zscaler™

The future of healthcare, secured.

Solution Brief

Introduction

Healthcare delivery is changing rapidly, and as patient care and improving patient outcomes top priority lists, cybersecurity has become a strategic imperative across the healthcare continuum. Why? The increase in adoption of telehealth, a mobile workforce and emergence of connected medical devices, healthcare is more accessible to patients from anywhere. The traditional networks powering the new modalities provided by innovations in healthcare delivery expand the attack surface and are more vulnerable to threats and data breaches.

This leaves IT and security teams to navigate the vast array of cybersecurity solutions on the market. In doing so, they often patch together, implement, and expend valuable resources while managing a wide variety of point security solutions, adding to the complexity.

- The healthcare industry saw the highest growth of ransomware attacks compared to 2021—a 650% increase[1]
- Healthcare data breach costs increased from an average total cost of $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase[2]
- Healthcare data breaches cost an average of $408 per record, which is three times higher than the cross-industry average of $148 per record[3]

1. Source: https://www.zscaler.com/press/zscaler-threatlabz-2022-ransomware-report-reveals-record-number-attacks-and-nearly-120-growth
2. IBM cost of a data breach report 2021
3. Becker https://techjury.net/blog/healthcare-data-breaches-statistics/#gref

How we help Healthcare transform securely

Healthcare organizations need to provide a secure way for patients and providers to access, manage, and monitor care with a consistent and continuous experience regardless of where the service is provided. Fast and secure access to cloud resources drives this healthcare transformation, and Zscaler helps these organizations securely migrate from on-premises network infrastructure to the cloud using zero trust principles.

Manage Cyber Risk

The adoption of telemedicine, cloud, and IoT have created new ways for bad actors to gain access to valuable healthcare data and systems. The number of ransomware attacks on U.S. healthcare organizations is nearly doubling each year, with most organizations having experienced at least one attack in the last year.

Each HIPAA violation for a data breach can cost between $100 and $50,000/per patient record.[4]

Zscaler restricts malicious access to a healthcare system's networks by making the internet the network for digital work. By keeping patients, providers, and devices off the network and continually verifying identity and access, Zscaler ensures that only the right users are getting access to the right information and systems when they need it. The resulting decrease in attack surface has been proven to reduce the number of malicious attacks by over 50%.

Zscaler's identity-based microsegmentation extends zero trust laterally, preventing broader infection in the data center, network, or cloud. With the ability to decrypt and inspect 100% of all SSL/TLS traffic at scale, Zscaler enables full visibility and prevents data leakage.

Customers have experienced a 35x reduction in affected machines and a greater than 40% improvement in endpoint security.

Contain Infrastructure and M&A Costs

Operating on razor thin and declining margins, healthcare organizations must make considerable investments in IT systems that will support and secure the future state of healthcare delivery, which includes extensive industry consolidation.

Hybrid cloud architectures are becoming the new standard, with business and clinical applications migrating to the cloud to improve efficiency and reduce administrative costs and burden. Zscaler helps ease this transition by allowing existing systems to remain in place while providing a more secure, convenient way to access them. Applying unified, standardized policies across all public clouds and on-premises data centers and securely connecting users, devices, and apps simplifies M&A and reduces integration timelines from months to weeks.

4. Source: https://www.medpagetoday.com/resource-centers/osteoporosis/much-data-breach-cost-your-practice/715#:~:text=Each%20HIPAA%20violation%20can%20cost,lawsuits%20and%20the%20associated%20expenses

Zscaler helps healthcare organizations connect branches, clinics, care centers, and clinicians to the internet (without backhauling) by leveraging multiple network connection types (broadband, LTW and MPLS). This optimizes application traffic routing and performance while reducing WAN costs and network operational expenses.

Customers generally achieve 60% or greater cost savings over their existing inbound and outbound security solutions, resulting in up to a 70% reduction in overall infrastructure costs.

Deliver on New Care Models

Healthcare systems are prioritizing "omnicare" approaches, combining telehealth, in-office visits, labs, remote monitoring, in-home care, and other modes of treatment—all to make healthcare more accessible, efficient, effective, and affordable.

Deploying such a model requires access to data from virtually anywhere, from any device, making it easier for providers, patients, insurers, and third parties to collaborate and share sensitive information. With data dispersed across different platforms, protecting it is a massive challenge. This challenge, along with the increasing number of endpoints created by the internet of medical things (IoMT), has been found to open extensive unpatched vulnerabilities.

Healthcare organizations can secure and simplify the connectivity brought on by the growth of IoMT, allowing new applications and devices to be added to the enterprise easily without adding complexity to the infrastructure. The Zscaler Zero Trust Exchange provides the ability to decrypt and inspect 100% of all SSL/TLS traffic at scale, keeping data secure at every step.

Zscaler's direct workload-to-workload connectivity means customers can increase bandwidth by over 100%, achieve 99.99% application availability, see 100% reduction in network outages, and improve employee productivity by up to 80% with near-zero latency.

Optimize Work from Anywhere

Recession, increasing costs, and significant labor shortages are top of mind for healthcare executives, and clinician and employee burnout is at an all-time high. These staffing constraints make it a struggle for health systems to meet patient care needs in an effective and efficient manner.

