REVIEW

Zero Trust and the future of cybersecurity in healthcare delivery organizations

George A. Gellert*, Sean P. Kelly, Edwin W. Wright, Leslie C. Keil

Imprivata Inc., Massachusetts, United States

Received: November 29, 2022 **Accepted:** January 30, 2023 **Online Published:** February 9, 2023
DOI: 10.5430/jha.v12n1p1 **URL:** https://doi.org/10.5430/jha.v12n1p1

ABSTRACT

Digital care transformation, the proliferation of disruptive technologies and the changing hybrid workforce have forced the evolution of traditional information technology network boundaries of healthcare organizations. The new landscape has rendered legacy existing perimeter defined and based cybersecurity solutions inadequate to meet increasing regulatory and federal demands for highly secure access management. Emerging compliance requirements, coupled with the concerning increase in healthcare data breaches, ransomware attacks, and security incidents targeting the healthcare sector, have transformed our historic notion of trust into an organizational vulnerability. A "Zero Trust" approach to information security is driven by an imperative to "never trust, always verify," and requires strict, rigorous and continuous identity verification to minimize trust zones and their associated risk of security breach. Healthcare delivery organizations need to appreciate the importance of a Zero Trust strategy in reducing vulnerabilities, strengthening health system information security, and preventing successful security breaches, while also recognizing how identity and access management serves as the foundation of achieving Zero Trust.

Key Words: Zero Trust, Cybersecurity, Identity and access management

1. INTRODUCTION

The digital transformation of healthcare delivery organizations (HDOs) through the adoption and proliferation of new technology solutions such as the Internet of Medical Things (IoMT), cloud-based computing, and the convergence and marriage of information technology and operational technology have led to the obsolescence of traditional information security perimeters and boundaries. Health information technology (IT) systems that were once siloed or physically isolated from unsecured networks are now connected to the much higher breach risk of the open internet. Sensitive medical records containing protected health information (PHI) are being accessed by diverse and dispersed connected devices. In this kind of technologically expanded or distributed environment, the ability to rely on any single point of secure trust can no longer occur – all interactions and end points today involve a level of inherent risk that necessitates what is increasingly described as a "never trust, always verify" approach to cybersecurity for HDOs.

Zero Trust is a strategic and operational framework that enables HDOs to prevent cybersecurity data breaches, and to protect hospital/health system information assets by assuming a priori that no external entity can be trusted. The National Institute of Standards and Technology defines Zero Trust as "a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised."[1]

*Correspondence: George A. Gellert; Email: ggellert33@gmail.com; Address: Imprivata, 20 CityPoint, 6th floor, 480 Totten Pond Road, Waltham, MA 02451, United States.

Least privilege access is a practice restricting access rights for users, accounts, and computing processes to only those information resources that are absolutely required to perform routine and essential activities. Zero Trust is a security model that requires strict identity verification, and moves the decision to authenticate and authorize access closer to the informational or data resource. Zero Trust focuses on authentication, authorization, and minimizing areas of explicit and implicit trust, while maintaining ready availability and seamless authentication mechanisms for personnel. Access rules are as granular as possible so as to enforce the least access privileges required to perform a staff member's requested action.

Zero Trust is governed by foundational principles that include access to corporate resources that are determined by a dynamically changing and evolving environment and resulting policy, enforced per user session, and updated based on assessment of the risk situation, the current state of identity in the HDO, available applications and services, the requesting staff, and other behavioural and environmental attributes. All engagement of information assets and resources must be authenticated, authorized, and encrypted, with authentication and authorization being indifferent or agnostic to the network location. The HDO monitors and measures the integrity and security posture of all owned and associated assets.

