

WHITE PAPER

IDENTITY AND ZERO TRUST: A HEALTH-ISAC GUIDE FOR CISOS










SCOPE STATEMENT

What does zero trust mean for health care organizations?

These days, you can't have a conversation about cybersecurity without talking about zero trust. The security concept requires that all individuals and devices on a network be continuously authenticated, authorized, and monitored. Gone are the days of letting someone in the front door, giving them a role with access privileges and then having them go about their merry way.

The concept of zero trust has been around for more than a decade but has gained momentum in the past couple of years, particularly in the wake of a White House Cybersecurity Executive Order and subsequent guidance that mandates a zero trust architecture for federal systems. As federal agencies begin to rollout zero trust frameworks, they are likely to become more pervasive. The purpose of this paper is to educate health care CISOs on the basic tenets of zero trust, the challenges that may be unique to that market, and how to begin implementing the architecture.

KEY TAKEAWAYS

-  **1** *A definition of zero trust*
-  **2** *How zero trust fits into the Health-ISAC Framework for managing identities*
-  **3** *Core tenets of zero trust and the implications for health care organizations*
-  **4** *Health care specific challenges with zero trust*
-  **5** *Steps to begin implementing zero trust*





INTRODUCTION

“Never trust, always verify,” was what John Kindervag from Forrester Research said when he coined the term zero trust.¹ The security architecture is based on the idea that organizations should not trust anything inside or outside its perimeter and verify everything that connects to its network before access is granted.

Zero trust does away with the idea of a security perimeter because if an unauthorized individual gains access to the “trusted network” the perimeter controls will fail to stop malicious activities. A zero trust architecture is designed to prevent data breaches and limit internal lateral movement. In this model all traffic is untrusted and instead of securing the perimeter; it’s a matter of securing the user.² Ultimately, the goal is to prevent unauthorized access to data and services combined with making access control enforcement as granular as possible.

In the early zero trust days the core tenets revolved around securing network access, controlling access based on least privilege, and inspecting log traffic to make sure no one is doing anything they should not be doing. In the intervening years since zero trust emerged additional tenets have emerged as mobile devices are being used and more organizations have moved from on-premise computing to the cloud.

At the core of zero trust is an identity-centric approach to cybersecurity that prioritizes use of multi-factor authentication (MFA) and fine-grained authorization. Here, the proper provisioning of roles and attributes for access is critical. Access rules need to be as granular as possible to enable least privilege and all subjects, assets, and workflows need to be explicitly authenticated and authorized.

MERGING ZERO TRUST AND THE HEALTH-ISAC FRAMEWORK FOR MANAGING IDENTITIES

In 2020 Health-ISAC released “An H-ISAC Framework for CISOs to Manage Identity.” It explained how different identity and access management (IAM) solutions should be architected to enable an enterprise to manage the full identity lifecycle of employees, practitioners, patients, and business partners in a way that guards against common attacks on identity, materially lowers risk, and increases operational efficiencies

This paper revisits that framework and updates it with zero trust in mind. The changes – **shown in red** – incorporate additional controls to deliver core elements of a zero trust architecture. The major changes include:

