Securely Transition to the Cloud with AWS

In Three Intelligent, Repeatable Steps

NETSCOUT®

WWW.NETSCOUT.COM

TABLE OF CONTENTS

Introduction

Healthcare organizations are undergoing a strategic, digital transformation as they modernize applications and migrate workloads to the cloud. They are pursuing these strategies to utilize the cloud's flexibility and scalability to serve patients better, improve healthcare outcomes, and reduce hospitalization rates. Cloud-centric infrastructure also improves the clinician experience. And overall, it enables healthcare organizations to function with more agility and interact more efficiently with partners in their ecosystems.

There are plentiful use cases for patient-focused, clinical, and business applications in the cloud—from patient portals to telemedicine visits to remote patient monitoring; from electronic medical records (EMRs) to radiology imaging systems; and from team collaboration tools to business platforms for accounting, billing, and claims. For any of these to succeed, however, organizations must be able to accomplish the transformation in a way that ensures a high-quality user experience before, during, and after the migration—while minimizing risks. When it comes to healthcare, business continuity, service quality, and security cannot be compromised.

However, healthcare organizations find that their digital transformations typically involve hybrid cloud environments, which amplify infrastructure complexities. The complexities can obscure infrastructure visibility and make it difficult to assure service delivery. NETSCOUT® offers this paper to help organizations remove these barriers and accelerate migrating workloads to the cloud. The paper focuses on three steps organizations can follow to implement the visibility they need for service assurance and cybersecurity. The steps are designed to help guide safe and effective workload migrations and position organizations to reap the full benefits of a hybrid cloud. NETSCOUT's alliance with Amazon Web Services (AWS) and migration solutions used in an AWS environment are also discussed.

When it comes to healthcare, business continuity, service quality, and security cannot be compromised.

Multiple Forces are Accelerating Healthcare's Shift to the Cloud

Cloud computing has become a necessity for healthcare organizations. As characterized by Accenture in early 2021, "Cloud is no longer a pure technology play in healthcare. It's a business play." The firm asserts that the cloud is the "common denominator" for advancing key business priorities, including virtual care; better, more direct, and more personal engagement with patients; optimized clinical operations; data-driven services; and even attracting top talent. Despite these drivers, however, "only half of healthcare organizations have mature cloud practices and tools in place" to fully exploit these benefits, the firm found.[1]

The gap between priorities and readiness is pushing organizations to catch up.

"People do not want to buy infrastructure anymore, nor should they," says David Chou, a seasoned healthcare technology executive and an honorary member of the IEEE Computer Society. "They want everything to function with the ease and simplicity of the internet. That's where the trend is heading."[2]

Business continuity is another driver and requirement for healthcare in the cloud. The dynamic demands presented by the COVID-19, for example, brought this issue front and center. Suddenly, organizations had to support videoconferencing for telemedicine services and remote working, implement new systems for vaccine administration, and bolster EMR systems to accommodate increased data volumes. In just a few months, healthcare providers ramped up their telehealth services, seeing 50-175 times more patients virtually than their previous practice, according to McKinsey & Company.[3]

"People do not want to buy infrastructure anymore, nor should they." —DAVID CHOU

As Chou describes it, healthcare organizations that were lucky enough to have been thinking "cloud-first" before the pandemic and already had the infrastructure in place could have responded quickly. They could have scaled their remote workforces and telemedicine services for video conferencing or unified communications in a matter of minutes, for example, from 1,000 concurrent users to 10,000. Organizations that did not have this flexibility or the ability to use a cloud solution when the pandemic hit were disadvantaged.

"They would have had to buy hardware, configure it, set it up, and make sure it's configured appropriately. And that can take months, at best," he says.

Continuity ultimately depends on the ability to monitor network traffic across systems. When pervasive monitoring is in place, it is possible to learn all the service dependencies. This service-level visibility, and the ability to look at application traffic from the network perspective, enables IT to measure the quality of patient and clinician user experiences at any location in the digital infrastructure. Healthcare organizations greatly benefit from reducing "time to results" by efficiently and effectively identifying the root cause of application performance problems and optimizing user experience before, during, and after workload migration to the cloud.