2. THE EVOLUTION OF ZERO TRUST

In the modern, digitalised operating landscape, the use of HDO legacy security solutions to enforce authentication and authorization to the cloud can reduce productivity, scalability, good user experience and increase immediate and near-term costs. Relying on legacy solutions can add complexity, administrative overhead and reduce staff ease of use. The proliferation of connected Internet of Things (IoT) devices across HDOs, the emergence of multi-cloud platforms require HDOs to implement and manage diverse new identities to authenticate them and ensure they are cybersecure. As a result, HDOs rely increasingly on secure identities and credentials. These credentials can attract cybercriminals seeking to exploit them for fraudulent purposes. Compromised credentials and identity theft in HDOs are primary contributors to security incidents and data breaches. Simultaneously, HDOs are managing challenges in regulatory compliance that demand powerful mechanisms for identity access, authentication and authorization of even routine organizational communications and processes. Failure to comply with regulatory and compliance requirements can incur substantial financial penalties if/when a security incident occurs. Changes in the global work environment including healthcare are enabling a hybrid workforce, in part accelerated by but predating the COVID-19 pandemic. It is estimated that up to 60% of the general workforce that will opt for a working environment offering greater flexibility by 2024, and there is little to suggest healthcare will be exempt from this trend.[2] The evolving information security environment will likely continue to accelerate the adoption of cloud-based platforms, which heightens the need to effectively – and efficiently – authenticate and convey HDO information processes and resources.

The concept of Zero Trust was first articulated in 2010, and affirmed that to truly secure the digital functioning and processes within any enterprise, all network traffic must be considered untrusted and a potential cyberthreat. From this perspective, trusting users within the network of any organization is an obsolete assumption that will increasingly engender significant security risks.[3] Under a broken trust framework, the authenticity of an identity is assumed to be compromised. Zero Trust recognizes that trust is an invited vulnerability. Once on the enterprise network, users – including external threat actors and malicious insiders – can move freely to access and steal data. In 2014, Google implemented Zero Trust by abandoning its reliance on the security provided by a very private network (VPN) and existing network perimeter security measures, such as threat surveillance detection, analyzing patterns, recognizing threats, and defending against and resolving them effectively.[4] Forester subsequently released a Zero Trust eXtended (ZTX) report updating Zero Trust in light of new cybersecurity challenges and work habits.[5]

In 2021, U.S. President Biden signed an Executive Order to strengthen cybersecurity of U.S. critical infrastructure, including a shift towards Zero Trust security architecture for all federal agencies.[6] In 2022, the U.S. Office of Management and Budget released a federal strategy moving the U.S. Government toward a Zero Trust approach to cybersecurity, building upon existing Department of Defense (DOD) guidance that "no actor, system, network, or service operating outside or within the security perimeter is trusted."[7,8] "Instead, we must verify anything and everything attempting to establish access...a dramatic paradigm shift...from verify once at the perimeter to continual verification of each user, device, application, and transaction". This threat assumption places organizations – including HDOs – in an optimized position to defend against efforts to exploit a network.

3. THE ZERO TRUST TRANSFORMATION OF HEALTHCARE

Implementing Zero Trust architecture is an essential transformation in how HDOs currently operate and respond to

cybersecurity incidents. HDOs are at elevated risk from cybersecurity threats, as evidenced by an increased frequency of ransomware attacks and data breaches. Over 11 consecutive years, HDOs had the highest industry cost for cybersecurity breaches, with a 51% increase in breaches since 2019,[9] and a 10% increase in the average cost of a cybersecurity breach from 2020 to 2021.[10] Seventy percent of healthcare ransomware attacks have resulted in longer lengths of stays in hospital and delays in procedure scheduling.[11] There was a $1.76 million cost difference in breaches where a mature Zero Trust implementation was deployed versus organizations lacking Zero Trust.[10]

Valuable PHI, smart IV devices, other Internet of Medical Things (IOMT), and even refrigerators for storing vaccines and therapeutics are connected to an HDO's network. When that network is breached, it can adversely impact an entire health system, its patients and clinicians. Cyberattacks can target health system electronic health records (EHRs), mobile devices, vendors, cloud applications, remote employees, and medical devices, all are potential entry points into an HDO network. HDOs possess data that is valuable on the black market and their cybersecurity safeguards must be insurmountable. The healthcare sector has much at risk from cyberattacks, but investments in cybersecurity are a low priority for 60% of hospitals and health systems,[12] and 64% of hospital IT teams surveyed reported being unprotected against frequent cybersecurity vulnerabilities.[13] Only 23% of hospitals reported having the resources to adequately secure their supply chain systems.[13]

Traditional network architecture creates a vulnerability for network scanning and lateral movement, while Zero Trust network access establishes difficult to surmount barriers to such movement. Zero Trust functions in a manner that is similar to software defined perimeters by preventing users from having visibility into any other applications and services where they do not have access permission. While Zero Trust may not prevent cyberattacks altogether, it increases network robustness against smaller breaches and attacks. If a threat actor manages to obtain credentials and manipulate any particular device, the risk that they will get much further through lateral movement with Zero Trust access architecture in place is significantly lower. The system constantly places barriers in the attacker's path, preventing access to the entire organization's network through a single crack in the foundation.

