

A large, intricate maze graphic in shades of blue and white, occupying the left side of the page. It features a central circular area with concentric lines, transitioning into a complex, winding path that leads downwards.

Zero-Trust is the
Outcome of
**Identity-Based
Access Control**

Introduction

As the IT landscape evolves, new and more sophisticated cybersecurity threats continue to appear. These threats present organizations undergoing digital transformation with a challenge: how does an organization provide access to data, apps, and devices while at the same time ensuring that protection is persistent and evolves with the threats? Data is the currency of digital transformation, with many of the changes being new ways to access, use, and benefit from data. Managing the access to these resources is a large project, but it is the only way to securely transform.

Zero-trust has entered the security lexicon with a bang. Once derided as merely a buzzword, zero-trust is now the de-facto method to deal with an overwhelming number of human-centric threats and device vulnerabilities brought in with digital transformation. An identity centric access solution is foundational to the zero-trust framework and encompasses users, applications, and infrastructure. Overall, the goal is to rebuild a dynamic, identity-based perimeter from the generalized anonymity of the cloud.

Zero-trust is about accurate identity, limited access, and verified trust, with the motto, “never trust, always verify.” You can significantly lower the risk of nefarious access by adding verification and continuous authorization measures to a given person, device, or machine. Identity is the pivot upon which zero-trust turns and is driving the development of the zero-trust framework to deal with human-centric cybersecurity threats.

In May 2021, the Federal Government of the United States published an “Executive Order on Improving the Nation’s Cybersecurity”ⁱ and called for federal agencies and their suppliers to “modernize their approach to cybersecurity.”

In addition, the order recognizes the role of a zero-trust security role, stating:

“The Federal Government must adopt security best practices; advance toward zero trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.”

Many other governments and regulatory bodies have also offered guidance to improve cybersecurity, and the zero-trust framework features prominently in all of them.

- EU - NIS 2 Directive (Network and Information Security (NIS) Directive)ⁱⁱ
- UK - DSPT (Data Security and Protection Toolkit) standard 20-21ⁱⁱⁱ
- U.S. - HIPAA (Health Insurance Portability and Accountability Act)^{iv}
- U.S. - CISA documents on Zero Trust^v

In addition, the U.S. standards body NIST has created a framework for zero-trust, publication NIST SP 800-207 ZTA that states:

“ZTA (Zero Trust Architecture) is a response to enterprise network trends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary.”



What is Zero-Trust, and How Does It Fit with Digital Transformation?

Developed to replace the traditional perimeter edge model of security, zero-trust is a methodology based on the ideal that access must be verified whenever and wherever it happens. An organization that implements zero-trust security uses identity to verify and control access to sensitive data and other resources. This aligns perfectly with the digitally transformed enterprise, where a perimeter is replaced with a distributed cloud computing model that supports a dispersed and remote workforce on devices that require always-on, anywhere access.

Identity-based security solutions are deployed as-a-platform alongside existing identity infrastructures, such as Azure AD, to control and simplify access to authorized assets. Because it is not restricted to network-based segmentation alone, a dynamic, adaptable, user-centric solution can apply granular, real-time policies to enforce secure access. As an enterprise implements digital transformation across its systems and processes, an identity-based security solution provides the validation layer needed to secure always-on, anywhere access.

“Zero-trust access is based on identities rather than networks, users can be granted more granular access to only the resources they actually need to do their jobs. This lowers both the risk of compromise and also the potential damage in the case that a cyberattack does occur.”

Eran Shmueli, chief architect and co-founder of Cyolo



The Five Pillars of Zero-Trust and Identity Controls

As more enterprises embark on the journey of zero-trust, there are some common challenges they encounter along the way. Having a clear plan to address these trouble areas makes all the difference when they arise. Below are five challenges teams should prepare to meet:

1. The Human Element

Since humans are a common target for data breaches and other cyberattacks, the focus must be on controlling the interaction of human operators with IT resources and data. This begins and ends with identity. However, adaptable identity and access control require an ecosystem of enabling components that provide visibility of people and devices across expanded cloud infrastructure and out to the fuzzy edge of modern devices. Successful zero-trust projects need to provide the needed cybersecurity level to secure each person in their digitally transformed business.

2. Cloud Technology

Cloud technology has empowered the enterprise by breaking the boundaries of the perimeter. However, this capability has also created a massive attack surface, with vast volumes of data flowing across devices and networks. Zero-trust enabled by identity control mimics the expanded nature of cloud computing and recognizes that identity is not a static object. Instead, zero-trust enabled by identity is dynamic and adaptable enough to adjust to the environment at any given access point.

3. Compliance & Data Privacy

Data protection regulations are fluid and evolve with the changing cybersecurity and technology landscape. The only way to keep up with this moving target is to move with it. The zero-trust model adapts to changing conditions and can be easily updated to reflect changes in regulatory requirements. In addition, many platforms provide auditing and reporting capabilities to help ensure regulatory compliance.