A 3-Step Methodology for Moving to the Cloud

Healthcare organizations are initiating cloud migrations from a potentially problematic starting point because the industry traditionally has been cloud averse. "Many legacy healthcare applications were developed to be on-premises and were not designed to work in the cloud," Chou emphasizes. "Now, organizations are finding that shifting to the cloud is not that simple because their applications were never designed to work that way."

Visibility has been a concern. Organizations fear losing visibility into how their workloads perform after migration, especially when migrating to the cloud by lifting and shifting existing on-prem applications. Whether migrating applications using lift and shift or refactoring existing applications, successfully delivering healthcare services on a highly complex infrastructure relies heavily on an organization's ability to address issues as they occur. It requires eliminating application performance and security blind spots that prevent teams from recognizing application performance and security problems.

NETSCOUT cautions that cloud migration is not a "one-and-done" proposition; it is an ongoing process that spans premigration planning, the migration itself, and optimizing services once they are deployed in the cloud. NETSCOUT recommends the following 3-step methodology to address each of these steps. The process emphasizes implementing visibility to inform decision-making and help expedite the transformation while minimizing risks through intelligent performance monitoring and troubleshooting.

STEP 01

Lay the Groundwork with Diligent Premigration Planning

STEP 02

The Transition to the Cloud

STEP 03

Deploying and Operating Cloud Services

STEP
01

Lay the Groundwork with Diligent Premigration Planning

Organizations must perform "know before you go" premigration planning to lay the groundwork for any transition to the cloud. This is the first milestone in every cloud migration. It focuses on assessing the current on-prem infrastructure and applications and defining what the organization wants to achieve—such as cost savings, agility, and ability to scale on-demand. Perhaps the organization needs new or additional capacity to support volumes of digital health records, for example. Maybe it wants to innovate with new cloud technology but doesn't want to damage existing health services inadvertently. Perhaps it wants to add remote medical sensor applications or other services to the cloud and push compute resources to the edge of the network to achieve performance requirements and further improve patient outcomes. The hybrid cloud supports these use cases, but to get there while optimizing performance and reducing costs requires unobstructed visibility into the infrastructure.

Know your system: Planning starts by developing a complete understanding of existing applications and determining which workloads to migrate as lift-and-shift and which to refactor. This includes mapping the vast interdependencies between the many components used in the entire service delivery stack, including the applications, networks, compute, storage, service enablers, and databases.

Organizations should take time to consider the following: What are the current service dependencies for an application to continue to operate as expected when the services move to the cloud? How will migrating to the cloud impact application interactions? What are the baseline key performance, traffic, and server indicators? Which workloads should be migrated to the cloud to reduce the on-prem data center footprint? Which workloads should be moved first? What are the estimated costs of running the applications in the cloud where capacity can be "right-sized"? To stay secure and resilient in a hybrid infrastructure, healthcare organizations must answer these and other questions as they plan each migration to the cloud.

Safe cloud migration starts with on-prem visibility: Deep and comprehensive visibility across a distributed and complicated healthcare infrastructure requires instrumenting application workloads. Here we are talking about using traffic data, which represents every action and transaction in the infrastructure, as a robust data source. Traffic data shines a light on how applications work on-prem so IT teams can effectively manage reliability, availability, and user experience issues when moving to the cloud. Insights gained from traffic data will guide the migration, reduce mean time to repair (MTTR) problems, and enable the organization to develop the appropriate compute, network, storage, and other infrastructure needed to migrate applications to the cloud.

STEP
02

The Transition to the Cloud

A typical environment will be hybrid, with some workloads staying on-prem and others migrated to the cloud. For those applications that migrate, enterprises will employ either a lift-and-shift process to accomplish the migration or refactor applications into microservices—small, loosely coupled pieces of code that frequently interact with one another to enable a service. Either way, the process must occur without risk of service degradation or service disruption so organizations can deliver a consistent, high-quality user experience for patients and clinicians during the transition.

Lift-and-shift involves lifting an application from its on-prem legacy system and shifting it to the cloud. The process is comparatively straightforward for IT teams, and cloud service providers have various automation and data-driven services to reduce the effort of migrating on-prem servers, applications, and databases. But it is not unusual for response-time issues and other performance problems to emerge later. Organizations need visibility to recognize migration problems as they occur in the cloud and quickly pinpoint the root causes.

