The IT Network Infrastructure Revolution in Healthcare

FEBRUARY 2021

Authors:
Adriana Allocato
Research Manager, Health Insights
Silvia Piai
Research Director, Health Insights

IDC #EUR147449521

IDC Infobite Sponsored by

JUNIPER NETWORKS
ACCELERATION OF IT NETWORK INFRASTRUCTURE MODERNISATION IS CRUCIAL TO STRIVE AND SURVIVE IN THE FUTURE OF HEALTHCARE

The pace of digital network modernisation has ramped up to address the emerging needs of the healthcare ecosystem, which a traditional legacy infrastructure cannot keep up with.

Accelerated deployment of telehealth/virtual visits, chatbot assessments and remote health monitoring

*Fuelled by COVID-19, digitally enabled remote care will drive 70% growth in spending on connected health technologies by providers and life science companies by 2023.*

Source: IDC Health Insights FutureScape 2021

Simplifying everyday tasks to enhance operational efficiencies: manage the virtual environments and streamline/redefine workflows with minimal disruption

*31% of EU healthcare providers consider workflow modernisation a top priority to improve operational efficiency.*

Source: IDC Multicloud Survey, 2020 (n = 71)

Healthcare providers need to prioritise an IT infrastructure modernisation strategy.

*Legacy healthcare systems are limited* in terms of modern functionalities and connectivity and can’t support innovative business and organisational settings.

*63% of European healthcare providers’ IT budgets are allocated to maintain or upgrade existing systems.*

Source: IDC European Tech and Industry Pulse Survey, 2019–2020 (healthcare)

These emerging trends need the support of high-performing IT networks able to scale on demand.

*Fuelled by COVID-19, digitally enabled remote care will drive 70% growth in spending on connected health technologies by providers and life science companies by 2023.*
A MODERN NETWORK INFRASTRUCTURE CREATES THE AGILITY REQUIRED FOR DIGITAL TRANSFORMATION

Healthcare organisations are focusing on their infrastructure modernisation to lay the foundation of a new digital healthcare ecosystem. Network modernisation will help healthcare providers deliver on their priorities and objectives. **Around 43% of European healthcare providers are investing in modern IT infrastructure.**

> Complete visibility into the network user’s experience, along with AI-driven troubleshooting tools to speed problem resolution, made Juniper Mist the right choice for Queen Elisabeth Institute.

**Stefaan Dewulf, IT architect, KEI**

---

**FLEXIBILITY**
Keeping pace with a rapidly changing environment to include innovative technologies and support any service both clinical and administrative

**PERFORMANCE**
Increasing access to clinical data at the point of care when needed to improve resilience and business continuity requirements

**OPTIMISATION**
Managing a vast amount of data quickly, as well as data transition and delivery, to activate the workflow through applications for clinicians, patients and administration

**EFFICIENCY**
Simplifying network management and keeping TCOs in control, for example by reducing the number of switches in the datacentre to deliver operational savings

**SECURITY**
Moving workloads to the cloud to separate applications with different security requirements

---

41% “We will invest in technology to close gaps in our digital transformation efforts.”

50% “Having a digitally resilient organisation will help us introduce new business model innovation.”

31% of EU HCOs prioritise the modernisation of traditional workloads.

28% of EU HCOs prioritise the modernisation of datacentre infrastructure to improve operations.

29% of EU HCOs have approved security investment to meet new operational norms after COVID-19.
CLOUD-BASED NETWORKING ENSURES HIGHER RESILIENCE AND BUSINESS CONTINUITY WHILE CONNECTING AND SECURING APPLICATIONS END TO END

Healthcare organisations are increasingly considering cloud when:
- Upgrading, expanding or replacing datacentres
- Modernising, transforming or replatforming key applications
- Business demands more agility or speed from IT

This is supporting every business need across the journey to resilience and digital transformation.

% of healthcare organisations considering cloud as a key technology across the different stages of return to growth and innovation

- 46% Business continuity
- 59% Operational resilience
- 47% Acceleration
- 39% Innovation

To gain efficiencies, optimise workflows, lower the costs associated with healthcare delivery and offer personalisation in care plans to improve outcomes.

Cloud networking for operational efficiency
34% of European healthcare providers use hybrid cloud for IT infrastructure management.
Source: IDC Multicloud Survey, 2020

Cloud networking for workforce experience
63% of European healthcare providers have adopted cloud-based productivity platforms to improve workforce experience.
Source: IDC EMEA Future of Work Survey, 2019

Cloud networking for patient experience
30% of European healthcare providers have adopted cloud networking for patient data specific solutions (EHR, medical imaging, medical information exchange).
Source: IDC European Tech and Industry Pulse Survey, 2019-2020 (healthcare)
SECURITY BY DESIGN TACKLES CHALLENGE OF GETTING THE BALANCE RIGHT BETWEEN COMPLIANCE AND BUSINESS TRANSFORMATION

Infrastructures need to be fit for purpose, supporting clinical workflows and patient experience. At the same time, they need to support compliance to data regulations, keep patient information safe and build trust. To get this balance right, healthcare organisations need to adopt a new layered approach to security to enable scalability, intelligence and automation.

Key aspects of layered network security technology should include:

- **Endpoint security** to manage vulnerabilities for individual devices
- **Identity management** to authenticate users and control access
- **Secure data exchange** to safeguard data in motion
- **Containerisation** to prevent threats spreading rapidly once they have gained access to the network
- **Trust management** to address the fact that users and resources can reside outside the network perimeter
- **A software-defined architecture** to provide the speed required to keep up with digital transformation

The nature of cybersecurity threats is changing. Hackers are using AI and ML to create more sophisticated, automated attacks. Digital transformation is further changing cybersecurity requirements, resulting in greater complexity and a perimeter that is disappearing, and all at an accelerating pace.

Healthcare IT executives are looking for solutions to address this complexity and help them become more proactive in managing security risks. In their security strategy:

- **39%** of healthcare organisations will prioritise security automation and orchestration.
- **29%** of healthcare organisations will prioritise the rationalisation of security tool environments.

Source: IDC, European IT Security Survey 2020