NETSCOUT Core Capabilities and Key Products

COMPANY OVERVIEW

NETSCOUT assures digital business services against disruptions in availability, performance, and security that can affect the user experience or threaten mission success. We have been serving the needs of government agencies of all types for more than 35 years. Our federal customers include civilian, intelligence and Department of Defense agencies.

CORE CAPABILITIES

Cybersecurity: DDoS Protection and Cyber Threat Analytics
Computer networks continue to be targeted for cyberattacks, even more aggressively during the COVID-19 pandemic, that are aimed at disrupting, damaging, or otherwise destroying an organization's ability to conduct its business or gaining unauthorized access to agency applications and stealing valuable information. We provide a range of network security solutions that enable organizations the ability to protect their networks from high-volume and application-specific DDoS attacks, which

are aimed at either overwhelming the network with traffic or over-exercising specific functions or features of a website with the intention to disable those functions or features. We have also developed new cybersecurity solutions that provide greater deep-dive forensic capabilities as well as analytics that can provide visibility into anomalous behavior on the network that may be indicative of an advanced threat. These security analytics enable existing customers to leverage their historical investments in NETSCOUT's service assurance solutions by using the Adaptive Service Intelligence (ASI) data already being generated to support service assurance as well as cybersecurity use cases.

Network Performance Management
Our solutions provide the necessary insight to optimize network performance, restore service and understand the quality of the users' experience. By integrating certain acquired product lines and product features into our core offerings, our customers can benefit from a consistent view across their traditional wired network infrastructures, remote offices, and wireless networks (Wi-Fi).

Application Performance Management: Data Center Transformation and Cloud Computing
We enable IT organizations, from their development operations to their infrastructure teams, to manage the delivery of services across virtual and physical environments, providing a comprehensive, unified real-time view into network, application, server, and user communities' performance. We proactively detect emerging issues with the ability to help analyze both physical and virtual service delivery environments within the data center which enables organizations to optimize data center infrastructure investments, protect against service degradations, and

simplify the operation of complex, multi-tier application environments in consolidated, state-of-the-art data centers. Our solutions are often used to support private cloud computing environments that are aimed at enabling greater, more cost-effective accessibility to applications without compromising the reliability and security of those applications and the network. Our solutions portfolio also includes a range of virtual appliances that can help customers extend their monitoring of applications deeper into their traditional data centers, confidently migrate applications into public cloud environments and gain a comprehensive, cohesive view into the resulting hybrid cloud environment.

Application and Desktop Virtualization
We provide clear and actionable insights that help customers fully realize the operational benefits associated with Application and Desktop Virtualization and reduce the time it takes to identify and resolve service problems. We offer visibility across all virtual desktop infrastructure (VDI) tiers including remote access, client, virtualization, web, front-end application, and related database systems, and help customers gain actionable metrics and insight from monitoring and analyzing the consumption and performance of VDI services

Key Products

Since our founding in 1984, we have been an industry innovator in using IP-based network traffic to help organizations manage and optimize the delivery of services and applications over their networks, improve the end-user experience and protect networks from unwanted cybersecurity threats. As mentioned previously, we use our patented ASI technology to instantaneously convert wire data, into high-value metadata, or Smart Data. In recent years, to further elevate our value proposition and address the near and long-term needs of customers and prospects, we have delivered major product upgrades across our product lines by integrating key functionality from acquired product lines, increasing the deployment flexibility of our solutions, and adding new features and capabilities that enable us to address a broader range of use cases. Our key product families are listed next.

nGeniusONE® Management Software and Analytic Modules

Our nGeniusONE management software is used to support our service provider, enterprise, and government customers enabling them to predict, pre-empt, and resolve network and service delivery problems while facilitating the optimization and capacity planning of their network infrastructures. Additionally, we market a range of specialized platforms and analytic modules that can enable our customers to analyze and troubleshoot traffic in radio access network and Wi-Fi networks, as well as gain timely insight into high-value services, applications, and systems, and better understand the subscriber's experience on the network. nGeniusPULSE is an active testing tool that enables enterprises to identify infrastructure performance issues and determine application availability, reliability, and performance.

