New Digital Architectures Require an Innovative Approach to Service Assurance

Business Results Depend on Improved Visibility into Complex, Hybrid Cloud Infrastructures

by Joe Weinman

Author, *Cloudonomics* and *Digital Disciplines*,
Principal, XFORMA LLC

Joe Weinman is a frequent global keynoter and the author of *Cloudonomics: The Business Value of Cloud Computing* (Wiley, 2012), *Digital Disciplines: Attaining Market Leadership via the Cloud, Big Data, Social, Mobile, and the Internet of Things* (Wiley CIO, 2015), both available in Chinese editions, and co-editor of the forthcoming *Fog and Fogonomics: Challenges and Practices of Fog Computing, Communications, Networking, Strategy, and Economics* (Wiley, 2018). He is also the Cloud Economics contributing editor of *IEEE Cloud Computing* magazine, and has written scores of articles for Forbes, InformationWeek, CIO and other print and online publications, as well as contributed chapters to textbooks published by the MIT Press, Springer, and CRC Press.

He has held a variety of executive leadership positions at Bell Labs, AT&T, HP, and Telx. He also serves on the advisory boards of a global non-profit and several technology companies.

Weinman has a BS in Computer Science from Cornell University, an MS in Computer Science from the University of Wisconsin-Madison, and has completed executive education at the International Institute for Management Development in Lausanne. He has been awarded 23 patents in cloud and distributed computing, applications, encryption, networking, and data communications protocols.

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) assures digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility, and insights customers need to accelerate, and secure their digital transformation. Our approach transforms the way organizations plan, deliver, integrate, test, and deploy services and applications. Our nGenius service assurance solutions provide real-time, contextual analysis of service, network, and application performance. Arbor security solutions protect against DDoS attacks that threaten availability, and advanced threats that infiltrate networks to steal critical business assets. To learn more about improving service, network, and application performance in physical or virtual data centers, or in the cloud, and how NETSCOUT's performance and security solutions, powered by service intelligence can help you move forward with confidence, visit www.netscout.com or follow @NETSCOUT and @ArborNetworks on Twitter, Facebook, or LinkedIn.

As global competition from traditional rivals and new entrants continues to intensify, businesses must deliver exceptional customer service and experiences. In an increasingly digital world, this necessitates holistic, end-to-end service assurance, i.e., monitoring, managing, and controlling the reliability, availability, performance, and security of increasingly complex, interdependent, distributed applications and services residing on an ever-growing variety of infrastructure options – such as private, public, hybrid, and multi-clouds – even as they shift and evolve at a dizzying pace.

However, this is easier said than done. IT leaders report that their three top remaining challenges include security, a lack of control over service quality and performance, and a lack of visibility throughout the service stack. Fortunately, innovative approaches to overcoming these challenges are emerging, such as the use of "smart data," i.e., efficient monitoring and correlation of the wire data, i.e., network traffic, flowing between the numerous, varied elements of today's complex digital architectures to develop actionable insights.

As customers become more knowledgeable and demanding, competition heats up, and digital architectures continue to increase in complexity, such new approaches to service assurance will help determine whether the enterprise survives, thrives, or nosedives.

Fortunately, innovative approaches to overcoming these challenges are emerging, such as the use of "smart data," i.e., efficient monitoring and correlation of the wire data, i.e., network traffic, flowing between the numerous, varied elements of today's complex digital architectures to develop actionable insights.

Key Trends and Challenges

Digital architectures are becoming exponentially more complex at an accelerating rate, due to more infrastructure options, greater resource dispersion, and finer applications granularity. To keep pace and maintain relevance, service assurance needs to span technologies, industries, and business processes, and shift from silos to a holistic, end-to-end view. Let's explore each of these factors in turn:

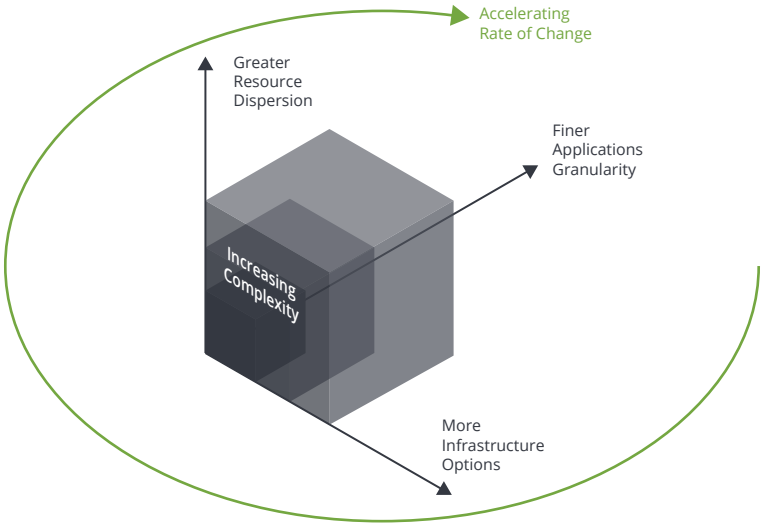

Figure 1: Strategic Scope of End-to-End Service Assurance as Complexity Increases Exponentially.

More Infrastructure Options

Most established enterprises—and even many cloud-native startups—use a heterogeneous mix of infrastructure approaches: legacy and custom systems, high-performance computing, containers, virtualization, private clouds in enterprise data centers or colocation and interconnection facilities, virtual private clouds, public clouds, hybrid clouds and multi-clouds. New options and ecosystem roles are emerging, such as federated clouds, cloud service brokers, cloud exchanges, and the Intercloud. These are being networked to each other, to an emerging fog and edge, and to mobile and fixed user devices and connected things.

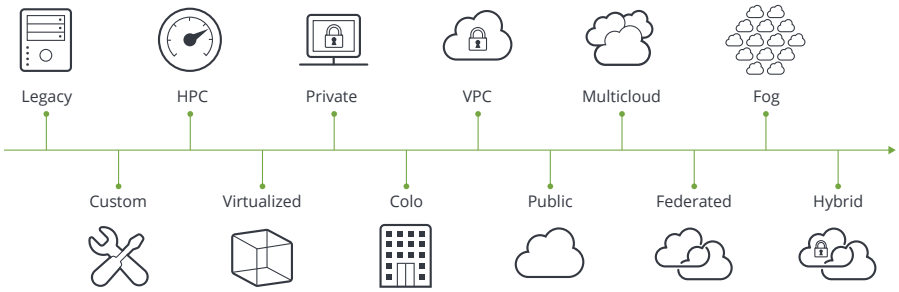

Figure 2: The Spectrum of Digital Infrastructure Options.

For example, a large global retailer uses its own private cloud running in its own data centers orchestrated together with multiple public cloud providers and in-store resources such as servers and point-of-sale devices.

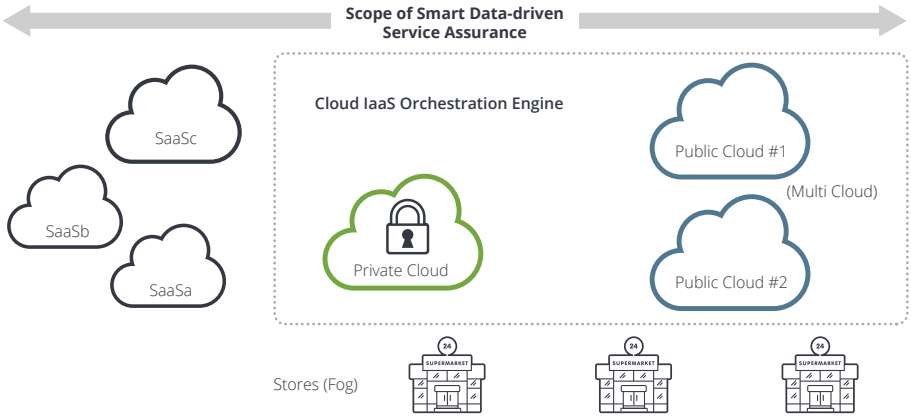

Figure 3: A Retail Example of Service Assurance Spanning a Hybrid Multicloud Fog.

There are many reasons for such a broad variety of solutions. Different enterprises are at different stages of their cloud journey. Financial returns from legacy system modernization may not justify the time and cost. Custom systems may achieve better price-performance. Public clouds may be more or less expensive than private clouds, depending on enterprise IT competence, workload variability, performance differentials, scale economies, and data gravity effects.

