NETSCOUT Broke Down IT Silos, Reducing MTTK and MTTR from Days to Minutes using Splunk and ServiceNow for AIOps

Powered by NETSCOUT Real-Time Contextual Intelligence

Executive Summary

NETSCOUT's multiple business acquisitions introduced many exciting growth opportunities for the company as well as some challenges—chief among them, a substantial technology debt due to the scale and legacy infrastructure inherited. These acquisitions added a fragmented and aging IT environment, including:

- 30+ branch offices, each with unique hardware-based infrastructures
- 150–160 hardware devices across 30 locations
- An MPLS WAN
- 600+ servers distributed across five VMware clusters
- Four corporate data centers
- Ten distinct storage platforms in eight locations
- Five separate backup and recovery platforms

This patchwork of legacy systems placed a considerable burden on NETSCOUT's IT department, complicating management, maintenance, and troubleshooting efforts.

To improve the digital experience for both employees and customers, the IT team launched a digital transformation initiative, aiming to modernize infrastructure and transition toward an AIOps-driven architecture. Key goals included consolidating physical assets, streamlining operations, and eliminating fragmented tools and dashboards.This patchwork of legacy systems placed a considerable burden on NETSCOUT's IT department, complicating management, maintenance, and troubleshooting efforts.

To improve the digital experience for both employees and customers, the IT team launched a digital transformation initiative, aiming to modernize infrastructure and transition toward an AIOps-driven architecture. Key goals included consolidating physical assets, streamlining operations, and eliminating fragmented tools and dashboards.

Problem Statement

Following the acquisitions mentioned above, data was scattered across siloed environments, and IT teams were overwhelmed by the sheer number of systems involved in resolving issues. For example, troubleshooting an Oracle-related problem required interfacing with multiple tools—each owned by a different team. This often led to six to eight people across three or four teams joining a two-plus-hour long troubleshooting calls, consuming up to 16+ man-hours just to identify a single root cause.

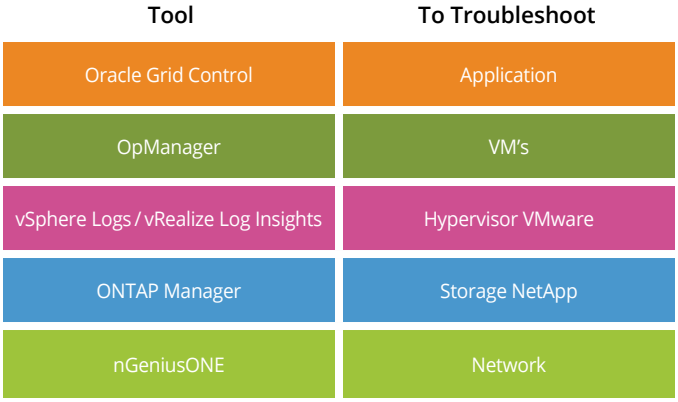

Figure 1: Legacy Data Silos & Tool Teams.