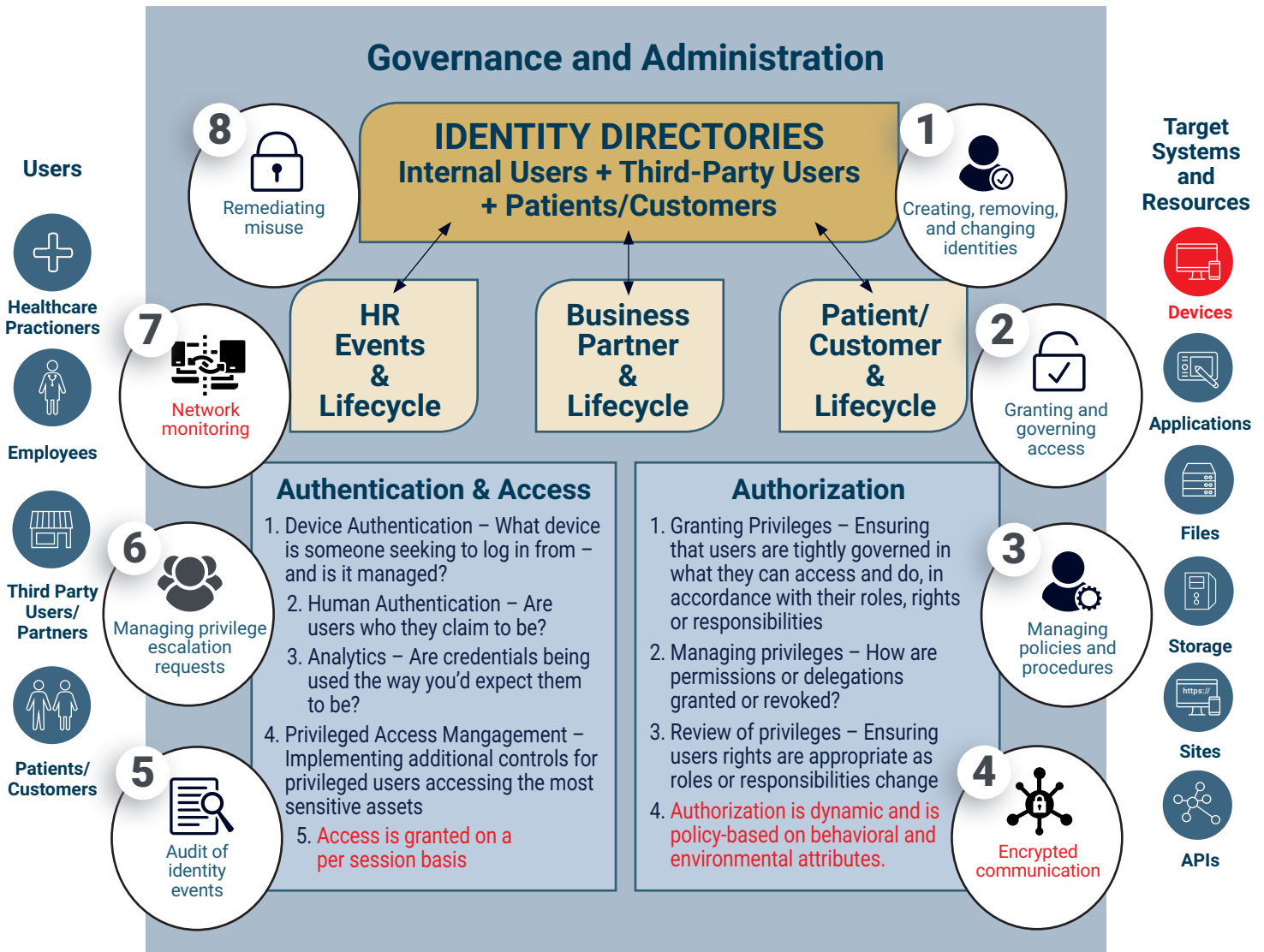
- Securing all communication.
- Monitoring the integrity and security of all owned assets, the network and communication
- Granting access on a per session basis.
- Creating policy-based authorization that is based on contextual information – e.g., what device are you logging in from, geolocation, and other behavioral and environmental attributes.
- Adding devices to the target system and resources.

¹ <https://www.techtarget.com/whatis/feature/History-and-evolution-of-zero-trust-security>

² <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP800-207.pdf>



AN HEALTH-ISAC ZERO TRUST FRAMEWORK FOR MANAGING IDENTITY





CORE TENETS OF ZERO TRUST

Many of the discussions around zero trust revolve around removing enterprise firewalls and other wide-area perimeters. The National Institute of Standards and Technology Special Publication 800-207, "Zero Trust Architecture," details some basic tenets of what organizations should consider.