While a mix of infrastructure options such as found in a hybrid or multi-cloud can often best balance multiple criteria, it creates its own service assurance challenges, because the reliability and performance of such a distributed, heterogeneous system may be only as good as its weakest link, and also due to the sheer number and variety of management silos. Without a holistic, end-to-end service assurance strategy, operational problems can be more difficult to pinpoint and troubleshoot, since applications and services span silos, e.g., across public clouds and enterprise datacenters, and the root cause could be anywhere.

Without a holistic, end-to-end service assurance strategy, operational problems can be more difficult to identify and troubleshoot, since applications and services span silos, e.g., across public clouds and enterprise datacenters, and the root cause could be anywhere.

Greater Resource Dispersion

Centralized hyperscale facilities and corporate data centers are increasingly being deployed on a regional or global basis to reach geographically diverse customers, partners, employees, and suppliers. Away from the cloud, there are already billions of user devices such as desktops and smartphones, and most studies project that we will soon have tens of billions of additional Internet of Things devices such as remote surveillance cameras, smart door locks, and connected cars.

To help interconnect these devices and the cloud, an emerging fog consisting of multiple layers will contain two types of functions: those moving down from centralized cloud datacenters to be closer to the edge and reduce interaction response times; and those moving up from devices to benefit from aggregation or proximity to cloud resources such as scalable processing, very large databases, or unique functions, such as artificial intelligence / machine learning services. As a result, there may be one or more layers between the cloud and devices, engaged in functions such as control loops, data compression, and distributed query processing.

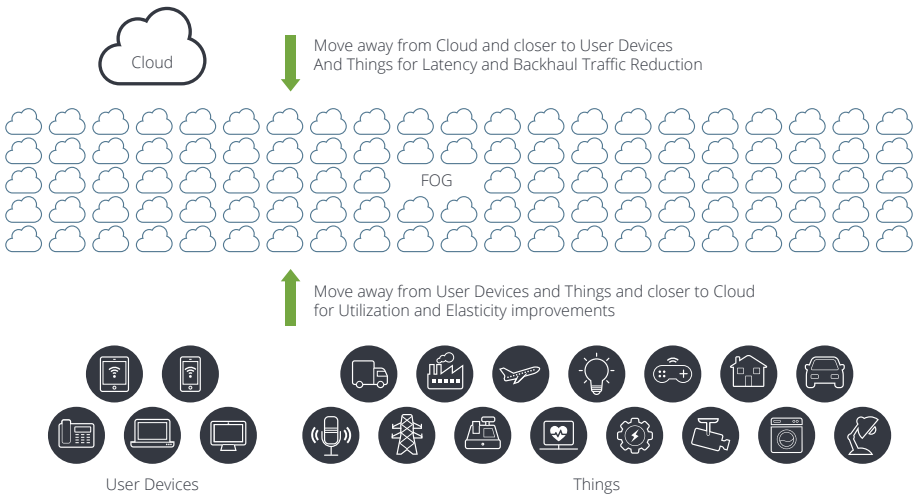

Figure 4: The Emergence of the Fog.

For example, wearable and implantable devices such as connected pacemakers can link to residential smart hubs and gateways, hospitals, physicians, electronic medical records, and emergency medical services.

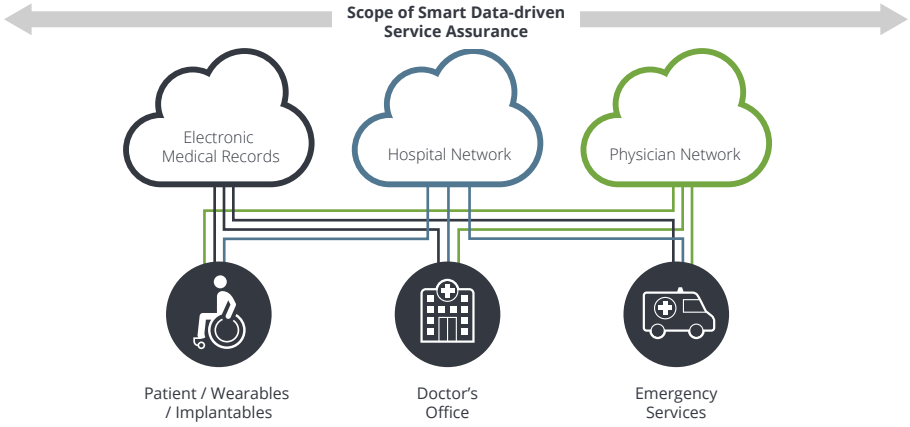

Figure 5: A Healthcare Example of Service Assurance Across Components and Ecosystems

It is an enormous challenge to securely monitor devices at scale dispersed across a regional or global footprint, because performance and availability problems may be due to a variety of permanent or transient root causes, endpoint devices may not have been designed to work together, and the trouble symptoms, the root cause, and the management tools and people may each be in widely different locations. As such, gaining an unobstructed view of the infrastructure and an understanding of the functions and behaviors of its various components are both needed to assure service delivery.