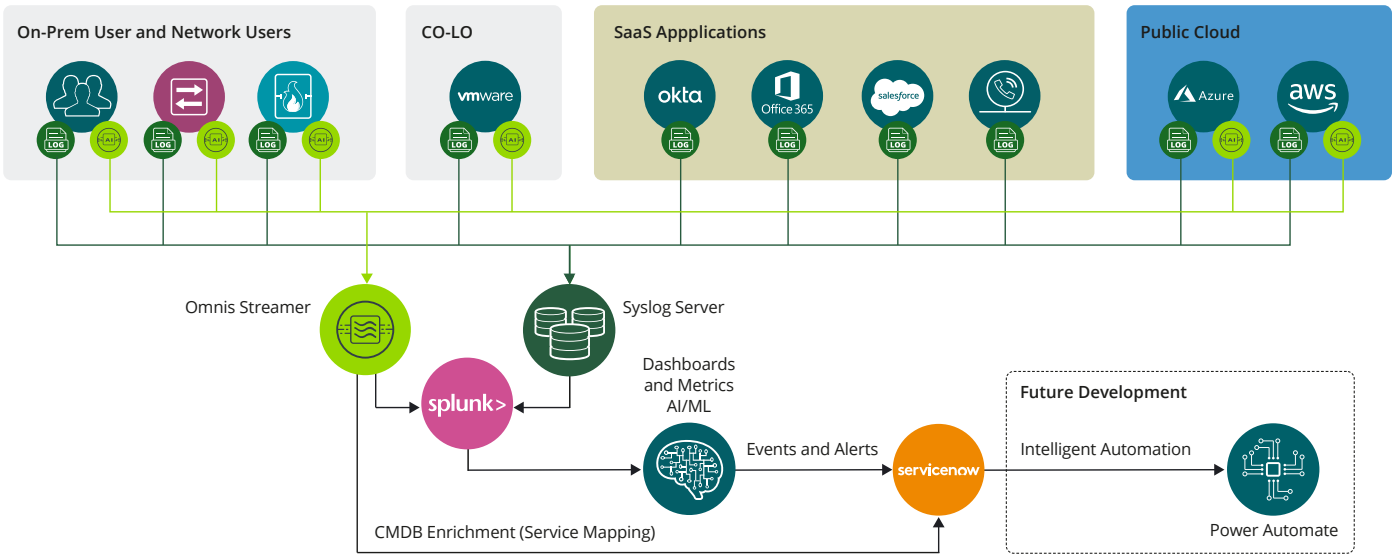

Figure 2: New Unified AIOps Frameworks.

Problem Resolution

To help address these issues, and to streamline the entire IT management process flow, NETSCOUT's IT team incorporated NETSCOUT's Omnis™ AI Insights product with Splunk's IT Service Intelligence (ITSI) and ServiceNow.

By leveraging Splunk ITSI, the IT team developed insightful dashboards that deliver unified visibility across the entire IT infrastructure—eliminating the complexity of managing multiple standalone monitoring and troubleshooting tools. While logs and event data from various disparate sources feed into Splunk, NETSCOUT's Omnis Streamer provides critical context and correlation, transforming otherwise isolated data points into actionable insights. Acting as the connective tissue between fragmented signals, AI Streamer significantly accelerates Mean-Time-to-Know (MTTK). Correlation searches within Splunk then trigger meaningful event alerts, which are automatically routed to ServiceNow ITSM for ticket creation and assignment to the appropriate teams—streamlining issue resolution and response.

Using the earlier Oracle example, when users reported that the application was slow, the Oracle team might observe that CPU utilization had spiked to 85%. However, this data alone provided little insight into the root cause of the performance issue. Resolving the true root cause typically required multiple teams to investigate further. By adopting a new approach that integrates NETSCOUT's Omnis Streamer data with logs, metrics, and events from other various complementary tools—such as Splunk's Universal Forwarder—into a centralized Splunk dashboard, the team was able to correlate key indicators. The dashboard revealed that the 85% CPU utilization coincided with a significant increase in server response time to 230ms and a connection count spike to 5,000 at the same time, providing immediate, actionable context and accelerating root cause identification.

By leveraging Splunk ITSI to correlate data across multiple systems, enhanced by NETSCOUT's Omnis Streamer to provide critical context, the IT team was able to pinpoint multiple areas of concern in real time and present clear evidence of what was impacted and when. This analysis revealed that a rogue database backup was the root cause of the Oracle performance issue, as it was triggering during peak hours and placing significant strain on the infrastructure. Once identified, Splunk automatically forwarded the correlated events to ServiceNow, generating targeted tickets for the appropriate teams. This automation enabled rapid resolution without consuming days of manual effort.

Figure 3: NETSCOUT's Real-Time Intelligence - Bringing Context and Relevance to Traditional Data Sources in Splunk.

This automated consolidation and correlation drastically reduces the time required to identify issues, pinpoint root causes, and determine resolution steps—from days of manual effort to just minutes. This substantial improvement in both Mean-Time-to-Know (MTTK) and Mean-Time-to-Resolution (MTTR) not only conserves valuable IT resources but also ensures a consistently positive user experience.

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

EUC_073_EN-2601 03/2026