

CLIENT ACHIEVES UP TO 70% FASTER APP ROLLOUTS WITH VMWARE NSX-T

Overview

As digital transformation accelerates across the financial sector, organizations are under growing pressure to modernize legacy infrastructure while maintaining airtight security and uninterrupted availability. One of Pakistan's prominent PSO/PSP organization recognized the limitations of its existing NSX-V environment particularly its inability to support physical infrastructure, modern workloads, and agile deployment cycles. To overcome these barriers, the organization partnered with Jaffer Business Systems (JBS) to implement VMware NSX-T, enabling unified security, network automation, and full infrastructure coverage. By adopting this next-generation platform, the institution significantly strengthened its operational agility, improved policy consistency, and **positioned itself for scalable, secure growth in an increasingly complex IT landscape**.

Solution Overview

- **Solution Partner:** JBS (www.jbs.live)
- **Solution Implemented:** Migration from VMware NSX-V to VMware NSX-T to modernize the organization's software-defined networking capabilities.

Challenges

Limited Support for Physical Infrastructure	NSX-V only supports virtualized workloads within VMware vSphere environments. This presents a significant challenge for financial institutions, which often depend on physical servers to run latency-sensitive or legacy systems such as trading engines, mainframe-based services, or core banking applications. Since NSX-V cannot extend its network and security capabilities to physical infrastructure, these critical systems remain outside the scope of centralized policy enforcement and visibility. This creates security blind spots and operational silos, increasing both risk exposure and management complexity.
No "DMZ Anywhere" Capability	NSX-V required physical firewalls and load balancers to establish DMZ zones for securing public-facing services. This dependency on hardware created cost overhead and delayed service rollouts, especially problematic for organizations seeking rapid deployment of digital channels such as online portals and mobile applications.
Fragmented Security and Policy Framework	Security policies in NSX-V applied only to virtual machines. This fragmented approach forced IT teams to manage separate tools and configurations for physical systems, increasing administrative overhead and the risk of misalignment. In a highly regulated financial environment, this disconnect threatened both compliance and resilience.
Inadequate Support for Modern Architectures	NSX-V didn't offer native support for modern technologies like Kubernetes or microservices, which are now widely used to build digital banking applications. As financial institutions adopt faster and more flexible development approaches, such as DevOps, NSX-V struggles to keep up. It lacks the ability to provide consistent networking and security for these dynamic environments, leading to operational inefficiencies and slowing down the rollout of new digital services.

The Solution Provided by JBS

VMware NSX-T is an advanced software-defined networking solution designed to **deliver unified security, automation, and visibility across diverse IT environments**, including virtual machines, physical servers, containers, and bare-metal workloads. Implemented by Jaffer Business Systems (JBS), the platform enables organizations to establish consistent network and security policies, streamline operations, and **enhance infrastructure resilience without reliance on physical hardware**. Ideal for modern enterprises, NSX-T supports scalable, agile application delivery and end-to-end threat containment across hybrid infrastructures.

How It Solved the Challenges

Full Infrastructure Coverage: Physical + Virtual

NSX-T extends its capabilities to include both virtual and physical servers, as well as containers and bare-metal workloads. This is especially important for financial institutions, which often depend on legacy or high-performance physical systems such as trading platforms and core banking applications. By enabling consistent networking and security policies across all types of environments, NSX-T eliminates silos and closes security gaps, ensuring a more unified and secure infrastructure.

Up to 90% Reduction in Lateral Threat Risk

Through micro-segmentation applied consistently across all workloads and platforms, NSX-T mitigates lateral movement by potential threats. This comprehensive enforcement mechanism significantly enhances internal security posture and reduces the risk surface.

Up to 70% Faster Application Rollout with DMZ Anywhere

NSX-T enables a flexible “DMZ Anywhere” approach so organizations can extend the DMZ into any part of the network by applying firewalling, load balancing, and security policies directly through software. This eliminates the need to redesign the network or invest in additional physical appliances to create or expand DMZ zones. For financial institutions, which must provide secure access to public-facing services such as customer portals and mobile apps, this capability is especially valuable. With DMZ Anywhere, secure deployments are accelerated from weeks to days enabling up to a 70% faster rollout of applications.

Reduced Infrastructure and Operational Costs

By eliminating the reliance on physical appliances for network security and traffic management, NSX-T reduces both capital expenditures and day-to-day operational costs. Built-in capabilities enable financial institutions to scale securely and efficiently without the financial burden of hardware expansion.

99.99% Application Uptime and Availability

NSX-T integrates automated high-availability configurations and disaster recovery capabilities. This ensures minimal downtime and robust failover support, which is critical for business continuity particularly in mission-critical environments like banking and trading.

25% Optimization in IT Resource Allocation

Through automation and streamlined network operations, NSX-T reduces the need for manual intervention. This results in a 25% reduction in required human resources, allowing IT teams to focus on strategic priorities rather than routine tasks.

Why JBS

- A **proven track record** of successful project deliveries with measurable outcomes
- **Expert-level certifications** in cybersecurity, guaranteeing deep technical expertise and best-in-class implementation

Key Benefits of the Solution

- **Up to 90% Reduction in Lateral Threat Risk**
- **Up to 70% Faster App Rollout**
- **99.99% Uptime**
- **25% Reduction in Human Resources**
- **Significant Cost Savings**
- **Full Infrastructure Coverage**

Conclusion

With JBS's strategic expertise and VMware NSX-T's advanced network architecture, the financial institution successfully modernized its infrastructure, achieving stronger security controls, faster application delivery, and streamlined operations. The shift enabled consistent policy enforcement across both virtual and physical environments, reduced operational overhead, and established a **resilient, future-ready foundation for secure digital transformation**.

Contact Us

For more information on how JBS can revolutionize your IT operations please visit www.jbs.live or contact us at marketing@jbs.live