Gaining an unobstructed view of the infrastructure and an understanding of the functions and behaviors of its various components are both needed to assure service delivery.

Finer Application Granularity

Monolithic applications are being refactored into interdependent components such as services, microservices, and on-demand "serverless" cloud functions, interconnecting to ecosystems, and executing on distributed, complex environments spanning containers and physical and virtual machines. These may be implemented in enterprise, partner, or service provider data centers or as cloud functions, and may be distributed across numerous physical locations and varied elements ranging from the cloud to the edge and devices.

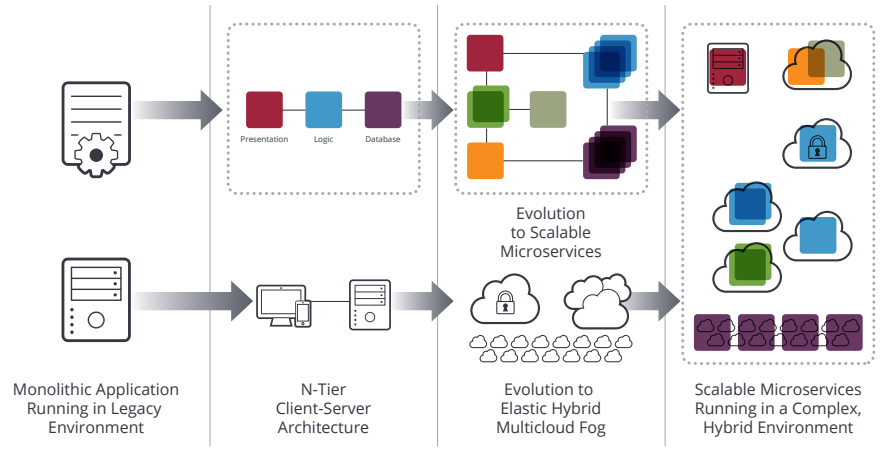

Figure 6: The Evolution to Microservices in a Complex, Hybrid Infrastructure.

For example, consider a hedge fund that uses an algorithmic trading program, itself composed of microservices, that calls a cloud-based AI engine to conduct real-time sentiment analysis on global tweets and other social media regarding a stock, then executes a buy or sell transaction on a remote exchange based on whether the sentiment is positive or not.

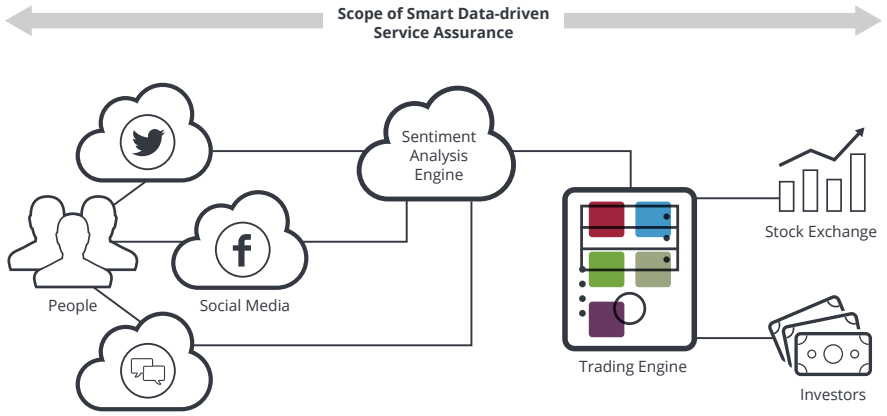

Figure 7: A Financial Example of Service Assurance across Networked (Micro-)Services.

Microservices and application ecosystem approaches have advantages around reusability, scalability, performance, cost, and time to value, but can increase complexity and the magnitude of the service assurance challenge due to the sheer number of interacting components, often running in different environments that are geographically dispersed, and at a range of layers, including not only the application layer but also lower layer services such as IP networking, directory, messaging, or queuing. A sound service assurance strategy needs to correlate these technology elements with business services and processes, workflows, and their interactions and dependencies.