When organizations adopt a Zero Trust strategy, in addition to protecting valuable data by reducing risk of a breach, studies indicate it results in 50% fewer breaches, with significant cost savings of up to 50% across the enterprise.[14] Importantly, a Zero Trust security strategy can increase organizational confidence to bring new business models and customer experiences to market,[15] to expand virtual and telehealth capabilities, and to invest in other diagnostic and therapeutic technologies, etc.

4. The Nexus between Zero Trust and IAM

Zero Trust security is built on strong identity and access management (IAM). The Identity Defined Security Alliance envisions that Zero Trust begins with an "identity" whose objective is to get access to "data". Identity is the "actor" in most transactions.[16] An identity is not restricted to human users but can include processes and devices that act on their own to independently access valuable data. By starting with an identity-centric approach to security, organizations can ensure the right people have the right level of access, to the right resources, in the right context or setting, and that access is assessed continuously, without burdening the user. This typically begins with an IAM solution. Establishing a user's identity before allowing them to step into the network is a key objective and a central function of the Zero Trust security model. Security teams can employ features such as shown in Table 1.

These core IAM components confirm that each user has a high assurance session, is using a valid machine and is accessing the appropriate types of file shares.

Table 1. Six Core IAM Features Integral to the Zero Trust security model

	IAM Features
1.	Segregation of duties to prevent one individual or device having full access to all of a healthcare organization's critical resources and assets.
2.	Least privilege access, with every user or device within the network accessing only the most essential resources needed and nothing else.
3.	Micro segmentation that divides the IT environment into security zones and requires separate authorization to access each zone.
4.	Multifactor authentication (MFA) requiring more than a single method of authentication to verify user credentials.
5.	Just-in-time access (JIT) to ensure that no user or machine identity should have permanent, always-on access to a critical resource.
6.	Auditing and tracking to ensure that there's always an up-to-date log of every connection along with a verified identity.

5. Zero Trust and IAM in healthcare

A Zero Trust approach to cybersecurity is driving demand for IAM solutions in healthcare delivery, where unique challenges exist for IAM in the areas of security, regulatory compliance, user experience and operational efficiency.

5.1 Security

Security for digital healthcare services is frequently targeted by cybercriminals. As most data breaches are caused by weak or stolen passwords, HDOs need to avoid password-only access to systems. IAM conveys alternatives to passwords such as biometrics, which can provide lasting verification of identity and stronger authentication that contributes to an effective Zero Trust security architecture. IAM also enables multifactor authentication, which makes it harder for attackers to get past more than one authentication factor and increases trust in the accessing party.

5.2 Regulatory compliance

Regulatory compliance often requires a high level of information security. Achieving HIPAA compliance without IAM is not possible because IAM capabilities allow organizations to meet certain regulatory criteria. These capabilities include self-service account management, flexible login capabilities and role-based access to data.

5.3 User experience

User experience for internal personnel and external customers/patients is critical for HDOs, and thus all authentication journeys within HDOs must not alienate users. IAM enables HDOs to provide seamless registration and login experiences, and enables a Zero Trust security strategy without disrupting user experience. This is important because healthcare users are diverse, with differing levels of digital literacy, and healthcare workers often work under time pressure to save patient lives where providing seamless access to medical records and devices is essential.

5.4 Operational efficiency

HDOs have multiple key stakeholders, requiring complex IAM workflows that may need to span across organizations to include connected care providers, payers, government institutions and supply chain vendors. Without a highly functional IAM solution to support critical workflows, operational efficiency can be undermined rather than seamless and enabling maximal operational efficiency.

