NETSCOUT Smart Edge Monitoring

Numerous, concurrent enterprise business transformations have converged, leaving many information technology (IT) teams to report feeling they have "lost control." Atop these collective challenges are the Data Center Transformations and Hybrid Workforce Realities described in the subsections that follow.

Data Center Transformations

The Data Center Transformation projects described below are at times rolled out concurrently, frequently involving multiple enterprise locations.

Cloud Migrations

Private, public, hybrid, and multi-cloud services are deployed to address numerous digital transformation strategies, such as application and workload migrations. Many enterprises take advantage of multi-vendor strategies mixing AWS®, Microsoft Azure®, Google Cloud Platform®, and Oracle Cloud Infrastructure (OCI) services to reduce reliance on a single provider, improve geographic coverage for regional offices, access competitive pricing, and secure premium service level agreements (SLAs).

The NETSCOUT Smart Edge Monitoring solution arms today's IT teams with a solution that delivers rapid troubleshooting and faster mean-time-to-remediate issues impacting remote users, with a combination of packet monitoring and synthetic testing in a single platform.

"As-a-Service" Adoption

Enterprise applications and services are moving out of the data center and onto "as-a-service" platforms, including software (SaaS), UC (UCaaS), Contact Centers (CCaaS), Desktop (DaaS), and Infrastructure (IaaS) solutions. With several of these services concurrently deployed across many enterprises, IT teams are again relying on multi-vendor solutions to support business services required by users, with some of these same third parties responsible for delivering reliable application performance in compliance with respective SLAs.

Data Center Migrations

Data center services are in the midst of an extended move to Co-located (Co-lo) and Carrier-Neutral Facility (CNF) environments, which offer the dual promises of cost containment and service efficiencies, but again involve migrating enterprise services from on-premises operations to trusted third-party (TTP) facilities.

Software-Defined Network (SDN) Rollouts

Enterprise IT teams are deploying SDN solutions like virtualized Software-Defined Data Center (SDDC) network services provided by Cisco Application Centric Infrastructure SDN and VMware to take advantage of simplified management, micro-segmentation security, provisioning agility, and improved data center economics. Amid these benefits, IT teams need visibility into SDN-based virtual services to assure performance before, during, and after migration.

Hybrid Workforce Realities

Today's hybrid workforce realities represent a second, equally important transformation that IT needs to manage. Initially established as an organizational response to stay-at-home work orders, the hybrid workforce is here to stay for reasons that include:

- **Safety** – Full on-premises workforce transitions will likely remain delayed until the healthcare impact of the pandemic subsides, with employees rotating back to corporate facilities according to controlled schedules (e.g., two weeks per month).
- **Investment** – Enterprise investments and IT efforts have focused on assuring virtual private network (VPN), virtual desktop infrastructure (VDI), and software-defined wide area (SD-WAN) services that were procured, scaled, and tuned to provide reliable business service access to remote workers. Other solutions include cloud access security brokers (CASBs),

