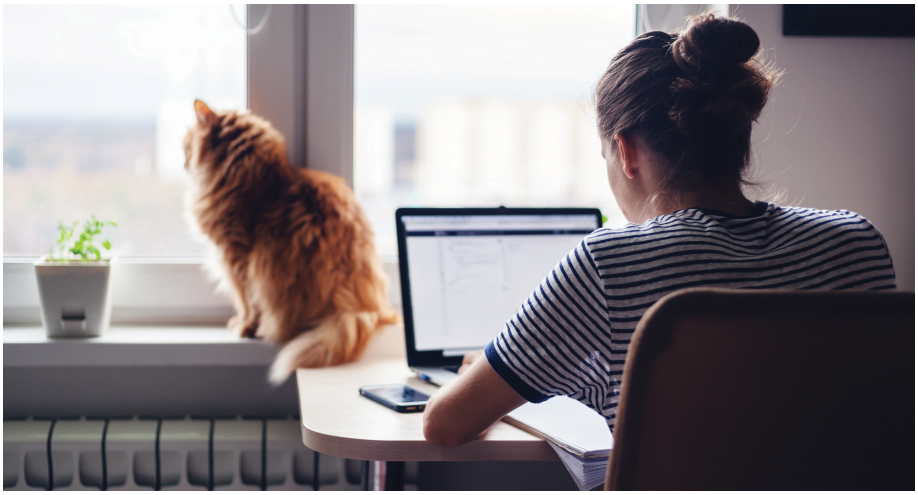
Visibility for Protecting Performance and Availability of Distance Learning Applications



Universities and K-12 educational institutions have been developing on-line and remote learning content for many years. This content can be accessed by large numbers of students using a variety of home-based devices and represents educational opportunities that, for large segments of students, would be unavailable for in-person access. With the advent of the recent worldwide health crisis, even students who typically take in-person university courses now require remote, secure access and distance learning (i.e., "flipped classroom") resources. This means:

- Commercially available distance learning platforms must scale as never before.
- With wider distribution, the security of remote access must be maintained and even enhanced.
- Visibility into the performance of multiple applications used to present course material must be provided to ensure connectivity and responsiveness.

In the last two decades, universities and colleges have evolved their distance learning and remote learning offerings from Open On-line Courses (MOOCs) to paid courses that offer as close to an "On campus" experience as possible.

At the same time these distance learning systems have evolved in complexity – no longer consisting of a single application or Learning Management System (LMS), but now have become multi-platform systems providing on-line students a richer set of resources than ever before.

Whether these services are offered from on-campus data centers, co-location facilities, or cloud implementations, a "gap" can develop, limiting IT's visibility between the edge of the infrastructure under institutional control and the remote user. This visibility gap can severely impact the NetOps and SecOps teams' ability to troubleshoot the network or the applications being employed. Issues such as poor audio or video quality, denial of VPN access, connections dropping, and applications freezing can arise. This can leave institutions vulnerable to performance-crippling interruptions in individual courses or even entire remote learning platforms. In addition to the obvious mitigation costs, there is a longer-term economic impact whenever an educational institution's reputation is impacted. With the prevalence of social media, any downfall in the delivery of distance learning can immediately be amplified to a level that impacts how many remote students sign up for digitally delivered courses or even applications for admission.

Our Approach

Even the best-designed information systems for remote access will likely have performance issues when the number of users has a period of extremely fast growth. In addition, the troubleshooting and performance monitoring challenges have increased and will continue to do so, as specialized applications are added to supplement the main LMS that an institution selects.

NETSCOUT® Smart Visibility provides the ability to examine traffic in your data center, at the co-lo, in the cloud, and all the way to the remote student's device.

Using packet-based traffic, NETSCOUT's patented Adaptive Service Intelligence (ASI) technology provides the most robust data sources available to ensure services are delivered by measuring the actual transactions and dependencies of the service.