#	TENET	EXPLANATION	HEALTH CARE IMPLICATIONS
1	All data sources and computing services are considered resources.	Networks may be made up of multiple types of devices from cloud services, laptops, mobile devices, even personal devices that could be used to access resources.	Health care organizations have multiples types of devices – echocardiograms, infusion pumps, blood oxygen measurement, sending data to central monitoring stations.
2	All communication is secured regardless of network location.	Network communication is secured regardless of whether its inside or outside of the perimeter. All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication.	Communication with the network and all devices – including IoT devices – must be secure via encryption or other secure method.
3	Access to individual enterprise resources is granted on a per-session basis.	Trust is evaluated before access is granted with least privilege in mind.	For caregivers and individuals accessing multiple applications at different times their access rights need to be evaluated and sessions established appropriately.
4	Access to resources is determined by dynamic policy and may include other behavioral and environmental attributes.	An organization protects resources by defining its resources, its members, and the resources those members need to access. In addition to authentication and authorization at the time of request, zero trust may also look at behavioral attributes – i.e., device analytics and environmental factors, such as network location, reported activity.	Individuals accessing health care or billing records need to be validated beyond the typical username and password; multi-factor authentication is a must. This may include and may include specific certificates on devices or other behavioral attributes. This would prevent a heart rate monitor from accessing personal health information.
5	The enterprise monitors and measures the integrity and security posture of all owned and associated assets.	Constant monitoring of all devices on a network to detect potential breaches or vulnerabilities.	In a health care setting the number of devices present on a network is more than what a typical enterprise may see and securing all of these different devices that use different standards could be challenging.
6	All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	All devices must have identities and roles within the enterprise to access only the necessary resources.	Individuals and devices must have restricted access based on least privilege.
7	The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.	Constant monitoring of all individuals, devices, and the network to spot anomalous or suspicious behaviors.	Monitoring all employees and devices on a network to prevent unauthorized behavior.





ZERO TRUST COMPONENTS

Implementing a zero trust architecture is not as simple as going to one vendor and picking a solution off the shelf. There are several components that need to be integrated together to create a holistic zero trust architecture. These solutions include:

- **IDENTITY AND ACCESS MANAGEMENT:** A comprehensive identity and access management system is essential for zero trust. This system needs to enable employee and patient access to all applications with one credential. The system should also enable end-to-end lifecycle management, multi-factor authentication, and fine-grained authorization, in line with the Health-ISAC Identity Framework.
- **CLOUD SECURITY GATEWAY:** Cloud security gateways are on-premises or cloud-based security policy enforcement points placed between cloud service consumers and cloud service providers to interject enterprise security standards as the cloud-based resources are accessed.³
- **DATA SECURITY:** The security principle of least privilege should be implemented enabling employees to access only the necessary information to perform their job.
- **NETWORK SECURITY:** Encryption is mandatory; all HTTP traffic and DNS requests need to be encrypted in a zero trust architecture.
- **WORKLOAD/APPLICATION SECURITY:** All applications should be treated as if they are connected to the internet and subject to routine vulnerability testing.
- **DEVICE SECURITY:** This would require organizations to implement a Mobile Device Management systems to manage devices on a network and maintain an inventory of devices authorized to operate within the network.

HEALTH CARE SPECIFIC CHALLENGES WITH ZERO TRUST

Implementing a zero trust architecture for any enterprise is no easy feat, but there are specific challenges that health care organizations may face, including:

- **IoT-ENABLED DEVICES:** Hospitals and health care settings have numerous Internet of Things devices on the network reporting back vital patient information. Defibrillators, nebulizers, oxygen pumps and other monitoring equipment are all configured to send information back to various workstations for monitoring. Enabling these devices to communicate via encrypted channels, giving them an identity, and keeping an up-to-date inventory may prove challenging but will ultimately help secure health care networks.
- **IDENTITY AND ACCESS MANAGEMENT:** Relative to other industries, health care workers are often moving from room to room, either logging into different workstations or carrying a device with them to perform documentation. The multi-factor authentication and fine-grained authorization necessary for zero trust may be difficult or require additional configuration or components.

³ <https://www.gartner.com/en/information-technology/glossary/cloud-security-gateways>





STEPS TO BEGIN IMPLEMENTING ZERO TRUST

Health care organizations need to assess the current state when it comes to the core tenets and components of zero trust.

- What authentication and authorization standards are in place and how would they need to be modified for a zero trust architecture? This includes business processes, data mapping, and workflow categorization.
- What devices are currently on the health care networks and can those communications be encrypted and/or monitored, and can applications tested on a periodic basis?
- What segmentation and additional monitoring can be implemented as input to continuously refine the zero trust architecture? This may require network/traffic evaluation and incremental adjustments to avoid impacts to the organization.
- What roles and responsibilities are in place? The workforce must have clearly defined roles and responsibilities for individual job duties to support the implementation of a least-privileged access model.

Organizations can then start to talk to current technology vendors and find out how they can meet the core tenets of zero trust and implementing some of the components. The criteria may seem daunting at first but will ultimately lead to better security for the organizations in the long term.

Feedback on this white paper and suggestions
for future topics are encouraged and welcome.
Please email us at contact@h-isac.org

www.h-isac.org