Refactoring is the process of moving from traditional monolithic applications to modern applications that use containers and microservices. Various tool kits and "cookbooks" are available to help guide this application modernization process. Although refactored applications provide a strategic foundation for efficient, flexible operations, the increased number of communications paths between each piece of code requires continuous monitoring of traffic data. Visibility into these microservices-based interactions, which are elastic and multi-location, is necessary so IT teams can "see it all," otherwise, they will "risk it all" with infrastructure blind spots.

Fundamentally, hybrid cloud visibility must be in place at the outset, or organizations may lose control during migration. Instrumentation on-prem and in the cloud is needed to monitor the new service delivery paths and end-user experiences. The instrumentation will give a complete view into service performance and reveal the source of problems, enabling IT to troubleshoot and resolve issues quickly.

Closing the visibility gap: The hybrid cloud, with its disparate applications and virtualized infrastructure, has made it harder to ensure performance and security. Service delivery spans the on-prem data centers and clouds in this environment, and the interconnections are challenging to monitor. That's why end-to-end visibility is the key to success during workload migration. It boils down to monitoring traffic data anywhere and anytime and gaining the ability to get the correct information to the right people at the right time so they can do the right thing—in short, enabling IT teams to succeed. Today, some cloud service providers enable traffic mirroring to collect and analyze traffic data at the source as it travels east-west within the infrastructure. It is an efficient and cost-effective way to gain end-to-end visibility into applications and security in hybrid cloud environments.

STEP
03

Deploying and Operating Cloud Services

Once workloads are migrated to the cloud, the objective is to optimize service delivery and application performance across the physical, virtual, and cloud environments. Postmigration visibility challenges are best solved by monitoring traffic data to distill real-time, precise, and relevant intelligence from all connected applications and services. These insights will help IT teams ensure service delivery and quality, optimize clinician or patient experience, and investigate vulnerabilities and security threats, including ransomware. Service disruptions can paralyze digital resources from hospitals to outpatient clinics, which is very costly. Anything can go wrong in the hybrid cloud, including application or database errors, DNS problems, QoS mismatch, and network issues. If service performance and availability are the most critical transformative metrics, reducing mean time to knowledge (MTTK) is key to service assurance.

The following sections highlight the importance of low latency, quality of service (QoS), and security to health services and how quickly pinpointing the root cause of performance problems and responding to threats can improve healthcare systems, optimize the user experience, and help protect clinicians and patients.

Low latency: Time-sensitive solutions such as connected health monitors, robot-assisted surgeries, patient video conferencing, and emergency communications have stringent low-latency performance requirements. To minimize latency for applications hosted in their clouds, many cloud providers are deploying compute and storage resources at the edge of the network within telecom provider data centers, at cell sites, and even on the premises of healthcare facilities. The mobile industry considers edge computing so necessary for low-latency services delivered via 5G networks that it has specified a new architecture for deploying multi-access edge computing (MEC) servers close to areas where customers access services.

Latency issues are always lurking in the hybrid

Ensure a high-quality user experience before, during, and after the migration—while minimizing risks.

infrastructure of highly demanding and agile healthcare organizations because there are simply more connections, more services, and more things that can go wrong. Getting ahead of performance problems before they impact patients and clinicians is a challenge. Meeting stringent low-latency characteristics requires end-to-end real-time visibility from all connected applications used for a service and throughout a data center, private and public clouds, and to the edge, with the ability to measure latency in milliseconds. If traffic monitoring data reveals that latency is increasing above a designated threshold, analytics should identify the root cause to fix it immediately. Actionable visibility based on traffic data is how IT teams can help deliver a flawless user experience.

Quality of Service (QoS): Any disruption in service quality has potential implications on clinical processes and patient care. Poor voice quality, one-way calls, bad connections, jumpy videos, and frozen videos wreak havoc on the clinician's ability to communicate in real-time with patients. Organizations need visibility and deep analytics to triage service quality and preserve the user experience.

Healthcare services delivered via streaming media, for example, must be monitored end-to-end to ensure the service meets key performance indicators (KPIs) for high-fidelity, high-definition voice, video, and data. Metrics to assess both voice and video quality include mean opinion score MOS (quality), MOS degradation, QoS mismatch, packet loss, and jitter. By leveraging these metrics, the healthcare organization can reduce MTTK and optimize voice and video performance.