Table 2. Zero Trust implementation challenges in healthcare delivery organizations

Zero Trust HDO Implementation Challenge	Rationale
Visibility into diverse distributed medical devices	Healthcare facilities have thousands of unmanaged medical and IoT devices invisible to the network, many never developed for connectivity and often lack integral security features.
Clinical impact	Healthcare devices may have vulnerabilities, outdated firmware or legacy operating systems, and required communications with external endpoints. When implementing Zero Trust policies, rating device clinical impact is critical in order to identify the most vulnerable assets on the network and prioritize the devices where Zero Trust policies should be enforced first to minimize impact on operations.
Unrecognized protocols	Healthcare devices often run proprietary, obsolete, unauthenticated, and/or unencrypted protocols and lack access controls. Standard tools can misidentify necessary vendor protocols and connections between devices as being anomalous and block them, which can disrupt clinical workflow and jeopardize patient safety.
Lack of device security	Medical and IoT devices commonly have intrinsic vulnerabilities and insecure open services for remote monitoring, management and support. Many have default configurations that allow connectivity with little authentication.
Unavoidable vendor and cloud connections	To function properly devices usually must connect to cloud services and vendors to function properly and thus blocking devices from all internet access cannot be achieved without elevating patient safety risk or disrupting clinical workflows. Plus, external connection with third parties risks exposing PHI and devices to attackers, and VPN connections are inadequate because they cannot provide a failsafe security option as HDOs do not control the security of third parties.
Long set-up times	Time enhances vulnerability due to network topologies that change rapidly, creating risk of disrupting device functionality/medical services if communications are interrupted. Mapping and profiling device assets to establish Zero Trust security architecture can be resource consuming without an automated solution.

6. Zero Trust implementation challenges in healthcare delivery organizations

When implementing a Zero Trust strategy to protect medical records and devices from compromising breaches, HDOs face challenges and considerations that are unique to the healthcare environment. For example, blocking all communications until authenticated, as directed by Zero Trust, can disrupt critical healthcare workflows, and could affect device functionality, neither of which can be tolerated in HDOs. The most significant challenges for HDOs are shown in Table 2.[17]

Table 3. Strategies to overcome HDO challenges in Zero Trust implementation

Strategy	Explanation
Identifying the information assets and access needing protection	Complete an inventory and ensure all assets are always accounted for. Understand which information assets and access need protection: (1) Patient confidentiality, devices having PHI and other critical patient information. (2) Patient safety and clinical care delivery information. (3) Clinical workflows and services, device functionality and network topology. Key questions: (1) What is the value of information stored on devices and how vulnerable are the devices accessing it? (2) How frequently are the devices used and are they essential to workflows?
Mapping your network data flows	(1) Use healthcare specific protocols to analyze network and asset behavior in order to identify risks/vulnerabilities. (2) Inspect critical workflows to identify communications that are mission critical for operational continuity.
Defining and enforcing information access policies	(1) Identify who needs access and when/why, and which server is a device communicating with. Identify the vendors a device needs to connect with to ensure needed maintenance. (2) Determine entities' identities in terms of assets, functions, users, uses, resources contained and routine communications. (3) Engage Zero Trust policies and practices to support operational continuity with access to critical medical devices and authorized/authenticated vendors. (4) Configure and enforce segmentation policies which divide a network into smaller, distinct sub-networks enabling network teams to compartmentalize the sub-networks and deliver unique security controls and services to each sub-network. Block unnecessary external communications, and unauthorized vendor/cloud connections to prevent PHI theft and reduce malware network penetration. (5) Configure and enforce micro-segmentation policies that create a secure perimeter zone around each workload, eliminating zones of trust that allow attackers to freely move laterally within the network.
Continuous monitoring of traffic on your network	Dynamic networks require ongoing maintenance, and traffic continuous monitoring to rapidly identify anomalous traffic and interrupt malicious communications.

To overcome these challenges, a number of strategies and actions can help HDOs achieve Zero Trust security safely and reliably, as summarized in Table 3.[17]

7. Four stages of Zero Trust implementation in HDOs

Implementing a Zero Trust strategy can be daunting, but by implementing four core technology stages, HDOs will have a solid framework to secure perimeter-less networks and prevent cyberattacks (see Table 4). Broader solutions may be added onto this foundation, such as anomaly detection, mobile IAM, and positive patient identification. The first stage focuses on strong identity governance and administration, and implementing a plan for regulations, and the required reporting, auditing, and analytics. This stage replaces burdensome, slow, and error-prone manual administration of user accounts with automated, secure, role-based access to systems and applications. The second stage focuses on access and authorization, setting up roles and permissions, so the right clinicians can access the right applications and then providing them with the ability to do so without introducing security friction. A single sign-on solution reduces need for passwords while improving security and supporting compliance requirements by enabling no-click access to on-premise or cloud apps from any device, anywhere.