4. Remote & Hybrid Work Models

With work happening almost everywhere but the office, each user and their location needs to be accounted for in the zero-trust program. This approach has proven efficient and effective as access resides with the verified user and device, no matter where they are; access will only be allowed if an identity is successfully verified. This verification can be enforced on sign-on and continuously validated as the employee works across devices, apps, and cloud services.

5. Total Experience (TX)











A TX strategy is a fundamental part of a successful digital transformation. A great TX brings together every aspect of a company, from employee to customer, to make interactions with an organization the best they can be. Behind this ethos are the identities of these individuals. Frictionless experiences are part of the development of a great TX. Zero-trust models of security place identity central to security, but they do so in a seamless way that enhances the overall TX.

Zero-Trust Deployment Checklist

Digital transformation of business processes cuts across all aspects of an organization and its commercial and operation models. For example, in manufacturing, digital transformation is witnessed in the IT convergence with OT (operational technology). In commercial and retail, digital transformation enables new and exciting ways to reach out to customers. All these improvements rely on a solid sense of identity, allowing organizations to ensure that only validated and verified users are allowed to access the applications, systems, and resources they need to do their job.

To make sure that you meet the challenges of securing your digital transformation journey, here is a checklist of identity must-haves:

“...the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.”
The White House

Area	Functionality and Fix	Benefit
 Remote & Hybrid Work	Dynamic and continuous access control	BYOD and remote working create an expansive threat matrix. Zero-trust securely connects remote users to apps and data centers, even when using an unmanaged device. Removes the scalability issues seen with VPNs.
 OT Operators	Risk-based, modern authentication enforced by granular policy measures and controls	The convergence of OT and IT has led to an increase in cyber-attacks. To limit attacks, assets must be hidden from external view and access control must be robust enough to verify the device as well as the person. Insider threats are an important consideration in cyber-security threat mitigation in manufacturing. Identity-driven zero-trust models help prevent insider threats by never inherently trusting and always verifying access.
 Privileged Users	Authenticate and authorize access using AI	A fine balancing act is needed for users with privileged access to sensitive resources. AI-based ZTNA solutions provide the tools to verify the user without creating extra friction.
 Granularity of Choice	Authentication and authorization	Granular control per application, based on user ID, biometric (fingerprint and face) authentication, geo-location, timing, one-time password access, and risk-based assessments based on its AI functionality.
 Web Applications	Visibility and access control	Full visibility and control of web apps is a must-have. Risky actions include copy-paste and file transfers – these must be controlled to prevent malware infection and data leakage risks.
 VPN Alternative	Provides better granularity of access control	VPNs have helped during the Covid-19 crisis but have been found to be lacking in scalability and have poor security controls. For example, no granularity in access control, allowing access to the entire network. Gartner predicts that there will be a significant move (60% of firms) from a VPN to a ZTNA platform by 2023.
 BYOD	Device identification	One of the key challenges of traditional access control is that devices are typically left out of the equation. However, identity-centric zero-trust ensures that devices as well as people are identified.
 Always on, Anywhere	Scalability and availability	Expanded cloud infrastructures with vast numbers of devices and users, often located in remote places, needs smart and adaptable scalability and availability.
 Compliance	Security controls and data protection	Identity-centric zero-trust provides an adaptable way to meet changing regulations.
 Reports	Audit and reporting	Reports and auditing provide data to allow security investigations. Reports also offer a way to evidence support of regulations.

Making Digital Transformation Work

Identity plays a vital role in the overall security of enterprise environments; this has always been the case. When an individual walks through the door of a building, they are asked who they are and to provide some form of evidence to verify themselves.

As the enterprise becomes increasingly digitized, verifying an identity remains a crucial requirement. However, with an expanded cloud-delivered infrastructure, this verification has become an adaptability challenge in securing access while presenting a great TX. Identity-driven zero trust architectures offer a way to ensure that access to resources is robust while delivering a seamless experience for users. Meeting this balancing act of security vs. usability comes down to using intelligent technologies that adapt to change as it happens. “Never trust, always verify” is achievable using identity-based access control as the foundation for success in digital transformation.



References

- i. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
- ii. <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union>
- iii. <https://www.dsptoolkit.nhs.uk/News/2021-2022-standard>
- iv. <https://www.hhs.gov/hipaa/index.html>
- v. <https://zerotrust.cyber.gov/>

About Cyolo

Critical assets and systems remain exposed because traditional secure access solutions have not been able to protect the legacy and custom apps that make up the last mile. Cyolo's purpose-built Unified Digital Access Management solution works alongside any and every existing security software to bring secure, frictionless and agentless user access to the edge. Within minutes of configuring, the last mile for IT, OT, and other critical infrastructures are protected with no change management. Now work can happen everywhere without compromising any security controls.

cyolo.io