Accelerating Rate Of Change

Cloud and technology providers are introducing new systems, services, technologies, and pricing at a rapid pace, even as competition intensifies, customer demands rapidly shift and evolve, and disruptive technologies emerge.

Nevertheless, responding to these discontinuities is an imperative, because digital transformation is underway in virtually every industry, as illustrated by the seismic shifts in media as print moves to online advertising; in entertainment as physical media has been replaced by streaming; in retail as ecommerce takes share from physical stores; in finance, due to cryptocurrencies; and so on.

Leading enterprises are accelerating time to market through organizational and process approaches such as DevOps, continuous delivery, and automated testing. They are engaging in digital transformation of products, processes, and infrastructure, migrating services into and out of various public clouds, or between clouds. They need the data and insight to make the right architectural choices and optimally deliver services.

Increasing Complexity

All these trends together lead to exponentially increasing complexity, expand the challenges of baselining, planning, and executing application refactoring and infrastructure modernization, evolution and migration, and exacerbate the difficulties of optimizing cost while assuring service performance and availability across a widely dispersed mix of owned resources and multiple cloud services. For example, a performance issue with a given application that impacts customer experience—such as poor response time—might be due to network congestion, a faulty directory service configuration in an enterprise data center, or a public cloud load balancing issue. How can such complex problems be surfaced, diagnosed, and remediated?

A new approach to service assurance bridges the gap between the business promise and the technical challenges of hybrid solutions

The answer to managing increasing infrastructure complexity—in hybrids of public or private, centralized or dispersed, legacy or greenfield—lies in a new, holistic, end-to-end approach to service assurance.

Service Assurance Through Smart Data

The first step is to achieve comprehensive visibility into the multiple, distributed, communicating components such as containers and microservices implemented across various infrastructure options by monitoring and analyzing wire data, the network traffic flows between components that are accessible and distilled in real-time, and drive end-to-end pervasive visibility spanning the entire enterprise. Since every action and transaction navigates the various components of digital infrastructure through traffic flows, wire data is the best source of information from which to gain actionable insight into today's complex, heterogeneous infrastructures.

Since every action and transaction navigates the various components of digital infrastructure through traffic flows, wire data is the best source of information from which to gain actionable insight into today's complex, heterogeneous infrastructures.

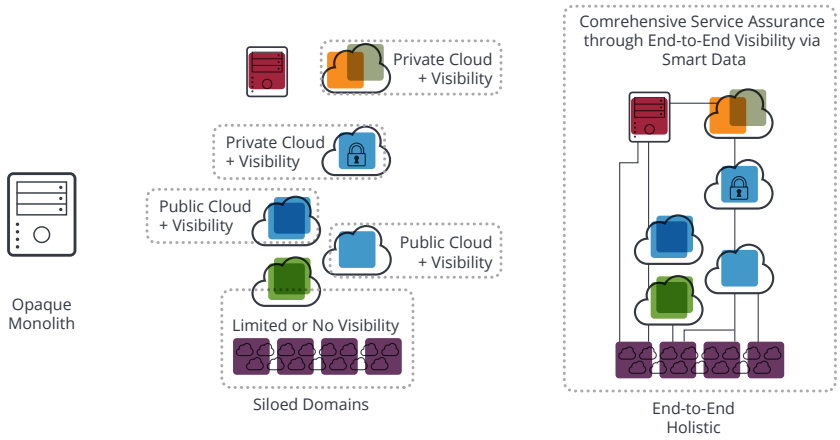

Figure 8: Evolution of Service Assurance to Smart Data.

This cost-effective approach to service assurance ensures that relevant wire data is collected, aggregated, and analyzed in real-time to generate smart data that provides critical insight into the performance, availability, and consumption of services, which is required for optimal control of service performance, all while ensuring the utmost level of security.

Ultimately, these help lead to positive business results: maximizing top-line and bottom-line business value through mechanisms such as revenue growth, enhanced customer experience and satisfaction, labor productivity improvements, and cost optimization.