The third stage provides a secure, auditable chain of trust across the enterprise – including remote access, EPCS, and clinical workflows that are invisible to the end-user. Multifactor authentication with user-friendly methods is critical to ensuring uninhibited workflows, such as push token notifica-

tion and hands free authentication. The final stage is ensuring adherence to the principle of least privilege by providing just enough access to third party or administrators to complete a task, and nothing more. Privileged access management technology makes this possible while enabling compliance by centrally collecting, securely storing, and indexing account access, keystroke logs, session recordings, and other privileged events. Figure 1 summarizes the digital identity components of Zero Trust architecture.

Table 4. Four stages in building a Zero Trust strategy

Stage	Operational Focus
Stage 1: Identity Governance	Replace burdensome, slow, and error-prone manual administration of user accounts with automated, secure, role-based access to systems and applications.
Stage 2: Single Sign-On	Reduce the need for passwords while improving security and supporting compliance requirements by enabling no-click access to on-prem or cloud apps from any device, anywhere.
Stage 3: Multifactor Authentication	Provide a secure, auditable chain of trust across the entire enterprise, including remote access, e-prescription of controlled substances, and clinical workflow while making security invisible to users with authentication methods such as hands free authentication.
Stage 4: Privileged Access Management	Adhere to the principle of least privilege by providing just enough access to third party or administrators to complete a task, and nothing more. Prove compliance by centrally collecting, securely storing, and indexing account access, keystroke logs, session recordings, and other privileged events.

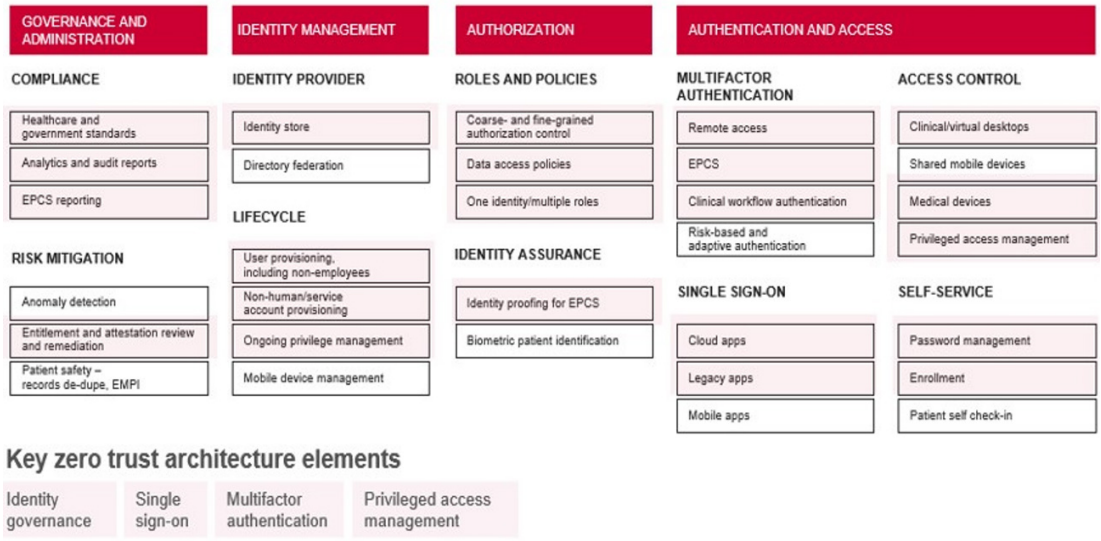

Figure 1. Digital identity components of Zero Trust architecture

8. Usability and HDO adoption of the Zero Trust framework

The three central vectors or areas of HDO information security investments focus on meeting compliance/regulatory and other requirements, assuring clinical end user satisfaction and minimal friction in accessing information and identity, and minimizing external cybersecurity vulnerabilities and threats. The usability of the Zero Trust framework – and its ideal adoption use case in healthcare – is best illustrated by considering a Digital Identity Maturity Model (DIMM) as a guide for assisting HDOs in prioritizing investments to achieve a unified and comprehensive digital identity program, with actionable steps based on current-state processes and solutions. As shown in Figure 2 the DIMM, modeled after Gartner's IAM Program Maturity Model[18] and building on H-ISAC's Digital Identity Framework,[19] introduces five tiered phases of digital identity maturity, with each phase mapping directly to four categories of governance and administration, identity management, authorization, and authentication and access.

