maximus

Keeping Customer Experience at the Heart of Zero Trust Architecture

Security policies and considerations for increasingly complex health agency enterprises

Federal health agencies face a unique convergence of increasing data security risks – from the increased proliferation of interconnected medical devices, to evolving federal requirements surrounding protection of health data, to the exponential growth in patient and provider portals – among other factors. The ever-expanding increase in points of health data collection and sharing creates a continual need to balance securing that data with making it readily available to those who need it to make medical determinations and provide care, thereby maintaining (and potentially even improving) Customer Experience (CX). At the same time, the increased availability of patient data presents an opportunity to health agencies to meet mission goals of improving equity of care and enabling greater insights that may lead to better overall health outcomes. These opportunities can only be realized, however, if the data that make them possible is protected.

Federal health agencies' journey to ZTA presents a roadmap for addressing both increased data security challenges as well as opportunities. The journey, however, will require changes in how cybersecurity is approached across health agency enterprises, as well as shifts in mindset for users/customers. Indeed, achieving success with ZTA hinges in part on understanding and addressing CX throughout the journey. Doing so will enable health agencies to achieve success in ensuring that sensitive health data and systems are fully secure at every point of collection, sharing, and management across increasingly complex healthcare ecosystems – ultimately helping agencies meet mission goals and even improve health outcomes.

Leveraging Security Policy Enhancements for CX

For health agencies, the convergence of exceptionally high data security risks combined with the need to have convenient access to patient information illustrates the importance of adopting a CX perspective on the ZTA journey. In particular, the Zero Trust pillars of Identity and Data are ripe with both challenge and opportunity.

Account and Identity Management

Under a robust ZTA, cybersecurity is no longer predicated on intrinsic trust. Instead, it's about the assumption that the enemy is already inside an agency's defenses. As such, tools to improve account and identity management while understanding how these requirements will impact CX, will be must-haves in any ZTA rollout.

Striking a balance between security and administrator access

Among the core components of ZTA is the need to put up guardrails for key personnel whose work is both instrumental to agency operations and potentially devastating to a mission when under the influence of bad actors. Privileged Access Management (PAM)

is becoming an increasingly critical tool for doing so, providing just-in-time access and just-enough access to strike a balance between strengthening security posture while enabling administrators to keep servers operating and critical health data available.

Facilitating a cultural shift for user access

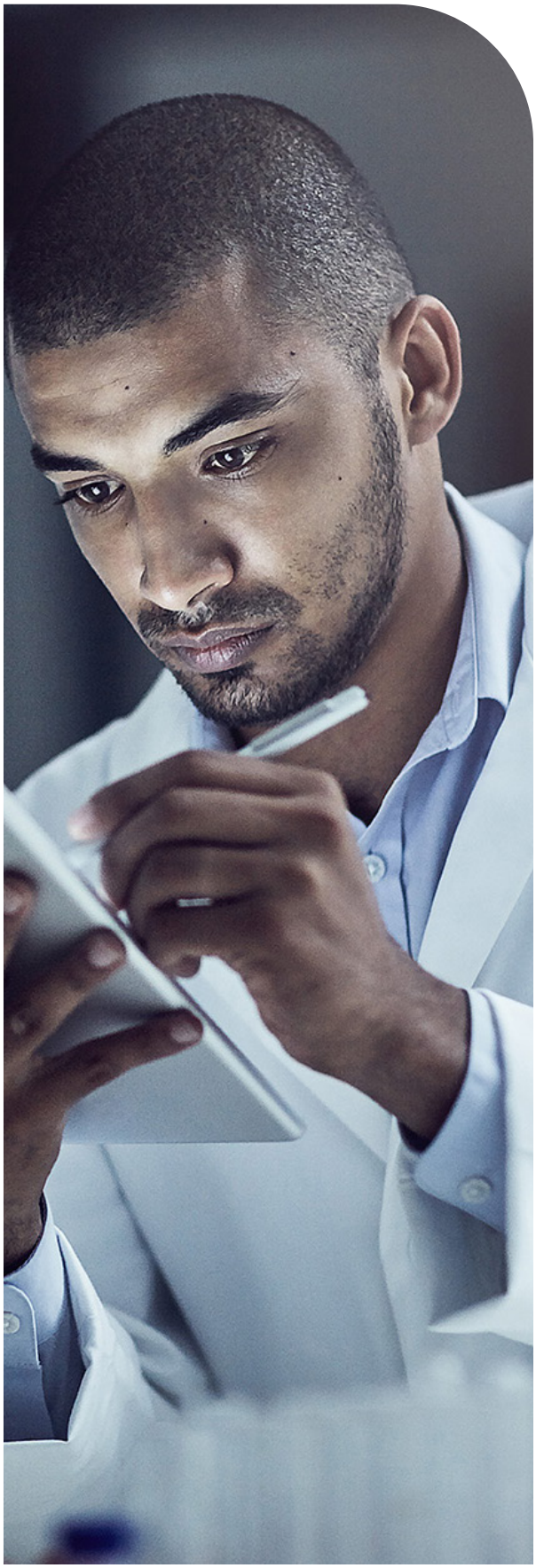
New ZTA policies ultimately keep data more secure and available, but they also present a potential Achilles heel: the increase in time, repeated logins, and resulting frustration that ride alongside more stringent requirements for user provisioning, authentication, and re-authentication. This shift will not be easy, and likely will necessitate a cultural shift to both understand and embrace the importance of these added steps as part of the ZTA, as well as considerations in implementation of security policies.

