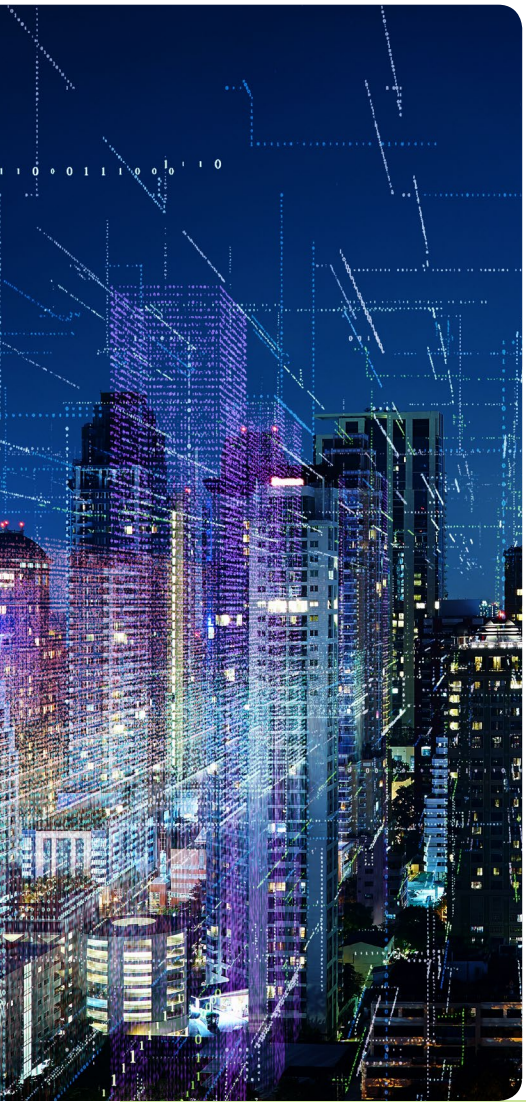
NETSCOUT®

CIO FROM IDG

Smart Data: Maximum Visibility Minimizes Risk and Drives Digital Transformation

Ensuring high-fidelity visibility into network communications is critical to ensuring efficient operations and optimal security.



The modern enterprise is dealing with more data than ever, and maintaining a high level of visibility into that data is critical to ensure optimal security and efficient operations. Application performance and security threat information is coming from data centers, multiple private and public clouds, and third-party networks and systems. With all this disparate technology, the one constant is the communications between applications and infrastructure.

Achieving full visibility into these communications can help accelerate an organization's digital transformation while continuing to provide exceptional user experience for business applications and services. "The digital transformation is about gaining better access to customers, serving them well, and driving profitability," says Suresh Tatavarthy, principal product manager at NetScout. "Organizations have to make better use of their assets and quickly fix problems as they arise, so IT needs full end-to-end visibility."

With this advanced level of visibility, IT is empowered to identify and mitigate critical errors, latencies, and security problems. It's essential to extract the most-critical information across various platforms and locations. Extracting, analyzing, and presenting the data provides IT with the key metrics it needs in real time.

"It can often be difficult to discern from a security or network problem at first blush," says Russ Currie, vice president of enterprise

strategy at NetScout. "We get the right information to the right person at the right time for network ops and security ops. We transform packet data in a consistent manner, regardless of how it's collected. And we present that view in a single pane of glass across any deployment model."

And the data packets themselves remain pure, to preserve contextual detail. "We don't abstract that information. We use that to derive intelligence. Our architecture listens directly to wire traffic," says Currie. "It takes packets to analyze in real time, and with that analysis, we surface metadata and apply key performance indicators."

This intense level of packet inspection can provide an early warning into any errors, latencies, or threats with pinpoint precision before they can cause damage or downtime. "When we detect something out of band, we can act on that in real time. The packet is that single source of the truth, the one thing that doesn't change," he says. "And the movement of that traffic contains the raw information that tells us what the attacker is doing."

Data Deluge

Most enterprises these days are managing diverse environments comprising disparate but interdependent collections of compute, network, and storage components working across a variety of interconnected hybrid cloud environments. Getting a handle on this diversity is an ongoing challenge. These myriad networks located across multiple silos of emerging multicloud and hybrid cloud platforms must all seamlessly integrate.