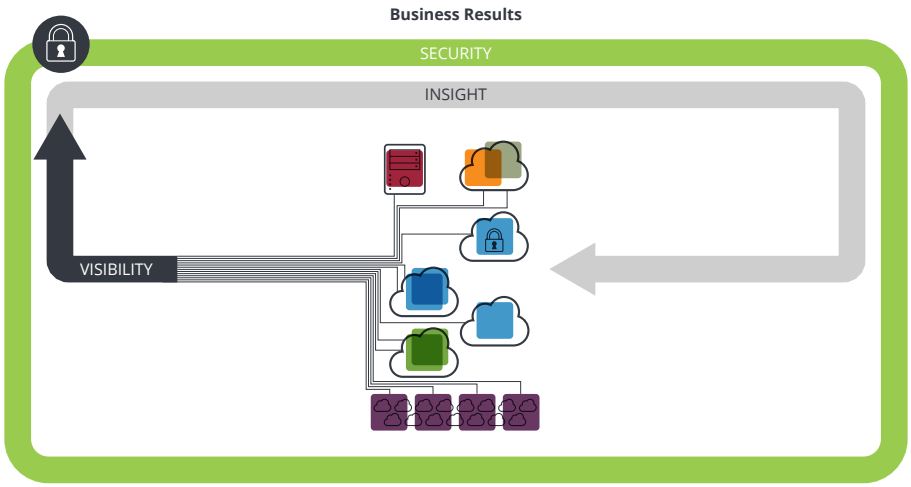

Figure 9: Securely Closing the Loop to Generate Business Results.

Business Alignment

To illustrate the linkage between business results and service assurance, consider response time.

From a business perspective, response time can dramatically impact customer, employee, partner, or end-user experience and thus either revenues or productivity. For example, faster response times for an ecommerce site mean more customers will have a better experience and view more products and more pages, including check-out, thereby boosting revenues. For internal applications, faster response times mean less idle time, boosting labor productivity and thus reducing costs.

From a technical perspective, however, response time depends on how infrastructure is architected, implemented, configured, geo-located, scaled, and operated. Are there network bottlenecks? Will the web servers scale? What about the database servers? Is QoS configured correctly?

In any event, smart data extracted from the end-to-end technical infrastructure is critical to maximizing business results, because a major systemic service performance issue may be caused by a minor fault anywhere and quickly understanding the root cause enables control of the user experience.

Digital Transformation

Digital transformation and migration to or from the public cloud is also a challenge, due to issues such as extended performance degradations, outages, or costly mistakes in cloud resource allocation exacerbated by the lack of service assurance across increasingly complex architectures and infrastructures. Enterprises need to be able to benchmark existing performance and availability levels, plan for migration, trial the new architecture, and then evaluate metrics and possibly roll back the solution.

In addition, such service assurance must be easy to use, cost-effective and optimize resource utilization, implying lower licensing or usage costs via fewer monitoring tools that are easy to set up and use. Cost effectiveness of a total solution also depends on efficiencies throughout the monitoring and management architecture. As one example, smart data collection and analysis can reduce processing, storage, and data transport costs compared to approaches that collect and transmit both relevant and irrelevant data.

Summary

The architectures enabling today's increasingly essential digital business strategies and the digital transformation to enable them are becoming exponentially more complex, requiring a new approach to service assurance.

Traditional siloed technology-oriented approaches no longer suffice for today's complex, heterogeneous infrastructures such as hybrid cloud and the distributed applications and data residing on them. Instead, business-oriented service assurance requires an end-to-end view aligned with customer and user experience, because business-critical workflows and applications now have elements bridging multiple domains, exacerbating the challenges of root cause analysis in the absence of a holistic approach.

Fortunately, a new approach to service assurance through smart data has become available that is tailored to these new digital infrastructure and applications architectures. Rather than being stymied by large numbers of heterogeneous, multilayer networked components such as found in hybrid clouds, this innovative approach intelligently exploits the wire data passed across these interconnections to provide cost effective visibility and insight into overall system performance.

Moreover, by managing and assuring a broad variety of components, it enables greater business and technology agility to support modernization, migration, and optimization initiatives to accelerate time to value in responding to changing customer demands, emerging market opportunities, or competitive threats.

Such visibility and control of the digital capabilities enabling customer experience and competitive differentiation have never been more important.

For more valuable information on Hybrid Cloud Environments, please visit NETSCOUT's Cloud Smarter page: https://www.netscout.com/cloud-smarter.

Data-driven service assurance enables greater business and technology agility through a complete understanding of dependencies and how applications work. This information supports modernization, migration, and optimization initiatives to accelerate time to value in responding to changing customer demands or competitive threats.

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

UWP_001-1801 03/2018