The time is now to adopt new and innovative delivery models, team-based care, and cloud technologies to drive efficiency and alleviate clinician burnout. Using resource pools of care providers across multiple locations and enabling non-clinical staff to work remotely has significantly improved engagement, productivity, and efficiency for care delivery models as well employee satisfaction.

Up to 60% of patient interactions for primary care will be conducted virtually in 3–5 years.[4]

Why Zscaler?

Zscaler, creator of the Zero Trust Exchange platform, has built the largest security cloud on the planet to deliver security at scale. Our cloud processes 250B+ transactions, handles 7B+ security incidents and policy violations, and applies 200K+ unique security updates per day from over 150 data centers worldwide.

This best-in-class, cloud native zero trust platform enables fast, secure connections and allows your employees, contractors, patients, and devices to access applications from anywhere using the internet as a health system's corporate network. It directly connects users to applications, securing these users, as well as the data and applications they're accessing, irrespective of their location. It also eliminates the security risks and challenges presented by perimeter-based networking and security appliances—such as firewalls and VPNs—that simply extend the corporate wide area network and expand the attack surface.

Zscaler is trusted by some of the largest healthcare organizations in the world to secure their users and applications. Based on the zero trust principle of least-privileged access, Zscaler provides comprehensive security by connecting the right user to the right application based on your business policies that leverage identity, context, and content of each transaction.

This approach securely connects users and devices directly to your healthcare systems' applications, not your corporate network, which:

- Protects healthcare organizations and their patients from cyberattacks by eliminating the attack surface
- Preserves confidentiality and integrity of patient data
- Maintains compliance with industry regulations including HIPAA and HITECH
- Enables total inspection of SSL traffic to defend from threats and reduce data loss

Analysts agree: Zscaler sets the standard for the new Security Service Edge (SSE) category, being positioned as a Leader and highest in "Ability to Execute" in the 2022 Gartner Magic Quadrant.

Analysts agree: Zscaler sets the standard for the new Security Service Edge (SSE) category, being positioned as a Leader and highest in "Ability to Execute" in the 2022 Gartner Magic Quadrant.

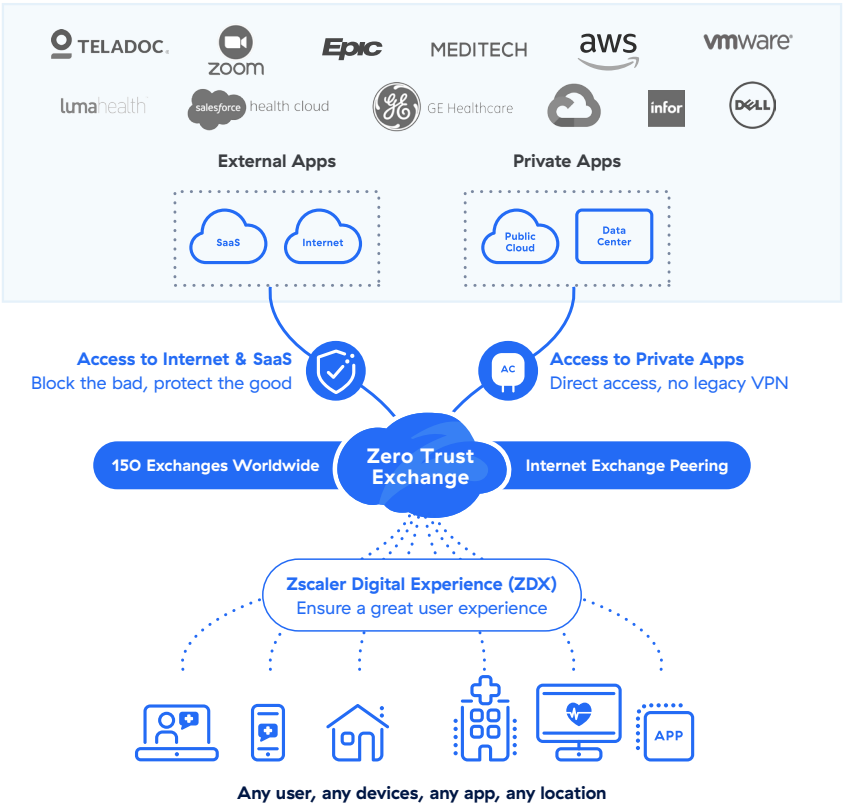
Zscaler in Action

The Zero Trust Exchange provides comprehensive security and risk mitigation by preventing compromise, stopping lateral threat movement, and preventing data exfiltration.

Elements of the Zero Trust Exchange

Extend zero trust across apps, workloads, and devices — Apply the principles of least privilege to give users secure, direct connectivity to private applications running on-premises or in the public cloud while eliminating unauthorized access and lateral movement. Create a seamless experience without the need for backhauling or tedious logins.

Monitor the digital experience — Measuring and improving digital experiences in a cloud and hybrid workforce world requires a unified view of application, CloudPath, and endpoint performance metrics. Analyze, troubleshoot, and resolve end user performance issues for any user or application, regardless of location.



zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com