White Paper

Digital Transformation and the Need for Network Visibility, Application Assurance, and Performance Management

Sponsored by: NETSCOUT

Adelaide O'Brien
September 2017

IDC OPINION

IDC has observed that in just a few short decades, information technology (IT) has moved from the back office, what IDC calls the 1st Platform of mainframe computers, to the front office, the 2nd Platform of ubiquitous PCs driven by business uses and apps, and now, finally, IT has embedded itself into nearly every aspect of people's personal lives and interaction with government and business — this is enabled by what IDC describes as 3rd Platform technologies and includes mobile, social business, cloud, and big data and analytics. This IDC white paper examines the impact of the 3rd Platform and digital transformation (DX) on IT priorities for enterprise network management and focuses on a shift toward pervasive instrumentation as an enabler of better network visibility, application assurance, and security assurance. The adoption of 3rd Platform solutions will continue to drive a need for capacity, bandwidth, performance, and availability. Cloud is fundamentally changing the characteristics of resource consumption and traffic generation within network operations.

In this era of 3rd Platform, enterprise network management includes many networked resources beyond the traditional view and control of enterprise IT departments. As technology becomes an explicit component of providing mission-critical information and services, government IT priorities should include network visibility, assurance, and risk management solutions that provide real-time actionable intelligence to ensure service assurance continuity for voice, video, and data services over physical, virtual, and hybrid cloud networks.

SITUATION OVERVIEW

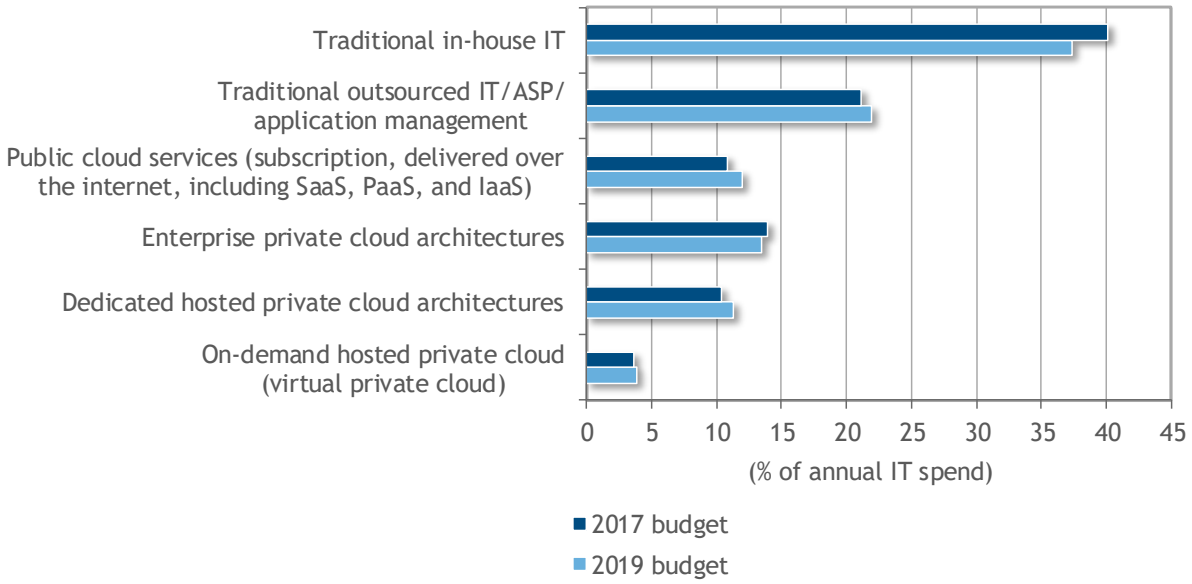
The 3rd Platform technologies of big data, mobile, and social collaboration technologies and solutions are all heavily dependent on the cloud services delivery model. In effect, these solutions can't exist without the cloud model as the underlying platform. The "innovation accelerator stage" enabled by the 3rd Platform will make cloud services much more valuable and strategic to government agencies and expand cloud demand and use cases. The expansion of the 3rd Platform's edge to multiple smart devices, including tablets, phones, and IoT, will create massive amounts of data and drive demand for cloud-based apps/solutions and back-end services. Government entities at all levels are challenged with making operations more responsive and effective. Transforming infrastructure in a way that avoids disruption to the agency enables government organizations to address their most pressing challenges while planning and preparing for future migration of workloads to cloud.

On their path of becoming cloud enabled, agencies should strategically plan for the best-fit mix of hybrid IT (i.e., traditional IT, private cloud, and public cloud), as these solutions will be utilized by agencies in the near term. IDC's March 2017 *CloudView Survey,* a global survey of 298 government decision makers at the national, regional (state), and local levels, indicates that government organizations in total are spreading their budgets into multiple IT options today and will continue this approach for the next 24 months (see Figure 1).