Traffic data is the single source of truth that provides a contextual view of voice and video performance across the service delivery environment. When voice and video degrade or break, analysis of traffic data provides the granularity needed to focus on the nature of the problem within the context of healthcare. Data traffic monitoring has been used, for example, to identify a server causing load balancing issues that degraded QoS; to solve voice quality issues caused by packet loss as voice traffic passed through a firewall, and determine that problems accessing radiology images were caused by archiving the images in the wrong cloud.

Traffic data is the single source of truth for evaluating performance across the service delivery environment.

Security: Cloud infrastructure is architected for security, but as healthcare organizations move some applications and resources off-prem to operate in the cloud and perhaps keep some applications in their private clouds, the overall attack surface expands compared to its original context. Further, security gaps can emerge at any step along the patient service chain, especially in hybrid cloud environments, as data makes its way across applications and systems—from an initial medical appointment to the EMR, perhaps on to diagnostic imaging, specialist services, prescriptions, and to follow-up appointments and billing. The increased attack surface and potential gaps make security an even higher priority than ever before. With an increased attack surface, DDoS attacks can be much more expansive and affect more users. The potential vulnerability is even spawning a new type of ransomware, in which cybercriminals threaten to launch a DDoS attack if their demands are not met by a deadline.

Organizations across the healthcare industry need help to secure dynamic infrastructures that span the cloud, on-premises, and network edge. To strengthen infrastructure security, healthcare organizations need to think about security holistically and comprehensively and architect their hybrid infrastructure to illuminate threats anywhere and anytime. This can be achieved with a shared security model that permits traffic mirroring within the cloud to facilitate monitoring, gain visibility into threats, and derive actionable insights before clinicians and patients are impacted. Such a traffic data approach will make it easier to discover expired certificates, weak ciphers, and other vulnerabilities and enable insights so that SecOps teams can intervene and investigate high-severity findings. An organization can confidently remediate cyber threats by turning network traffic, and global threat intelligence feeds into highly contextual investigations of security risks and proactively examine Indicators of Compromise.

NETSCOUT, Your Trusted Partner for Healthcare Business Continuity Before, During, and After Migration to the Cloud

NETSCOUT is a trusted partner for healthcare organizations migrating applications to the cloud to improve patient care and clinical services. The company's solutions ensure that hospitals and health systems have the real-time, pervasive visibility and insights they need to accelerate the migration and optimize and secure their cloud services. NETSCOUT provides a consistent set of service-oriented workflows to achieve seamless, contextual transitioning across multiple layers of analysis and service dependencies. Its solutions support healthcare's mission-critical applications—whether the applications run on bare metal, in a private cloud or in a public cloud, in a co-located facility, or through a SaaS provider's environment—so healthcare providers can facilitate efficient and informed hand-off of incident response tasks across different groups and foster IT team collaboration.

Visibility: NETSCOUT delivers a unified, consistent view of infrastructure performance and conditions based on real-time traffic data, whether a system is on-prem in an organization's data centers, in the cloud, or at the network edge.

When slowdowns and outages in modern, multi-cloud healthcare environments occur, visibility into the packets flowing throughout the infrastructure can be used to quickly and accurately diagnose the root cause. NETSCOUT harnesses traffic flow information to proactively monitor and manage these

inherent complexities in a cost-effective manner, delivering dramatic CapEx and OpEx reductions and ensuring a high-quality patient experience.

Visibility begins with discovery during premigration and continues throughout the lifecycle. A critical capability is NETSCOUT Service Dependency Map, which allows teams to see all dependencies displayed on a single dashboard across their service environments. Visibility is delivered via NETSCOUT's Visibility without Borders, enabling teams to view and monitor the full range of performance, availability, and security risks impacting their services. Visibility is informed by smart instrumentation, which monitors data traffic as it traverses the network, and virtual private cloud (VPC) traffic mirroring, which facilitates the collection and analysis of traffic data from cloud provider networks. This end-to-end visibility, and the intelligence it generates, is what makes it possible for organizations to optimize service performance, reduce the impact of cyber threats, contain costs, and ensure outstanding customer or user experience in hybrid cloud environments.