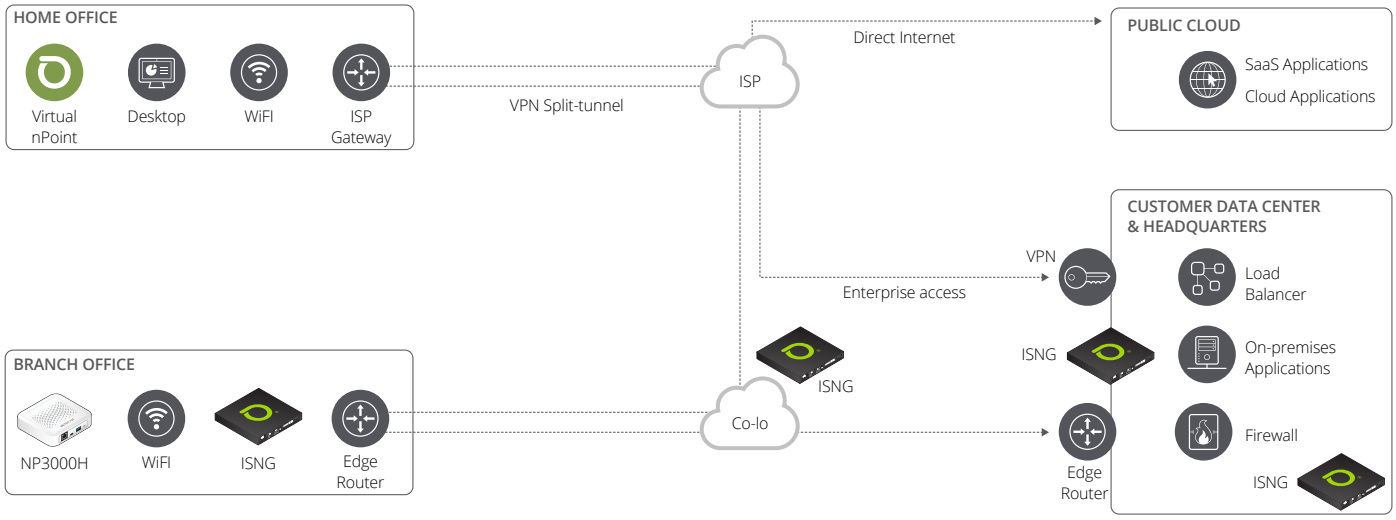

Figure 1: The NETSCOUT Smart Edge Monitoring solution provides visibility into user experience from any location, on any enterprise business service platform.

and secure access service edge (SASE) technologies. Given those investments, as well as employees shifting from corporate locations to WFH environments and vice versa, these remote business services will require continued visibility, monitoring, and troubleshooting to assure reliable operations, factoring the following considerations:

- **Productivity** – Remote employees may well return to their employers' on-premises facilities, but the home offices and anytime/anywhere work habits developed during the pandemic are here to stay.
- **Economy** – With more employees in WFH environments, many businesses are re-evaluating their corporate real estate footprints.

These collective challenges have left IT operations resources with a sense they need to be "everywhere at once" to assure user experience and service quality.

Our Approach

The NETSCOUT® Smart Edge Monitoring solution expands the scope of visibility into user experience and service delivery critically needed by IT operations to monitor their transformed enterprise environments. NETSCOUT Smart Edge Monitoring provides visualization into today's service edge environments, specifically including:

- **Client Edge** – Wherever the user is performing their job, including: WFH environments; remote branch offices; Contact Centers; individual floors at a company headquarters; manufacturing factories and plants; hospitals and medical buildings; and warehouses and distribution centers.
- **Network Edge** – A physical or network boundary that often coincides with a change of control or ownership in an end-to-end service, including: Connection from a remote site to the Internet, WAN, or SD-WAN; peering locations in Co-los (e.g., with public cloud, Internet); VPN concentrators and/or VDI load-balancers for remote access; firewalls, DMZs, and load balancers for security; centralized SD-WAN concentrators at data centers; Co-lo's and/or public cloud; private data center edges.
- **Data Center Service Edge** – The first Server Edge is the first application server that traffic from the client hits (first north-south traffic), and other Server/Workload edges are the subsequent tiers (east-west traffic) in the service delivery chain.
- **Cloud Service Edge** – The Cloud Service Edge factors widely "as a service" business (e.g., Microsoft Office 365, Salesforce, Workday, NetSuite) and UC&C (e.g., Cisco Webex, Microsoft Teams, Zoom, Slack) applications, as well as cloud infrastructure solutions (e.g., Microsoft Azure, Amazon Web Service, Google Cloud, Oracle Cloud Infrastructure).

Our Solution

Leveraging NETSCOUT's "last-mile" visibility across the full service edge environment, our Smart Edge Monitoring solution uniquely combines and extends the benefits of our market-leading nGeniusONE® Service Assurance smart analytics with our award-winning nGenius®PULSE synthetic testing solution in a single platform to provide critical insights into end-user experience.

Our Smart Edge Monitoring performance analytics take advantage of NETSCOUT's patented Adaptive Service Intelligence® (ASI) technology in both InfiniStreamNG® (ISNG) and virtual vSTREAM® packet-based data sources, as well as nGeniusPULSE nPoint synthetic test sensors for key metrics. nPoint sensors deployed at the client edge in work-from-home (WFH) and other remote environments can be configured to generate synthetic tests for analysis by nGeniusONE to provide critical visibility into end-user experience. Of particular importance for WFH employees are frequently accessed as-a-service platforms, including SaaS, UCaaS, DaaS, and IaaS. The remote workforce often directly connects to these services through the Internet, bypassing the traditional north-south traffic visibility used by IT operations for communications passing through corporate data centers (as exhibited in Figure 1).

