NETSCOUT

Manufacturer Successfully Migrates to Edge Cloud Architecture with NETSCOUT

Worldwide Visibility and Quick Time-to-Value with nGeniusONE, nGeniusPULSE, Arbor Edge Defense, and nGenius VaaS

OVERVIEW

The Challenge

- Legacy data center technology in remote locations was costly, inflexible, and difficult to maintain
- Planned on technology refresh but needed visibility for migration success and ongoing performance and availability

The Solution

- nGeniusONE® Service Assurance platform, Arbor Edge Defense, and nGenius®PULSE
- InfiniStreamNG™ software and vSTREAM™ virtual appliances
- nGenius Packet Flow Switches
- nGenius Visibility as a Service

The Results

- Migrating to cloud services with confidence with visibility and analysis
- Achieving goals of cost-effectively bringing services closer to end-users, while maintaining quality performance

Customer Profile

This US-based manufacturer of high-tech software has several development centers and dozens of sales offices globally. Their customers, some of the world's largest, most demanding enterprises, government agencies and service provider organizations, depend on their 24 x 7 x 365 support services for maintaining production deployments of the manufacturer's equipment.

Availablity for communicating among and between all these locations is critical, as new product development, sustaining engineering, training, sales & marketing, and customer service & support services are conducted out of many of these offices, and each function depends on immediate collaboration at any given time. Slowdowns or unavailablity in voice, video or business data services are simply not an option, which is why they have been a long-time NETSCOUT® customer.

The Challenge

The manufacturer had more than a dozen development centers with varying levels of on-premise data center equipment. The company had deployed a common architecture at the time – hosting most of their core services, like e-mail, unified communications (UC), file sharing, authentication (i.e., Microsoft Active Directory), and customer resource management (CRM) – in the primary data center, with expensive Multi-Protocol Label Switching (MPLS) links supporting remote site access. However, this approach had an expensive total cost of ownership, required high touches to maintain, and needed IT professionals to help troubleshoot. The manufacturer needed greater agility in service changes than this deployment allowed them, and they knew IT transformations offered beneficial approaches with significant advantages. Over time, many of their core services had transitioned to cloud and virtual, including:
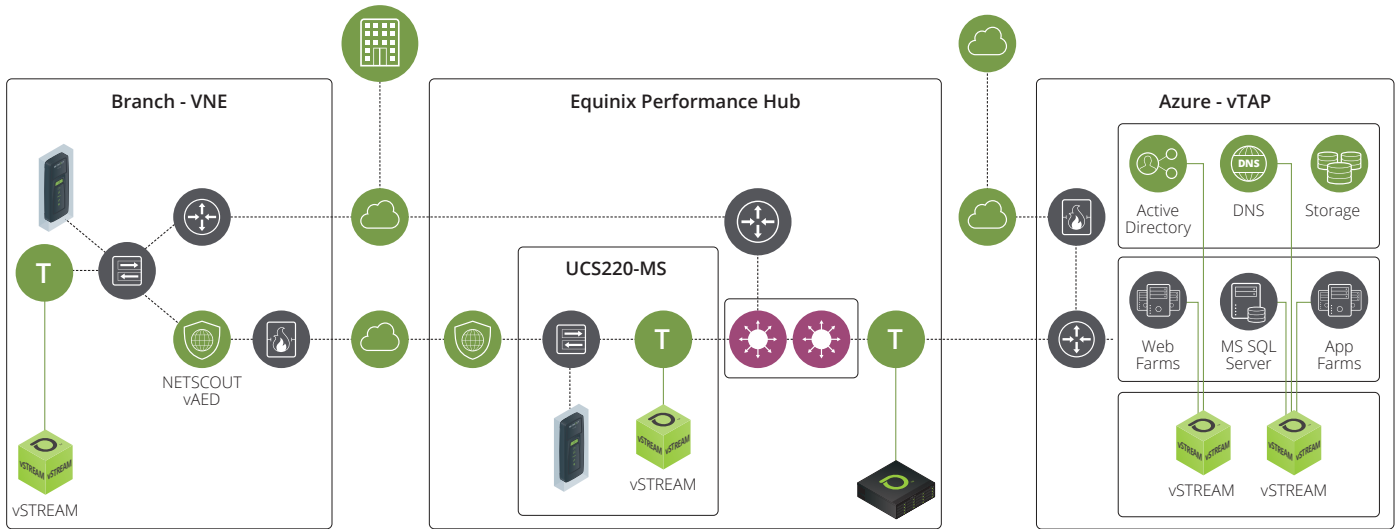
ENTERPRISE

Figure 1: Manufacturing company's deployment model for performance and security management of their multi-cloud migration. Visibility is provided by nGeniusONE with ISNG software and vSTREAM virtual appliances, nGeniusPULSE and virtual nPoints, and AED across the branch, co-lo, and public cloud network.

- Microsoft Office 365 Software-as-a-Service (SaaS)
- Cisco WebEx collaboration services
- SalesForce.com CRM
- ServiceNow service and support software

These new service rollouts were accessed via Internet links at the company's remote offices.