IDC asked survey respondents to estimate what percentage of their organization's total annual IT budget (including servers, applications, software, databases, storage products, networking, IT staff, and services) is allocated to each of the procurement/management models discussed in Figure 1 today and in the next 24 months. Agencies indicate that today traditional in-house IT makes up just over 40% of their total annual IT budget, and two years from now, traditional in-house IT will still make up over 37% of their total annual IT budget. So the change to cloud is happening, albeit rather slowly.

FIGURE 1

Government Organizations' Total Annual IT Budget Share by Procurement Model, 2017 and 2019



Source: IDC's *CloudView Survey,* 2017

As agencies transition to a hybrid IT state, they face many challenges. Cloud doesn't install and run itself. Cloud services can add tremendous value, but they require careful, thought-out, and well-executed steps including an awareness of application dependencies and the ability to ensure successful and cost-effective application rollouts and ongoing service performance. IoT increases the volume of connected devices and impacts prioritizing network operations requirements. For example, citizen devices accessing information at the network edge shift traffic from the center of the network outward to the edge inward, impacting computing and communications architectures. Many applications require consistent and low latency, especially those that generate frequent database calls or move large volumes of data. And, as the internet routes traffic on a best-effort basis, increased

packet loss and latency during periods of heavy usage and network congestion can negatively impact important traffic used by mission-critical applications. Poor network performance and application design can result in slow application response times/time-outs, frustration for users, inefficient use of bandwidth, and lost productivity.

Moving from on-premise to multiple cloud providers can cause a lack of packet-based visibility and control, with components on different platforms and disparate tools. Traditional systems and network management tools focus on monitoring the health and status of specific hardware/software components and do not provide end-to-end visibility into the performance of applications, making it difficult to pinpoint issues and resolve them.

In addition to these challenges, the increasing use of DevOps and Agile development methodologies is driving more frequent application updates and blurring the line between development, test, and production deployments. End-user experience insight and real-time dependency awareness are critical to providing robust SLAs and avoiding runtime problems. Agencies find that relying on siloed application and infrastructure monitoring tools that limit true visibility of traffic impairs their ability to perform an accurate diagnosis of performance bottlenecks when the traffic is moved to the cloud.

Solutions for Better Network, Visibility, Performance, and Availability

Today, with the emergence of agency use of on-premise, public cloud, and hybrid cloud, the need for service assurance solutions across an agency's entire network is critical. Agencies need solutions that look across complex operational environments, discover hardware and software dependencies and topologies, and track transactions, packets, and code traces on an end-to-end basis, providing application impact assessments and context.

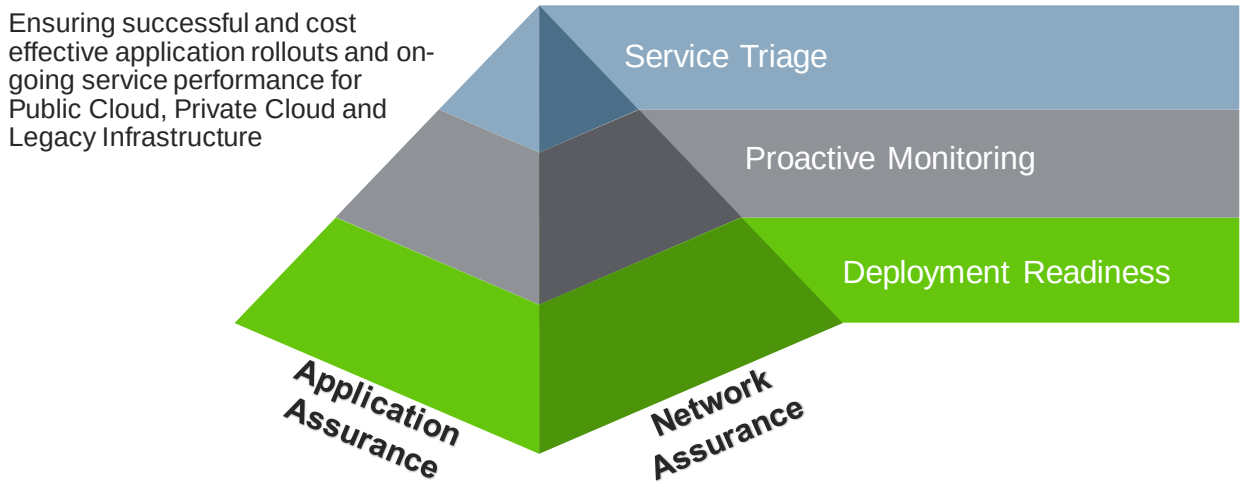
Agencies require monitoring, maintaining, and optimizing the performance and health of their applications across development, test, datacenter, and network environments with end-user/real-user/business transaction monitoring. A single, unified view of performance across applications and infrastructure allows IT and DevOps teams to easily understand whether the source of a performance issue is from the application code or in the infrastructure layer. Agent-based and agentless approaches such as synthetic transaction monitoring, end-user experience insight, and real-time dependency awareness provide SLAs and avoid runtime problems. In addition, advanced visualization/executive dashboards as well as predictive analytics and modeling capabilities can enable rapid and proactive detection, diagnosis, and remediation of application performance problems and incidents.