Actionable intelligence for business continuity and security: Actionable intelligence, derived from NETSCOUT technologies deployed throughout the network, gives organizations the insights and tools they need to ensure the best possible performance and uninterrupted end-user services. NETSCOUT solutions include the nGeniusONE Service Assurance Platform, which analyzes critical traffic flows across the network, on-premises, or in the cloud. It provides a single pane of glass teams can leverage to view and manage business-critical applications' data, voice, and video performance. nGeniusONE works in conjunction with NETSCOUT's Adaptive Service Intelligence (ASI) technology, which generates "smart data" analytics from real-time IP traffic flows to interpret the user experience.

NETSCOUT draws on this smart data, as well, to inform its portfolio of security solutions, including NETSCOUT's Omnis™ Cyber Investigator (OCI). Omnis Cyber Investigator's cloud-first approach helps healthcare organizations manage threats across increasingly complex digital infrastructures marked by migrating workloads to the cloud such as Amazon Web Services (AWS). By combining Omnis Cyber Investigator's agentless packet access

with AWS-resident virtual instrumentation, SecOps can seamlessly extend their cyber visibility to AWS. AWS native packet acquisition features such as Amazon VPC Traffic Mirroring combined with Amazon VPC Ingress Routing and Gateway Load Balancer enable NETSCOUT OCI to monitor both East-West and North-South network traffic on AWS, convert packet data into smart data, and give SecOps teams an unprecedented level of visibility. NETSCOUT OCI is also integrated with AWS Security Hub to strengthen security posture and reduce risk by aggregating, organizing, and prioritizing findings, and enabling streamlined highly contextual guided threat investigations or unguided hunting to resolve the highest priority security issues. This integrated solution delivers actionable insights to help protect the healthcare organization from attacks that may span AWS, on-premises, and hybrid environments.

NETSCOUT technology alliance with AWS: NETSCOUT partners with cloud providers to help customers migrate to the cloud and address issues as they occur. The company is an advanced technology partner with AWS, which has vetted and validated NETSCOUT solutions for enterprises based on the cloud provider's stringent guidelines for vendors. NETSCOUT has received advanced tier migration and networking competencies from AWS. The benefits to healthcare organizations from this alliance include reduced capital and operational expenses and the ability to accelerate application modernization and workload migration while retaining a superior end-user experience.

Another tangible benefit of the collaboration is that AWS provides NETSCOUT access to its traffic data via VPC traffic mirroring. The capability optimizes sharing of traffic data between the two companies. It enables NETSCOUT to extend its network visibility throughout the AWS cloud and plays a crucial role in NETSCOUT's Visibility Without Borders solution. NETSCOUT also uses the mirrored data in its Adaptive Service Intelligence (ASI) technology to generate "smart data" into actionable, intelligent analytics needed to assure performance, manage risk, and facilitate superior decision-making regarding application and network services.

AWS provides access to NETSCOUT solutions in the AWS Marketplace so healthcare organizations can access the solutions they want directly and begin using them immediately.

NETSCOUT is an advanced technology partner with AWS, which has vetted and validated NETSCOUT solutions for enterprises.

Conclusion: Visibility Can Be Achieved to Enable Safe, Effective Cloud Migrations

Healthcare organizations have more reasons than ever to migrate to the cloud. Still, the process can be intimidating for any company because the migrations will involve hybrid cloud environments more often than not. The complex architectures require the capability to visualize and monitor traffic across systems to ensure proper performance and security. NETSCOUT suggests a 3-step migration methodology to guide a smooth transition process. It includes laying the groundwork for diligent premigration planning, the migration itself, and deploying and operating the cloud services. As a trusted partner to healthcare organizations, NETSCOUT offers a full portfolio of solutions for network visibility that provide the foundation for business continuity and security during and after migration. Organizations can take advantage of NETSCOUT's role as an advanced technology partner with Amazon Web Services to accelerate their migrations further while retaining a superior end-user experience. To learn more, visit NETSCOUT's Amazon Web Services page on the NETSCOUT site or contact Steve Horneman at steve.horenman@netscout.com.

Endnotes

1 "The Cloud Imperative in Healthcare," by Chris D'hondt et al., Accenture, 24 February 2021, pp. 2–5.

2 David Chou comments were provided in an interview with NETSCOUT on 17 March 2021.

3 "The Great Acceleration in Healthcare: Six Trends to Heed," by Shubham Singhal and Cara Repasky, McKinsey & Company, 9 September 2020, p. 8.


NETSCOUT
WWW.NETSCOUT.COM
75 YEARS
IEEE COMPUTER SOCIETY