The strategic plan developed by the IT staff covered several data center transformations including an Infrastructure and Platform-as-a-Service initiative that included moving their Active Directory, Storage, and Print services to the Microsoft Azure (Azure) cloud. They also decided to leverage Network Function Virtualization (NFV) on-prem to virtualize their routers, firewalls, storage, backups, ancillary applications; and SD-WAN access through Equinix Co-location (Co-lo) facilities to both Amazon Web Services (AWS) and Azure public clouds. This has now effectively built a cloud edge for their North America, EMEA, and APAC remote locations that gives them freedom to deploy resources where it makes the most sense for a particular workload, while significantly reducing their on-premise data center requirements.

Albeit the many benefits to this new architecture design, cloud-based operations created new 'blind spots' that prevented the manufacturer from knowing and ensuring their end-users were getting the level of performance and stability that they had come to expect in an on-prem world. Furthermore, security is different in virtual, software-based infrastructure. So, in order to ensure both quality performance and secure availability, they worked with their strategic partner NETSCOUT for service assurance and security solutions for this new environment.

Solution in Action

The IT staff implemented NETSCOUT solutions for visibility of their critical cloud and SaaS applications to assure both performance and security needs were met with the new architecture. They selected a combination of the following:

- **nGeniusONE Service Assurance platform** for real-time application and network performance, leveraging Adaptive Service Intelligence (ASI) technology in InfiniStreamNG (ISNG) software and vSTREAM virtual appliances.

- **nGeniusPULSE** is providing insight via nPoint active testing sensors into the IT ecosystem for availability, reliability, and performance of business services across the multi-cloud environment – from wherever users need access, even during off-business hours to get ahead of emerging issues.

- **Arbor Edge Defense** (AED) for security protection as the first line of defense against inbound DDoS and Incidents of Compromise as well as the last line by detecting and blocking outbound communications to known bad sites.

To gain the most cost-effective and complete visibility into their multi-cloud environment, the IT team architected the following deployment strategy.

- **Public Cloud (Azure)** – vSTREAMs are deployed to monitor east-west traffic of each the virtualized applications (i.e., AD, DNS, MS SQL Server, Web Farms, and other applications) leveraging Microsoft Azure vTAP capabilities.

- **Co-lo Hubs** (Equinix) – There are four points of visibility at these locations:
    - AED is deployed at the Internet connection side of the Hub for DDoS protection.
    - vSTREAM is deployed to monitor SD-WAN traffic and the MPLS routers.
    - Virtual nGenius PULSE end-points are implemented for continuous testing across SD-WAN, even when users are not sending traffic.
    - ISNG appliances are monitoring north-south traffic from the Co-lo to the public cloud for service assurance analysis by tapping the physical link to the internet.

- **Branches Worldwide** – Here again, they are selecting multiple visibility points at the branches
    - vSTREAM is monitoring SD-WAN traffic and the MPLS routers.
    - Virtual nPULSE end-points are implemented in the virtual server for continuous testing of SD-WAN, even when users are not sending traffic for proactive analysis.
    - AED is deployed just inside the virtual firewall for DDoS protection.

Finally, with the IT team heavily invested in the cloud migration project already, the IT team augmented their "staff" with NETSCOUT's nGenius Visibility as a Service (nVaaS), experienced personnel from NETSCOUT that manage the new equipment and help configure and optimize the overall deployment. With professionals well-versed on all the products, the nVaaS team was able to build dashboards, service monitors, reports, business transaction tests, alerts and logical workflows, and processes across the platforms to stay ahead of problems as they emerge as well as investigate and troubleshoot issues that may impact their environment. The nVaaS team was also able to share their best practices for tuning and optimizing the manufacturer's services across the cloud to improve user experience overall.

The Results

The new architecture design is giving this manufacturer the freedom they need to deploy resources where it makes the most sense for their critical services and workloads, while significantly reducing their on-premise data center requirements and expenses. The IT team is working closely with their third-party vendors around the world leveraging their NETSCOUT solutions for collaboration with visibility and evidence to meet their evolving needs and assist in troubleshooting when necessary to meet their agreed upon SLAs. And as a result, with the service assurance and security management solutions they have deployed from NETSCOUT, they are realizing valuable, early returns on their investment in this cloud strategy.

The combination of these solutions enables the IT team to get ahead of, and to logically troubleshoot challenging, cross-domain issues, quickly and efficiently, to reduce the time to respond to performance and security issues. By lowering mean-time-to-resolve (MTTR) complex issues, this manufacturer is reducing the impact on revenue and customer quality of experience while simultaneously avoiding time lost to vendor finger pointing and unproductive war room sessions.

The IT team at this manufacturing company is benefiting from broader, more detailed level of performance and security visibility than they have ever had. With precise analysis, the solutions pinpoint the source of a performance degradation or a security risk. With nVaaS involved in many of the issues, they have experienced an accelerated time to value of the overall solution set and are reaping the benefits of getting information to the right staff member at the right time, so they can quickly proceed with the appropriate corrective action to restore quality service to all their users around the world. Working with a single vendor has cut down on both vendor and tool complexity, unnecessary maintenance costs, and improved solution interoperability across all their monitoring solutions.

For a high-tech business that has quality customer service as a cornerstone of their success, this manufacturer is achieving that goal with visibility from NETSCOUT.

LEARN MORE

For more information about NETSCOUT solutions for Manufacturing organizations, please visit:

https://www.netscout.com/solutions/digital-transformation-manufacturing

NETSCOUT.