OVERVIEW OF NETSCOUT'S SERVICE ASSURANCE SOLUTION

NETSCOUT's Service Assurance Solution was created with a singular purpose of providing cost-effective, pervasive visibility. The goal is to ensure successful and cost-effective application rollouts and ongoing service performance for public, private, and hybrid cloud and legacy infrastructure deployments. NETSCOUT's approach provides a clear picture of how applications are performing to the expectation of the business or agency before, during, and after rollout or migration to the cloud. Figure 2 presents a summary of NETSCOUT's capabilities.

FIGURE 2

NETSCOUT's Service Assurance Solution

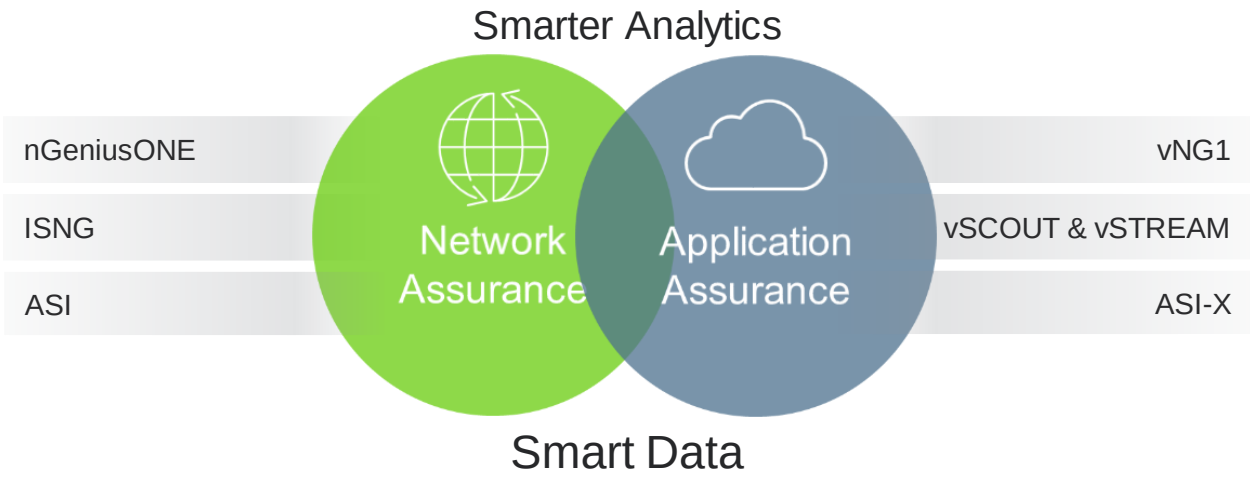


Source: NETSCOUT, 2017

NETSCOUT's Adaptive Service Intelligence (ASI) technology continuously collects, organizes, and contextually analyzes traffic and application data to provide rich information about the performance of applications, networks, and the entire service delivery infrastructure. ASI is the core technology that allows NETSCOUT to scale wire data and transform it into Smart Data for both Network Assurance and Application Assurance. Wire data is the richest source of information on the performance of networks and applications actions and is the single source of truth that provides insight into the performance, use, and complex dependencies of the modern application environment. ASI-X is a "disaggregated" implementation of the ASI engine that allows it to be deployed similar to an agent on application servers for Application Assurance. ASI technology is the underpinning of NETSCOUT's Service Assurance Solution (see Figure 3).

FIGURE 3

NETSCOUT's Service Assurance Solution: Network and Application Assurance



Source: NETSCOUT, 2017

The components of NETSCOUT's Service Assurance Solution are as follows:

- **Network Assurance** is an application view of network services supporting the delivery of business services. nGeniusONE is a highly scalable analytics platform that utilizes ASI data. ISNG is the platform that consolidates multiple specialized analytics tools and feeds a common set of metadata to a wide range of analytics stacks for insights into service assurance, application performance management, cybersecurity, and business intelligence. ISNG models can be deployed throughout for seamless analysis across the entire network, making it easier and more cost effective to monitor and gather intelligence from multiple sources, with no disruption to business processes.
- **Application Assurance** provides application teams visibility into increasingly complex and distributed applications. vNG1 is a virtualized version of the nGeniusONE analytics platform that is fully integrated with nGeniusONE for seamless workflows and can be deployed on-premise or in the cloud and connect to nGeniusONE to provide insights into service performance across the entire IT hybrid environment from the network, application, and user community perspective. vSCOUT is similar to an agent that runs on a virtual machine or bare metal server that enables pervasive instrumentation and can send KPIs to vNG1 or can create a tunnel and forward packets to vSTREAM. vSTREAM provides full ASI capabilities and is deployed on a virtual machine that connects to vSCOUT via tunnels, or in the case of a private cloud, it can accept wire data directly from the vSwitch or hypervisor.
- **vSCOUT and vSTREAM** offer pervasive visibility with software-based instrumentation of traffic flows and application workloads in datacenter and hybrid cloud environments. As the foundation for end-to-end service assurance, including application and network assurance, these tools give IT organizations visibility and control of hybrid cloud environments. vSCOUT and vSTREAM utilize ASI technology to generate Smart Data and extend service assurance solutions from the network to applications, whether they run in physical or virtual datacenters or in the cloud. Such Smart Data can also be exported to external data lakes to infuse big data and analytics projects. When vSCOUT and vSTREAM are used in conjunction with the

nGeniusONE or vNG1 Service Assurance platform, they help identify application and network performance issues across datacenters, cloud environments, and branch offices. vSCOUT and vSTREAM can be deployed in combination with physical and virtual InfiniStream appliances.

- **ASI-X** is deployed with the application that provides a smart data approach to the performance and quality of applications, offering a scalable and affordable option for managing the complexities of applications deployed in hybrid environments.
- NETSCOUT's **nGeniusPULSE,** in addition to the analytics that nGeniusONE provides, offers infrastructure intelligence that combines active tests with monitoring of infrastructure and server health to identify current and potential connectivity and performance problems to ensure that applications are available and meeting expected service levels whether they are in private, public, or hybrid cloud. By enabling full IT instrumentation and providing full-stack end-to-end visibility through a single-pane-of-glass view into the performance of agencies' applications as well as the infrastructure hosting those applications, nGeniusPULSE enables agency IT to pinpoint issues and quickly resolve them.

CHALLENGES/OPPORTUNITIES

Although few agencies can afford to become 100% cloud in the near term, IDC Government Insights believes the trend to place more workloads in the cloud will steadily increase, allowing agencies to update to the latest versions, enhance security and capability, enable rapid deployment of new functionality, spin up new features, support fully functioning disaster recovery sites, and develop an easier way to test and deploy applications. The U.S. federal government's demand for new services is driving growth of network bandwidth/capabilities and computing/storage technologies. Deployment of hybrid cloud technologies increases the need for visibility, analysis of data packets, and assurance across the entire deployment (on-premise, public cloud, and private cloud).

NETSCOUT's traditional strengths have been in the network assurance area for physical datacenter environments. NETSCOUT's movement into application assurance with a software-based approach for private cloud, public cloud, hybrid cloud, and multicloud is a new direction for the company. While NETSCOUT is well known for its capabilities in the network service provider segment, a challenge for NETSCOUT is to increase its visibility in the government sector. NETSCOUT should expand its engagement with DevOps and LOB decision makers that are using public cloud services and embracing multicloud strategies, as they need to maintain consistent end-user experiences and meet stringent SLAs for applications deployed across multiple clouds. NETSCOUT's 360-degree view of application and end-user performance helps predict capacity requirements, optimize workloads, and improve end-user experiences and engagement.

PARTING THOUGHTS

Government is accelerating DX and becoming more reliant on interconnected software applications, driving the need for optimized application performance management. With increased dependence on hybrid cloud, the risk of these technologies slowing down or failing is greatly increased. Deploying cloud should be accompanied by sophisticated and intelligent service assurance tools for both the migration to the cloud and subsequent efficient, secure operations in the cloud. This substantially increases the complexity of deploying and managing these new services. Government IT organizations are looking for ways to improve cloud governance and control while ensuring continuity and continued innovation. Many agencies cannot afford any mission-critical apps to go dark and must be aware of the increasing importance of service assurance within software-centric networks and automation frameworks. An important part of this is finding vendors and solutions that agencies can trust and vendors that can help clients accelerate, transform, and innovate their network and services. NETSCOUT has taken a disruptive pivot to focus on the paradigm shift toward software-based instrumentation. This next-generation instrumentation provides real-time actionable intelligence to ensure service assurance continuity for network providers delivering voice, video, and data services over physical, virtual, and hybrid cloud networks. IDC Government Insights believes that NETSCOUT is well positioned to assist agencies to cost effectively transition networks into the cloud, providing greater intelligence and enabling total visibility into physical, virtual, and hybrid environments.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com