Automated security policies

Simplified operations

Enables seamless disaster recovery

Reduced dependence on network hardware devices

Secure modern applications across multi-cloud environments

VMware Simplifies And Hardens Security Operations For Bharti Airtel, Enabling Rapid Time-to-Market

Improved service roll-out with VMware

In today's dynamic telecom industry, operational simplicity and accelerated application adoption is the key to business transformation and customer experience.

Bharti Airtel Limited, also known as Airtel, provides telecom services to more than 420 million customers in 18 countries across South Asia, Africa and the Channel Islands. The company's Airtel Thanks application is especially critical to the company's customer experience strategy, giving users more visibility and control over their service subscriptions, data consumption and billing—a critical requirement for today's increasingly savvy consumer.

In light of fierce competition and high consumer demand for the roll-out of new services, Airtel felt limited due to its existing legacy networking and security architecture. Despite the size and the scale of its operations, Airtel found it challenging to adapt to the changing preferences of its consumers. Among the primary reasons for these challenges were complexities and limitations in the use of traditional physical firewalls.

Bharti Airtel is a leading telecommunication company in India. Besides operating one of India's largest cellular networks, it offers a wide range of products and services such as Airtel Payments Bank and Airtel Live TV to customers in 18 countries.

INDUSTRY

Telecommunications

HEADQUARTERS

New Delhi, India

VMWARE FOOTPRINT

VMware NSX®
VMware Site Recovery Manager™
VMware Horizon®
VMware vRealize® Operations™
VMware vRealize® Automation™
VMware vRealize® Log Insight™
VMware vRealize® Network Insight™
VMware vSAN™
VMware vSphere®
VMware Professional Services

The mobile application runs in a private cloud split into development, production and DMZ environments. Securing and segmenting the three zones proved difficult using the company's 200 physical firewalls that protect approximately 4,500 physical servers and more than 15,000 virtual machines. The appliances required hair pinning of traffic that created latency, scalability, visibility and performance issues—especially during periods of massive traffic spikes due to new roll-outs. Additionally, it also made it difficult for engineers to iterate quickly and roll-out new features and app updates because of the complexity required to steer traffic through multiple environments.

Transitioning from legacy systems with VMware

Recognizing the benefits of VMware's integrated, best-of-breed network security stack, Airtel deployed VMware NSX® Data Center, VMware Horizon® and VMware vRealize® Automation™ to easily create virtual security zones and granularly segment the app during peak traffic demands. Taking a software approach to network segmentation allows Airtel to radically simplify its network security architecture, scale capacity and services as needed and harden security. This change in strategy makes it easier to iterate quickly and launch updates of the Airtel Thanks app.

Unparalleled efficiency unlocked with NSX Service-defined Firewall

Airtel deployed VMware's NSX Service-defined Firewalls (SDFW) across approximately 12,500 virtual servers. This East-West internal firewall enables granular segmentation and security across the development, production and DMZ zones without having to add additional firewalls or increasing complexity. Eventually, Airtel plans to phase out more than 200 physical firewall appliances—migrating to an exclusively software-defined network security model powered by VMware.

The use of a tag-based approach enabled Airtel to optimize its firewall policies and accelerate the movement of virtual machine applications. Moreover, the system dynamically adapts to any change.

SDFW now enables Airtel to configure and manage its operations from a single panel instead of having to troubleshoot across a wide array of physical components. In addition, it offers the convenience of seamlessly upgrading existing security policies.

SDFW gives Airtel greater control over specific application servers at a vNIC level—unlocking a new level of granular control and complexity that was previously unattainable with physical firewall appliances.

The implementation of the NSX Data Center enables segmentation, distributed routing and switching capabilities and the automation of networking and security services while ensuring seamless day 2 operations.

In addition, the move from physical appliances to software-defined infrastructure will greatly reduce complexity and enable cloud-scalability.

Scaling the development of applications with vRealize Automation

VMware vRealize Automation helps Airtel deploy network and security on-demand with its application stack. As a result of the close integration between NSX and vRealize, Airtel is able to speed up the delivery of its business-critical applications and support the growth of its business.

"Previously, our legacy physical firewalls added layers of complexity during mission-critical troubleshooting. Besides, the lack of automation and inconsistency in configuration limited policy information when we needed it the most. Deploying NSX SDFW has turned this around by optimizing our firewall policies by reducing our firewall rule count by over 30 percent."

MANISH SINGH
GENERAL MANAGER – CLOUD OPERATIONS, BHARTI AIRTEL

Simplified Day 2 operations with Professional Services

The Airtel Engineering team had always found it a challenge to operationalise and optimise network security. VMware vRealize Automation provides a single dashboard with access to performance parameters allowing the team to easily automate processes with just a few clicks.

The VMware solution improves efficiency, automates mundane mechanical tasks and empowers the team to deliver seamless service roll-outs. The management of security policies is now streamlined and consistent, with regular monitoring and alerts happening in real-time. The surge in resource utilization during the roll-out of a new service for Airtel is no longer a challenge but an enabler to delivering better services for customers.

With an exponential growth in network operations, it was critical for Airtel to streamline day 2 operations to reduce complexities in managing their environment. A reduction of firewall footprint by identifying dormant firewall rules in the NSX environment led to efficient management and enhanced network security.

The VMware Professional Services team and Technical Account Manager partnered closely with the Airtel Network Operations team to ensure a healthy environment and continuous operations improvement through automation and implementation of industry-leading practices.

VMware vRealize Network Insight (vRNI) solution has helped simplify network and security operations monitoring by introducing customised pinboards for firewall insights and network insights that helps provide a detailed view of NSX logical network, components and proactive reporting of configuration issues along with best practices recommendations. To sustain network operations effectively, proactive upgrade of network solution has ensured continued reliability, stability of the environment.

Looking Ahead

The COVID-19 global pandemic and its aftermath resulted in a 30 to 50 percent traffic surge. Thanks to network simplicity and flexibility provided by NSX and network segmentation, Airtel has been able to manage the increased traffic seamlessly without impacting planned services roll-outs and upgrades.

Moving forward, the organization is looking to expand its investment in NSX with capabilities such as Federation, Advanced Load Balancer, Container Networking, IDS/IPS, and Firewalling for bare metal infrastructure.

Moving away from legacy technology, #Airtel has transformed operations and augmented capabilities through automation in partnership with @VMware

---