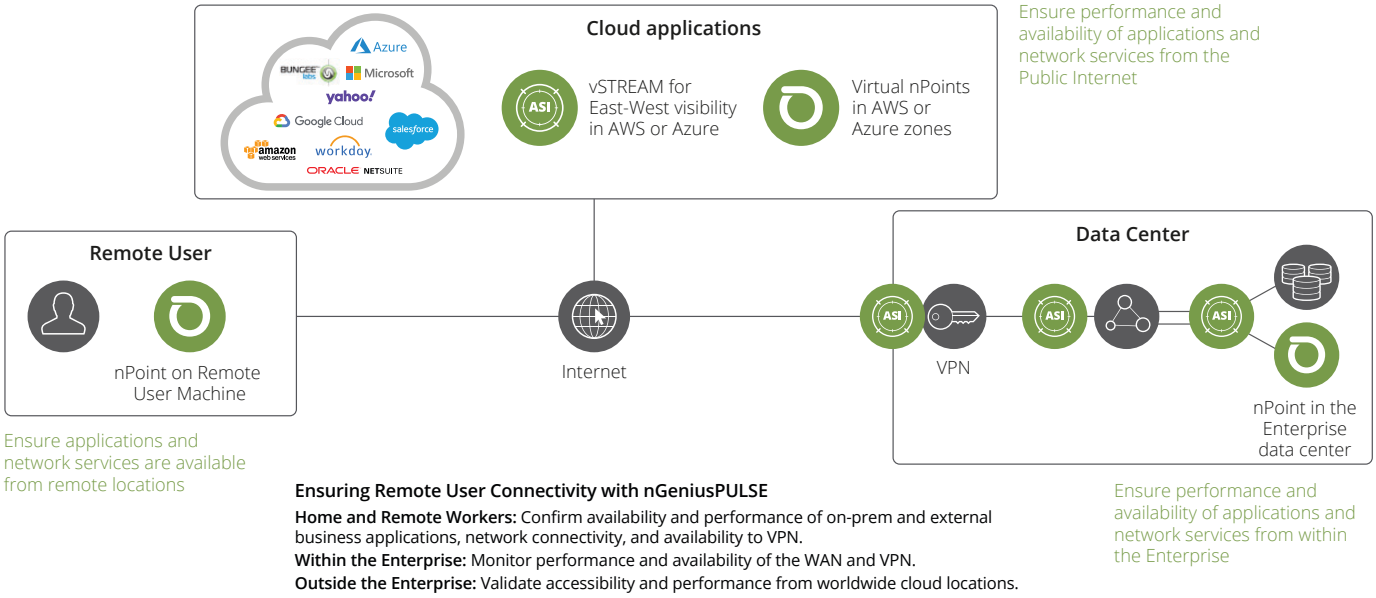


Figure 1: NETSCOUT provides visibility all the way from the Data Center or Cloud implementation to the remote user, including the remote user's device if required.

NETSCOUT analytics are the industry-leading standard for scalability and ease-of-use, enabling proactive service triage to keep all aspects of distance learning running smoothly end-to-end. Leveraging Adaptive Service Intelligence™ (ASI), the nGeniusONE® Service Assurance platform informs IT teams, often, even before user experience degrades. The NETSCOUT Arbor Edge Defense (AED), an in-line solution for DDoS attacks, is instrumental in protecting network and services availability.

With these elements in place, even today's complicated on-line learning environments can be monitored continuously and diagnosed quickly when scaling or availability issues arise.

Our Solutions

NETSCOUT solutions allow system administrators to determine the exact location of network delays, across the complex chain of application servers, platforms, clouds, internet service providers (ISPs), carrier links, and ingress routers for clouds. This capability extends all the way through the LAN to the widely varying home or remote devices that students may be using.

Rapid, focused investigation can determine whether the issue is an application availability, performance, or security problem.

The metadata gathered about the network traffic, and the packet data by InfiniStreamNG® software and hardware appliances and vSTREAM™ virtual appliances, are interpreted by NETSCOUT's nGeniusONE performance analytics. In this manner, the nGeniusONE platform continuously monitors the institution's distance learning systems and provides a wide variety of performance data about them. The nGeniusONE solution:

- Provides user-configurable, extremely flexible service alerts when performance drops below acceptable parameters.
- Monitors and helps IT teams troubleshoot the main learning applications, also monitoring network services (e.g., DNS, Email, file and print services), VPN services, LAN/WAN, and VoIP services that students depend on.
- nGeniusONE has direct drilldown capability, so it's easy to see exactly where a problem is and assign the appropriate resources necessary for resolution.
- nGeniusONE's ASI technology provides unique capabilities to track application performance across private and public cloud environments to determine exactly where performance bottlenecks may be emerging, if it is determined that the current issue resides inside an application, not in the infrastructure.

These troubleshooting capabilities are available whether applications are being hosted on premises or in a variety of multi-cloud environments, with NETSCOUT InfiniStreamNG (ISNG) appliances and vSTREAM virtual appliances providing ASI-generated smart data used by nGeniusONE to monitor these platforms.

In complementing nGeniusONE, nGenius®PULSE provides valuable visibility to close the "gap" in monitoring of remote users and assuring service availability and performance for students. Continuous synthetic tests that simulate user actions, can run 24X7 to identify potential network and application availability and performance issues before users are impacted.

For the Wi-Fi environment, nGeniusPULSE and nPoint 3000 support advanced service testing over Wi-Fi and Ethernet connections, providing IT teams a way to compare the trended results for fault isolation and determine if any service impact is, or is not, due to Wi-Fi. nGeniusPULSE synthetic tests can also measure the difference in latency over Wi-Fi and Ethernet on the same nPoint 3000. These tests will help identify the cause of the issue as the Wi-Fi network, the application, a device, or the wired network. This is a good option either on campus when communities of users in dorms or classroom buildings may experience issues with application performance or for professors teaching from home who experience quality issues between their device and campus data center.

Modern-day DDoS attacks are a dynamic combination of volumetric, TCP state exhaustion and / or application-layer attack vectors. The NETSCOUT solution in this area for enterprises is Arbor Edge Defense (AED), which provides:

- Always-on, in-line, detection and mitigation of DDoS attacks ranging from sub-100 Mbps to 50 Gbps.
- Ability to stop inbound and outbound DDoS attacks, malware, and C2 communications.

Our Value to Institutions Offering Distance Learning

- **Complete visibility across the network to remote learners** – We provide visibility of digital services at unparalleled resolution, scale, and speed to prevent or resolve the most challenging performance and security problems faced by providers of distance learning across a wide range of technologies. There is no "gap" in monitoring of remote student traffic.
- **Performance Monitoring** – nGeniusONE is already programmed to closely monitor hundreds of widely used applications and has capabilities for IT users to quickly and easily construct service monitors for custom applications. nGeniusONE can monitor all the applications involved in your distance learning platform.
- **Monitoring of other network services and applications** – which the distance learning platform depends on (e.g., DNS, email, VPN and VOIP).
- **Arbor Cybersecurity solutions** – include industry-leading mitigation of DDoS attacks, whether they are huge volumetric attacks that are best-defended against using massive on-line assets, or low & slow attacks which are best focused on by local appliances. Our Cybersecurity solutions can be integrated with existing security stacks.
- **Availability of VPNs is protected** – with visibility into Volumetric DDoS Attacks, TCP State-Exhaustion DDoS Attacks, and Application Layer DDoS Attacks.

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_018_EN-2001 07/2020