From the bottom left of Figure 2 moving to the bottom right, the X axis shows the level of risk associated with five phases, determined by the types of tools and processes an HDO cur-

rently has in place. For example, an organization without a digital identity strategy likely relies on ad hoc, manual, and siloed solutions for controlling and managing digital identities – and will likely be exposed to more security risks as a result. As an HDO implements specific tools and processes to optimize identity management, it will better manage its security posture. From the bottom left and moving to the top left, the Y axis of Figure 2 shows the level of user access associated with five phases. The higher the phase, the more an organization has optimized its access management for secure user access.

Most HDOs have a varied mix of solutions and processes based on program budgets, priorities, and other factors. Thus, most will not fall squarely into a specific stage across all categories, and it is not possible to define a single use case or adoption sequence that would apply to all HDOs. Nonetheless, the future requires a fusion of HDO user access, cybersecurity, and compliance – which is only achievable by enabling, controlling, and monitoring digital identity.

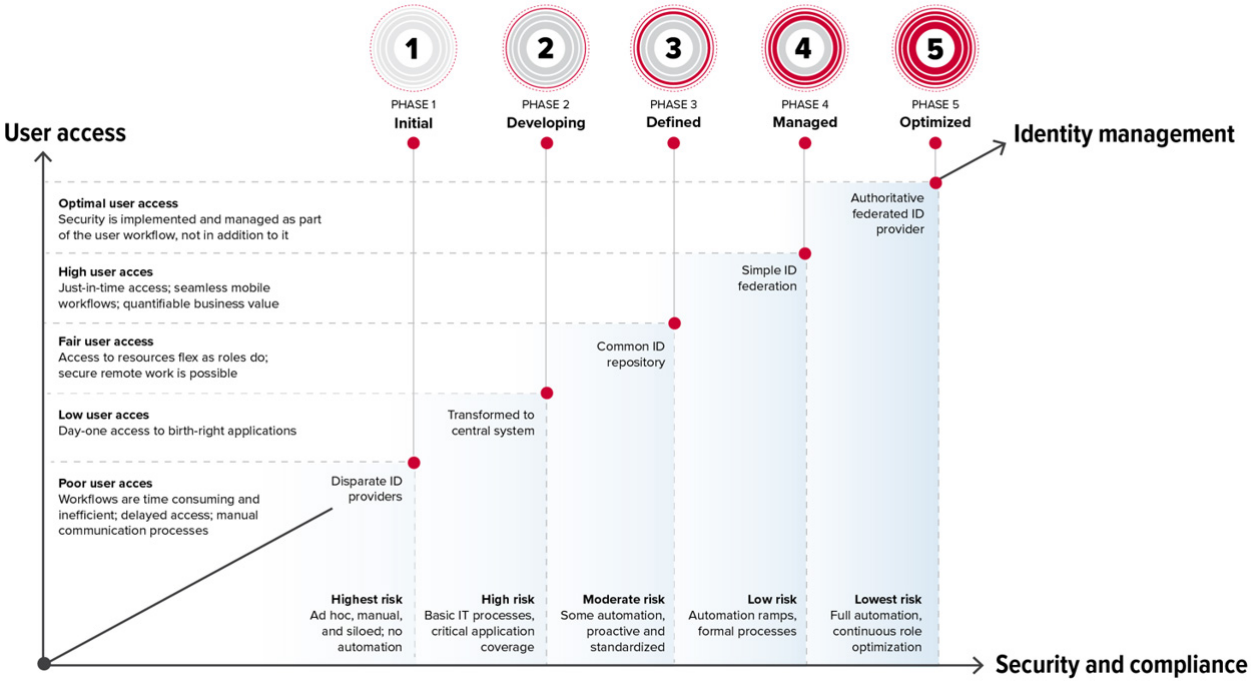

Figure 2. Digital identity maturity model

9. Conclusions: Benefits Realized by HDOs through Implementation of a Zero Trust Strategy

Once Zero Trust is in place, HDOs will benefit in four primary areas: (1) time – end users will spend less time on technology and access and have time liberated for other key areas of HDO focus, such as patient care or organizational innovation; (2) efficiency – information security staff will be relieved of the burden of manually managing many user identities and can instead focus on other strategic initiatives and implementing new technologies into the organization; (3) reduced operational costs – with robust and effective IAM, cybersecurity teams and help desks will no longer be burdened with requests to reset passwords; and (4) holistic security – if properly implemented, all IAM solutions work seamlessly together to close vulnerability gaps, strengthen security posture, remove information technology complexity, and provide a frictionless, satisfying user experience. Given both the increasing frequency and sophistication of cyberthreats against healthcare delivery organizations, implementing a Zero Trust strategy to enable HDOs to defend against cyberattacks should be viewed as an imperative.

Funding

This work had no external financial support.

Ethical Statement

No patient data was utilized in this analysis.

Conflicts of Interest Disclosure

GAG is an external medical advisor to Imprivata Inc. SPK, EWW and LCK are Imprivata employees.

REFERENCES

[1] Rose S, Borchert O, Mitchell S, et al. NIST SP 800-207, Zero Trust Architecture. 2020. https://doi.org/10.6028/NIST.SP.800-207

