

Securing IT Infrastructure in Healthcare



Contents

Reducing Breaches and Building Resiliency in Healthcare IT Operations..... 3

The Growing Complexity of Healthcare IT Operations 4

The Challenges and Risks Associated with Increasingly Complex IT Operations 5

Improve Resiliency and Reduce the Risk of Data Breaches with Teleport..... 7

Reduce security risks associated with identity-based attacks7

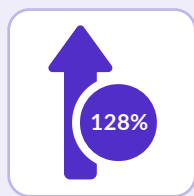
Eliminate the risk of employees using back-door or workarounds to bypass security controls.....8

Streamlining compliance processes.....8

Conclusion..... 9

Reducing Breaches and Building Resiliency in Healthcare IT Operations

Recent cyberattacks, including the devastating 2024 incidents that crippled operations at Lurie Children's Hospital and Change Healthcare, a subsidiary of UnitedHealth Group, have underscored the urgent need for enhanced cybersecurity in the healthcare sector.



In 2023, ransomware attacks on healthcare organizations nearly doubled from the previous year, with a 128% increase in the United States alone ([DNI.gov](https://www.dni.gov)). The financial impact has been staggering, with remediation costs averaging \$1.85 million per incident ([HealthcareBrew](https://www.healthcarebrew.com)) and reaching into the billions for the largest breaches. These attacks highlight the growing threat to both healthcare operators and the digital healthcare technology companies that serve them.

The rise in cyberattacks is directly correlated with a dramatic change in healthcare IT operations. Significant advances in telehealth services, Electronic Health Records (EHRs), and personalized medicine powered by Artificial Intelligence (AI) are revolutionizing healthcare delivery, improving patient engagement, and optimizing clinical outcomes. Supporting these innovations has also necessitated a shift in healthcare IT, resulting in the rapidly expanding scale and complexity of IT operations.

With the growing number of users, devices, and applications accessing the network, managing and securing access to IT resources is more difficult than ever before. Additionally, the dynamic nature of modern IT infrastructure, characterized by frequent updates and deployments, makes it difficult to establish and maintain the robust access controls and audit logs necessary to support industry compliance requirements like HIPAA. As a result, healthcare organizations of all types face significant security, operational, and compliance risks.

Teleport provides a unique solution to these challenges for securing access to infrastructure, with a platform that eliminates credentials and standing privileges, often the target of threat actors for executing breach and pivot tactics. Teleport's approach enhances security, improves operational efficiency, and streamlines compliance processes to support healthcare organizations' digital initiatives.

This whitepaper explores the challenges and risks faced by healthcare operators and digital health technology companies and provides practical solutions to overcome the most challenging obstacles associated with reducing breaches and improving resiliency in IT operations.

The Growing Complexity of Healthcare IT Operations

Healthcare operators, such as hospitals and clinics, as well as technology companies that design and develop healthcare solutions, have seen a dramatic acceleration in market demand for digital health technology in the last several years. To support these initiatives, organizations have increased IT staffing and budget, expanded their adoption of cloud infrastructure, and increased their reliance on SaaS vendors.

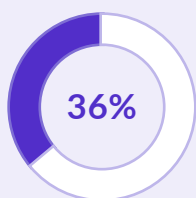
Since the COVID-19 pandemic, healthcare organizations have significantly increased their hiring of IT staff, including engineers, data scientists, and cybersecurity experts, to manage the growing complexity of their digital infrastructure. Hiring for IT roles is expected to grow 32% from 2020 to 2030, much faster than the average for all occupations ([BCG](#)) ([BLS](#)).

Additionally, 75% of healthcare providers increased their digital and IT budgets from 2019 to 2023, with 1 in 5 reporting increases of more than 30% ([Guidehouse](#)). This trend is expected to continue, with significant budget allocations toward cybersecurity infrastructure, EHR modernization, digital care, and advanced analytics.

The adoption of cloud infrastructure has also rapidly expanded. The global healthcare cloud computing market, valued at approximately \$23.4 billion in 2020, is expected to grow at a compound annual growth rate (CAGR) of 14.1%, reaching \$64.7 billion by 2026 and nearly three-quarters of healthcare IT executives plan to expand their use of cloud services ([McKinsey & Company](#)).

Finally, the proliferation of SaaS applications in healthcare has dramatically accelerated. In 2023, healthcare organizations were using an average of 371 SaaS applications, marking a 32% increase from 2021 ([Vena](#)) ([Cloudwards](#)).

These trends have contributed to a rapidly changing environment for IT, security, engineering, and compliance teams. The integration of new people, resources and infrastructure components has caused an explosion in the complexity of IT operations that many organizations struggle to manage.



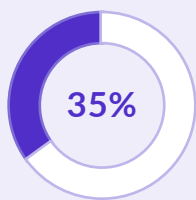
According to RBC Capital Markets, healthcare data will make up 36% of the world's data by 2025, outpacing manufacturing, financial services, and media and entertainment ([RBC Capital Markets](#)).

The Challenges and Risks Associated with Increasingly Complex IT Operations

More users, devices, and applications are accessing healthcare networks than ever before. This expands the attack surface, making these organizations more vulnerable to data breaches and business disruptions.

As healthcare entities integrate more cloud-based solutions and third-party SaaS applications, they introduce multiple potential entry points for cyber threats. Consequently, managing these diverse and interconnected systems becomes challenging, increasing the risk of security vulnerabilities that cybercriminals can exploit. As a result, security, engineering, and compliance professionals face a series of challenges and risks, including:

- Increased security risks associated with identity-based attacks
- Increased risk of employees using workarounds to bypass security controls
- Difficulties in establishing and proving adherence to compliance requirements



Brute force attacks, including password spraying and credential stuffing, accounted for 35% of identity-related breaches in the healthcare industry. Additionally, 32% of organizations reported breaches involving socially engineered passwords, highlighting the various methods attackers use to exploit credentials ([Identity Defined Security Alliance](#)).

Healthcare organizations are particularly vulnerable to identity-based attacks that exploit credentials and standing privileges to breach and pivot within networks. These organizations face an average of 43 identity-based cyberattacks per year, nearly one per week. Successful attacks disrupt IT operations in 26% of cases and overall business operations in 32% ([Safety Detectives](#)).

In the majority of these attacks, stolen credentials and standing privileges are the primary vectors used by malicious actors to gain initial access and escalate privileges further into the network ([Verizon](#)). The risk of these “breach and pivot” style attacks is pervasive. According to a recent survey, 87% of respondents indicated that shared privileged accounts were in use within their organizations, amplifying the risk of extensive network intrusions ([EMA](#)).



Want to view more? Unlock the full PDF.

Fill out the form to unlock the full PDF.