Fortunately, key security enhancements and tools can help to address CX as part of the ZTA journey by managing the growing complexity of user logins and authentication, including:

- Password reset and recall
- Device recognition
- Identity proofing
- Fraud detection
- Data privacy and compliance
- Multi-factor authentication
- Soft tokens

Understanding security needs for different personas

As part of their ZTA, health agencies should consider the different security configuration requirements of different personas (e.g., session lockout durations), including personal



versus nonpersonal identities and logins. This inventory can help the agency gain a clear picture of the full identity environment, identify any gaps, and inform the creation of new policies and processes for security integrations such as Advanced Malware Protection (AMP) and other enhancements.

Securing and maintaining access to interconnected devices

Providing multiple advances in care for patients, the proliferation of interconnected Internet of Things (IoT) medical devices also sharply increases security risk. Security policies for account and device registration should be informed by the real danger of medical device data breaches that can impact not only data availability, but even lead to inaccurate medical determinations and care. Through a combination of software and policies, Comply to Connect (C2C) can be achieved to ensure that an endpoint is secure before connecting to the enterprise and gaining access to device data and systems.

Data Management

Protecting data throughout an organization's infrastructure is central to Zero Trust (and indeed to agencies' ability to improve health outcomes). All networks, users, and workloads are about accessing, analyzing, manipulating, and utilizing data to help agencies meet mission goals. However, without the due diligence needed to organize and optimize that data, its value to patients and providers is depleted and its contents vulnerable to those who would exploit it for their own value instead. Shepherding in an era of laser focus on data security, ZTA is poised to help health agencies extract the most CX value from health data by focusing on four key areas:

Data Customization and Security + AI = The Future of Improved Patient Care?

Key data management enhancements as part of ZTA may provide a window into the future of improved patient care. For instance, like any document, a patient's medical record can be tokenized by section, category, or word – and tagged for viewing only by the patient or medical professionals who need access to the specific information.

For example, some sections of the record might be viewable only to a dentist if it pertains to the patient's dental health, while other sections may be viewable only to a cardiologist if the data pertains to the patient's heart health. And of course, both sections could be tokenized for viewing by both clinicians if there are dental conditions listed that could be linked to heart conditions. This capability could provide more timely and meaningful health data to clinicians and collaboration among them when making medical determinations.

In fact, artificial intelligence (AI) may be increasingly leveraged to enable more detailed connections between patient symptoms and health conditions as these tools become ever more sophisticated and capable. With ZTA, security policies can be put in place to allow clinicians to securely leverage that insight for improved care.

Protecting data

A core principle of ZTA is data protection by using granular, context-based policies. This includes development of data categories, tags, and security rules, as well as a comprehensive approach to applying them to loosely structured or unstructured data generated by IoT devices in order to secure sensitive data against unauthorized access. Zero Trust can go a long way toward better securing data and creating further visibility into who or what is using or accessing it and where it's going. This requires knowing what data you have, where it's located, what risks might affect it, and how it travels between systems and applications. Only with this understanding can new security products and processes be modified or added with the confidence that they will have the intended impact.

At a minimum, it's important to ensure that data can't be modified, deleted or encrypted by any non-authorized person, device, or service. While some workloads may need to be kept on premises for government agencies, the convenience, availability, and user friendliness of most cloud environments is an up-front win for CX – and industry-leading cloud providers already have many "baked-in" security features of ZTA. These solutions inspect and log traffic and create secure data layer protection (DLP) where data is always encrypted, both at rest and in-flight across clouds or sites.

Obscuring, securing, and retracting data

The data redaction technologies and processes needed to pull back data in the event of an emerging security risk are usually employed reactively – put in place after a problem has occurred as a defensive maneuver to limit potential damage. Implementing Natural Language Processing (NLP) and Named Entity Recognition (NER) provides a more proactive approach, hiding sensitive information such as health agencies' personally identifiable information (PII) and protected health information (PHI), safeguarding it from exposure. This allows patient data to be shared without the fear of exposing it to unauthorized parties, creating safer user portals and data sharing practices.

In addition, data obfuscation enables obscuring and securing information as it's made available

across a network from those who should not have access to it while enabling improved customization of access for those who should. Through obfuscation, medical personnel can gain access to a wider range of data tagged for their use, while support personnel may access only a subset of that data for which they need access to help streamline patient encounters and data sharing between providers.

Encrypting data

As a basic principle of Zero Trust, encrypting and authenticating all data traffic as soon as possible, including internal traffic, will continue to be a critical component of data management. In addition, terminating every connection so that all traffic (even encrypted traffic) can be inspected in real time before it reaches its destination enables proactive identification of unusual data movement, ensures secure data transfers, and ultimately helps to maintain the trust and confidence of patients and providers.

Tagging and customizing data

The use of data tokenization throughout the data layer itself to tag data at increasingly granular levels can result in tremendous benefit to the security and convenience of document control for classified or controlled unclassified information (CUI). Even if such a document is somehow released publicly, the secure or classified sections would only be visible to those with provisioned access. In addition, the sidestepped data breach can automatically be sent to the health agency's security team for remediation, along with a notification to the user – providing a built-in self-correcting mechanism that can improve the security mindset of users in learning from mistakes and missteps.

Partnering to Meet the Mission

As a trusted partner for many federal agencies, Maximus has a deep commitment to supporting federal health agency missions. Our cybersecurity experts are renowned in the field, combining technical acumen with a nuanced understanding of user experience (UX) design principles that can improve CX to drive the success of Zero Trust adoption across health agency enterprises. Our understanding of health agency missions is coupled with a commitment to actively engage with agency leadership to empower decision making and ensure the most value from their Zero Trust technologies and processes. Our culture of innovation is centered around small teams to develop quickly and efficiently. While we work in an incubator type of environment to develop and nurture new ideas, we have the resources of a large company to execute and deliver quality results.

Learn how Maximus is assisting federal agencies to establish data strategies that improve efficiency, drive interoperability and support their missions.

maximus.com/federal-health