[2] Gartner HR Survey Finds 60% of Non-Knowledge Workers Want Their Organization to Provide More Flexibility. STAMFORD, Conn. August 26, 2021. Available from: https://www.gartner.com/en/newsroom/press-releases/08-26-21-gartner-hr-survey-finds-sixty-percent-of-non-knowledge-workers-want-their-organization-to-provide-more-flexibility

[3] Kindervag J. Forrester Research: Build Security into Your Network's DNA: The Zero Trust Network Architecture. 2010. Available from: https://www.forrester.com/report/Build-Security-Into-Your-Networks-DNA-The-Zero-Trust-Network-Architecture/RES57047

[4] Ward R, Beyer B. BeyondCorp: A New Approach to Enterprise Security. 2014. Available from: https://research.google/pubs/pub43231

[5] Cunningham, Forrester. The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem, 2018. Available from: https://www.forrester.com/report/the-forrester-wave-zero-trust-extended-ztx-ecosystem-providers-q4-2018/RES141666?objectid=RES141666

[6] Executive Order on Improving the Nation's Cybersecurity. May 12, 2021. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[7] Young SD. Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. Available from: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[8] DoD Zero Trust Strategy. Available from: defense.gov

[9] Constella 2021 Identity Breach Report. 2021 Identity Breach Report | Constella Intelligence. Available from: https://info.constellaintelligence.com/2021-identity-breach-report

[10] IBM. IBM 2021 Cost of Data Breach. Available from: https://www.dataendure.com/wp-content/uploads/2021_Cost_of_a_Data_Breach_-2.pdf

[11] Ponemon Institute. The Impact of Ransomware on Healthcare During COVID-19 and Beyond. September 2021.

[12] McKeon J. Cybersecurity, Vulnerabilities Not Priorities for Most Hospitals. August 12, 2021. Available from: https://healthitsecurity.com/news/cybersecurity-vulnerabilities-not-priorities-for-most-hospitals

[13] CynergisTek. The State of Healthcare Security & Privacy 2021 Annual Report. Available from: https://insights.cynergistek.com/cyber-security-resources/the-state-of-healthcare-security-privacy-2021-annual-report

[14] Jakkal V. Microsoft Zero Trust solutions deliver 92 percent return on investment, says new Forrester study. January 12, 2022. Available from: https://www.microsoft.com/security/blog/2022/01/12/microsoft-zero-trust-solutions-deliver-92-percent-return-on-investment-says-new-forrester-study/

[15] Adopt Next-Gen Access to Power Your Zero Trust Strategy. Jul 23, 2018. Available from: http://www.dataproof.co.za/index.php/2018/07/23/adopt-next-gen-access-to-power-your-zero-trust-strategy/

[16] Considering a Move to Zero Trust Security? Keep these Identity Security Practices and Resources in Mind - Infosecurity Magazine (infosecurity-magazine.com).

[17] Imprivata White Paper, Zero Trust messaging guide. Imprivata; 2021.

[18] Allan A, Perkins E, Scholtz T. Gartner Research, Gartner identity and access management program maturity model. Oct 8, 2009. Available from: https://gartner.com

[19] H-ISAC. An H-ISAX framework for CISOs to manage identity, H-ISAC 2020, April.