NetScout listens to all communications between the applications and creates valuable information about application performance and security. It can then apply that to critical use cases—improving business operations, security, and application performance. "Detailed transaction and conversational data is necessary to collect evidence and take decisive action to fix service delivery issues, empowering IT operation teams to react to both service assurance problems and security threats," says Tatavarthy.

NetScout extracts data on performance and security threats from the network packets as they move throughout these diverse networks. Only the most critical information is extracted across the entire environment. As a result, IT organizations can get a real-time view into service assurance and cyberthreats while safeguarding data privacy. NetScout refers to this highly versatile visibility

> "We don't abstract that information. We use that to derive intelligence. Our architecture listens directly to wire traffic."

into performance and security threats as Smart Data.
What benefits does this Smart Data offer?

- Advanced data analytics rely on actionable data already set into context to streamline operations and business performance
- Quality business insight—structured, contextually-oriented data to help inform better decision-making between IT and security teams
- Seamless collaboration and operational efficiency across IT operations, including DevOps and SecOps

"We leverage packet collection technology and collect data everywhere in a cost-effective and pervasive way. We collect right at the source and then organize and automate that process so key metrics are available to IT teams in real time. They have access to the level of analytics they need," says Arabella Hallawell, senior director at NetScout. "As soon as they see a problem, they can go right to the source and see what happened and where and why it happened and can get the right information to the right people at the right time and troubleshoot service problems more effectively."

That packet inspection is executed through a scalable, lightweight, distributed architecture. Collecting and processing data at the source and applying intelligent automation for precise, real-time knowledge is the true differentiator in gaining timely insights for optimizing digital services.

Smart Data is the reliable signal in the noise of all the traffic moving through aggregated data streams. One thing is certain in such complex environments: constant or near-constant communication between applications. This steady stream of data feeds applications and helps them function properly. Smart Data consistently converts that raw wire data into actionable information to better inform IT and security teams.

And having that actionable information presented as a single pane of glass greatly simplifies operations. "Having too many monitoring tools results in higher-cost overhead; management complexity; personnel cost for different people managing a different tool set; and unmanaged alerts and alarms, which make problems difficult to find.
It becomes a needle-in-a-

"We collect right at the source and then organize and automate that process so key metrics are available to IT teams in real time."

haystack situation," says Tatavarthy. "You need a centralized monitoring solution that provides visibility across all the parts of the IT environment: from desktops to servers, network infrastructure, application components, and network storage."

Complete Visibility

The modern enterprise continues to redefine the requirements for visibility as networks span remote locations, multiple cloud platforms, and modern application architectures. Visibility Without Borders is the goal for organizations striving to operate efficiently in a fluid cloud-based architecture while managing the massive data influx. This refers to the full depth and breadth of visibility across remote locations, different cloud services, new application architectures, multiple cloud platforms, and data traffic going back and forth between them to all endpoints.

Visibility Without Borders is about maintaining a simplified yet meaningful level of understanding of the communications between service and infrastructure, regardless of physical location. Relatively few organizations have the competence or efficiency to handle the data they need in order to operate, maintain, secure, and upgrade their digital infrastructures at scale. A lack of visibility significantly increases the business risk.

A high level of visibility can help modern enterprises anticipate and avoid negative business outcomes through views into application performance and critical dependencies, user experience, and potential threats. Enterprise IT and security teams can then:

- Monitor activity levels to stay ahead of any potential issues that may impact performance
- Proactively detect and mitigate any inbound threats
- Perform advanced data analytics
- Fully understand service interdependencies and their interaction
- Make timely and better-informed business decisions about security, capacity planning, application, and service usage trends
- Leverage global threat intelligence to stay ahead of advanced threats
- Save significant time by eliminating manual updates

The Long View

"Today's world is a ready, fire, aim world," says Currie. "Things are moving so fast. Everyone is talking about visibility, but the question is, 'What level of visibility is sufficient?' You've got to have that high-fidelity visibility."

Visibility Without Borders provides a deep understanding and comprehensive monitoring of all applications and services and their dependencies. It helps enterprises distill issues in real time, regardless of the type of cloud platform or service architecture. This level of seamless data visibility is fundamental to driving the digital transformation for the world's largest companies and government agencies.