The NETSCOUT Edge Adaptor is an add-on module for the NETSCOUT InfiniStreamNG and vSTREAM appliances. The NETSCOUT Edge Adaptor enables nGeniusONE to analyze smart data from nGeniusPULSE nPoint synthetic tests to be combined with the packet-based smart data from ISNG and vSTREAM appliances for assuring user experience from remote offices and WFH locations. Rich analysis from the integration of the passive packet data with the active test results enables detailed nGeniusONE dashboard and monitor views, reporting and contextual drill-downs to key performance indicators, session analytics, and packet-based forensics.

Delivering Value to IT Operations

NETSCOUT Smart Edge Monitoring is a first-of-its-kind solution that merges synthetic test data with packet-based smart data derived from passive network monitoring for comprehensive analysis of end-user experience and business service performance, regardless of the respective locations of those employees or solution platforms.

In this manner, NETSCOUT Smart Edge Monitoring returns "control" to IT teams managing complexity in an evolving hybrid workforce and multi-vendor business service transformation environments, including:

- Improving quality of end-user experience at remote locations.
- Reducing MTTR and troubleshooting complexity with streamlined triage workflows.
- Collaborating more effectively with third-party vendors with verifiable performance data that validates SLA compliance.
- Getting ahead of issues before users are impacted.

NETSCOUT Smart Edge Monitoring in Action

Our Smart Edge Monitoring approach has provided NETSCOUT customers with solutions to the service edge visibility and user-experience service delivery challenges described opposite.

Improving Healthcare Service Edge Visibility

When this nationally acclaimed healthcare organization opened a new office facility on their main campus, IT Operations, Security Operations, and the newly outsourced Network Operations team quickly determined they did not have required visibility into this new service edge. That meant collective IT and NetOps resources could not visualize, monitor, or troubleshoot user experience, Epic Electronic Medical Records application performance, Microsoft Teams collaborations service quality, or business services that would be running in these new patient treatment, research, and administrative buildings. The NETSCOUT smart edge visibility approach closed those gaps, with IT operations supplementing already-deployed nGenius data sources by adding software-based ISNG appliances at the remote service edges. Adding software-based nGenius PFS's helped IT Operations to collect, distribute, and aggregate network traffic from various links in the new buildings to the ISNG appliances, as well as other cybersecurity tools employed by SecOps. NETSCOUT smart edge visibility provided IT Operations with the means to visualize and monitor healthcare service delivery to 5,000 essential staff members (i.e., doctors, nurses, research associates, and scientists) working at these new remote locations.

Closing WAN Service Edge Visibility Gaps

After one natural disaster came a little too close for comfort, IT leadership at this U.S. healthcare provider made the strategic decision to augment their existing business continuity preparedness by establishing a back-up location, which would also serve organization efforts to maintain compliance with regulatory standards regarding uninterrupted access to patient records. Major challenges faced IT leadership in terms of executing the required data transfers from the primary to the new DR location and subsequent daily updates (How much data needed to be replicated? How would the data be transmitted? What is the best way to back it all up without failures - e.g., dropped packets, errors, etc.?).

This NETSCOUT customer added ISNG appliances at the WAN edge of their existing data centers, which enabled IT Operations to monitor application back-ups as they were replicated to the new disaster recovery data center facility. IT executives in Data Center and Capacity Planning also added the nGenius 5100 packet flow switch (PFS) for visibility into wire traffic at the existing data centers to pass to the ISNG appliances for analysis across the WAN to the distant data center to ensure they had the necessary capacity for seamless replication of applications and patient records.

Reducing MTTR from 15 Hours to 15 Minutes

This company had recently experienced more than a dozen outages lasting in excess of five hours to triage, troubleshoot, and resolve. In some cases, they required a War Room to be spun up that involved 20+ IT staff members, vendors, and third-party service providers. Not surprisingly, some of these protracted outages gained the scrutiny of the new CIO and led to the formation of several action plans to reduce and avoid similar, future incidents.

Following a rigorous analysis of the several choices for network and application performance management available to this organization, the IT team collectively determined NETSCOUT, with its recently introduced Smart Edge Monitoring solution provided the level of detailed visibility, proactive analysis, early detection of emerging problems, troubleshooting workflows, and trending for baselining and capacity planning that would help them meet the CIO's directives.