We also market our nGenius® Business Analytics solution, which enables service providers to quickly and efficiently analyze their network traffic to gain greater and more timely insights into their subscribers, services, networks, and applications, as well as easily export our smart data into their data lakes and into third-party analytic platforms.

Visibility Products (Probes, Packet Flow Systems and Taps)

Our InfiniStreamNG™ platform provides real-time collection and analysis of information-rich, high-volume packet-flow data from across the network that is displayed through the nGeniusONE Service Assurance Solution. The InfiniStreamNG is an advanced passive network probe that can be deployed as a traditional appliance with integrated hardware and software, as software-only for use in commercial-off-the-shelf hardware or in virtualized or software only form factors. The virtualized form factor version of our intelligent data source, which is marketed as vSTREAM™, can be deployed to support NFV environments as well as to cost-effectively monitor application performance in traditional data center, private cloud, and public cloud environments.

We also provide comprehensive packet flow systems under nGenius® Packet Flow Switches family, that deliver targeted network traffic access to a range of monitoring and cybersecurity tools and systems, including the nGeniusONE Service Assurance platform. Additionally, we market a suite of test access points (TAPs) that enable full, nondisruptive access to network traffic with multiple link type and speed options.

DDoS Protection

We provide cybersecurity solutions that enable service providers, enterprises and government agencies to protect their networks against DDoS attacks. Dozens of service provider customers around the world also resell these solutions as a managed DDoS service to their enterprise customers. Our portfolio of DDoS solutions offers complete deployment flexibility spanning on-premise offerings and cloud-based capabilities to meet a broad array of customer needs, as well as specialized analytics and comprehensive threat intelligence information. Our smart DDoS offerings for service providers include NETSCOUT® Arbor Sightline with Insight™ for DDoS visibility, threat detection, and advanced analytical and forensic information, and NETSCOUT® Arbor Threat Mitigation System™ for removing DDoS attack traffic from the network without disruption to key network services.

Our smart DDoS offerings for enterprises and government agencies include NETSCOUT® Arbor Edge Defense™, a perimeter-based appliance for identifying and blocking incoming DDoS attacks and outbound malicious communications, and NETSCOUT® Arbor Cloud®, a global, cloud-based traffic scrubbing service that quickly removes DDoS attack traffic. We plan to further enhance and expand these capabilities in ways that will enable greater adoption of our solutions by service provider, enterprise and government customers.

Advanced Threat Detection

We are actively expanding our enterprise cybersecurity offerings to better leverage the investment that our customers have made in our traditional service assurance solutions. By collecting network traffic via our probes, we can expand our value proposition by providing specialized analytics for both service assurance and security. We have introduced and will continue to advance solutions such as new packet forensic capabilities, Omnis® Cyber Intelligence, designed specifically for security operations teams as well as new anomalous behavior analytics that security teams can use to identify and investigate potential advanced network threats.

USE CASE

Omnis Cyber Intelligence Increases Network Visibility and Improves Threat Hunting Maturity Model

Company Background

This government agency has thousands of employees and supports millions of customers each year in multiple functions.

OVERVIEW

The Challenge

- Company had visibility gaps in the network and cloud
- Security Operations Center (SOC) Maturity Model for Threat Hunting was underdeveloped
- Not using previous Omnis® Cyber Intelligence (OCI) purchase and packet metadata to its full potential

The Solution

- Knowledge transfer to improve SOC analysts threat hunting capabilities and get more value out of original purchase
- Adding additional Cyber Adaptors to gain a more comprehensive visibility of their attack surface
- OCI bootcamps for ongoing SOC Analyst development

The Results

- Better visibility into their network and understanding of existing infrastructure
- Discovered Log4j vulnerability during onboarding and applied immediate remediation
- NETSCOUT® is a trusted advisor and continuously provides key insights into their visibility and threat hunting challenges
- OCI was able make their existing security technology stack stronger with easy integration and higher quality data