Implementing the NETSCOUT Smart Edge Monitoring solution for end-through-end visibility not only helped the IT team meet their goal of eliminating War Rooms, they also reduced the average time to research, troubleshoot, and remediate problems from the earlier 10-to-15 hours per incident to 15-to-20 minutes

Improving Financial Technology Performance With Service Edge Visibility

This company found itself balancing commitments to expand corporate operations with efforts to manage pandemic-related business service disruptions. As a result, a team was established, whose mission included improving network operations reliability.

As this new team worked to resolve emerging service performance and application-related issues as part of their mission, they frequently referred to recommended-practices guidance provided by their NETSCOUT Premium Support Engineer (PSE). In these collaborative troubleshooting efforts, the PSE regularly discussed how adding smart visibility in a segmented environment was a NETSCOUT-recommended practice. This area had been established to secure primary data center operations and by adding visibility to these segments, they would succeed in closing blind spots that had surfaced across expanding network domains (i.e., service edges), including load balancers, gateways, and other critical network elements. Additionally, this area was serving as a hub for multiple services and incredible visibility around business-critical applications, where downtime meant lost revenue.

These smart edge visibility enhancements allowed Network Operations to meet their targets for reliable business application performance and reduced downtime instances.

Leading Utility Company Improves Service Edge Visibility With NETSCOUT

Given the expanse of this Energy company's technology footprint – as well as wanting to realize business goals focused on reducing operating expenses (OpEx) and improving service quality – executive leadership had outsourced select IT operations to industry third parties, including corporate network oversight. In providing these corporate network oversight services, the third-party provider hosted business service platforms at two data center locations.

Over time, IT operations leadership saw how service edge visibility gaps in the third-party IT environment created issues in assuring utility company's corporate network operations. When an operations issue traversed to the corporate network, the third-party IT team experienced challenges and lengthy delays trying to identify root cause.

Using NETSCOUT-recommended practices, the third-party IT team deployed software-based ISNG data sources to reduce visibility gaps in the following domains:

- **Service edge:** Including on-premises data center edges, including core and distribution layers (i.e., down from the service edge); capturing at firewalls (i.e., close to the service edge); and three internet service providers (including QSatellite services specific to the energy industry).
- **Client edge:** Traffic from hundreds of remote business offices routed through dozens of hub sites.

Visibility enhancements in their DMZ allowed IT Operations to meet their targets for improved service reliability, reliable business application performance, and reduced downtime instances.

Maximizing Service Edge Monitoring across Multi-National Operations

Business expansion and remote workforce transitions had combined to create service edge visibility gaps that this financial services' IT team had to reconcile to return business service reliability to thousands of investment professionals distributed across a vast WFH geography. These service edges included:

- **Client edges** – Where expanded VPN and Citrix VDI deployments supported thousands of financial services professionals who had moved from corporate facilities to WFH environments. IT had earlier configured these VPN and VDI deployments in the pre-pandemic timeframe, when the remote worker base was not as large and dynamic as their current-day WFH population. As a result, even veteran IT professionals experienced difficulties in both visualizing this client edge and assuring high-quality end-user experience in WFH environments.
- **Network edges** – Which had expanded to include a corporate network added through an acquisition that needed to be merged with the company's infrastructure. Of additional relevance, users at one remote financial office had engaged Help Desk resources about sluggish application performance at this on-premises facility. Further, IT had added on-premises Wi-Fi network segments at other corporate facilities during the remote workforce transition that had not been performance-tested. Absent visibility and load testing, there were concerns regarding how well the enhanced Wi-Fi network would perform when employees returned to corporate offices.
- **Data center service edges** – Which included an expanding mix of Equinix Co-lo facilities and an evolving on-premises operation.

When it came time to address these challenges, IT leadership looked to a familiar business partner to assist them — NETSCOUT. As part of expanding this long-time relationship to address new business demands, NETSCOUT representatives and IT leadership focused their dialog on identifying company remote locations that were perhaps deficient in network bandwidth and application visibility. Using this approach, to a large degree, the IT leadership team was able to leverage already-deployed NETSCOUT investments to address service edge visibility and end-user experience issues, as well as iteratively add ISNG smart visibility instrumentation and nGeniusONE licensing to address the application performance concerns that had emerged in one remote office.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

EFS_022_EN-2103 12/2021