

# IAM and Zero Trust: Modernizing to a Zero Trust Architecture

Identity access management policies should include zero trust architecture principles to build resilience against modern threats.

## Introduction

Traditional security architecture is becoming out of place in a world of global connectivity, global data, and global threats. Enhancing security is not simply a matter of replacing or augmenting passwords with multi-factor authentication. Conventional perimeter defense, or castle-and-moat protection, grants wide access to users and devices capable of breaching an exterior-facing barrier. Against the evolving threat landscape, this level of trust is unsustainable—and insufficient.

Zero trust architecture (ZTA) inverts the premise of traditional perimeter defense. Instead of a perimeter barrier followed by an open-door policy, a zero-trust architecture continually analyzes and validates requests for access against a wide range of criteria, including the nature of the requesting device, the device's geographic and network location, and known data about the requesting user. By continuously challenging requests and granting limited credentials, ZTA helps organizations keep data and applications secure inside and out, and is a welcome advancement for identity access management (IAM) practices.





## Assessing Your Security Maturity

Because zero trust architecture can be built through a variety of vendor solutions and process changes, there is no single path to implementation. Consider these questions as you assess how ZTA can reinforce your security practices:

- **Can you articulate not only who should be granted access but when and how that access should be allowed?** Since context is a crucial component of ZTA, an effective understanding of the circumstances in which a valid user should still be denied access is important. (Examples: a login from an unauthorized device, from a network location that is inconsistent for a given user, or at a time of day unusual for that user.)
- **Are your networks already internally segmented?** A traditional security architecture allows wide lateral movement to authorized users. More mature approaches have additional internal protections cordoning data and application resources even from “trusted” users.
- **Is your identity management system centralized and robust?** The automated provisioning and policy enforcement principles of ZTA are easier to apply when a centralized system controls access privileges at a granular level and tracks user activities after authorization.
- **Have you performed root cause analysis on previous security compromises?** Understanding the weaknesses that led to any previous security breaches can help inform the first steps in your ZTA journey.

## How to “Right-Size” Zero Trust

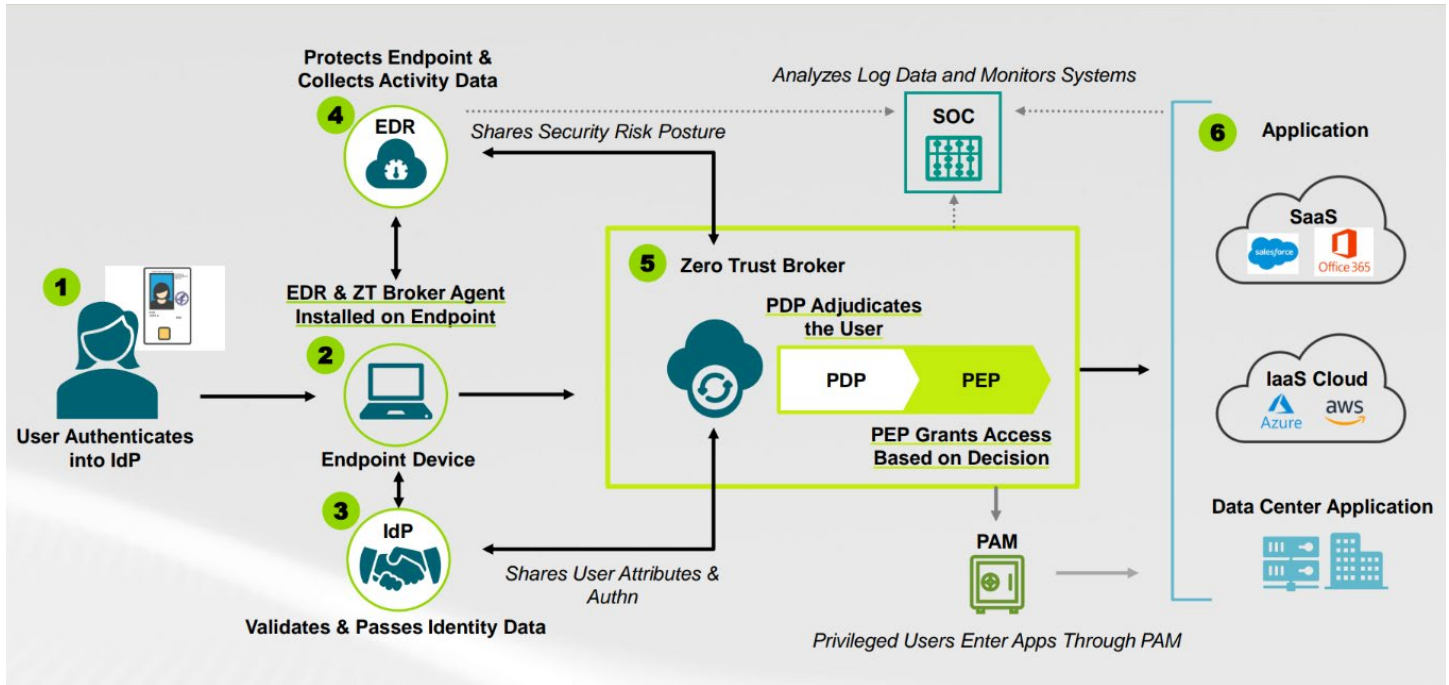
Zero trust looks a little different in every organization that has successfully made the transition. But all ZTA implementations share common characteristics. The six principles below are not the only components of ZTA, nor are they exclusive to ZTA. But conforming to all six means an organization is well positioned to take the next step in evaluating ZTA technology and implementation vendors:

1. Use contextual authentication (never trust, always verify).
2. Authorize access decisions based on all available data
3. Log and monitor networks continuously and apply analytics for better visibility.
4. Adhere to the principles of least privilege and least functionality.
5. Use end-to-end encryption.
6. Microsegment networks, systems, and applications.

Finding the path to effective zero trust architecture is easier when working with an experienced, vendor-neutral partner like Guidehouse. Our ZTA experts put your organization’s current security needs, capabilities, and shortcomings in context. For example, an organization with strong identity management practices may be able to start the ZTA journey with a focus on network segmentation. If application access is poorly mapped, a full audit and overhaul of those controls is prudent before any other steps. Based on each organization’s specific needs, we create a roadmap that includes communication strategies and rollout practices to help affected employees, customers, and partners maintain access and productivity during and after the transition.

A right-sized approach to ZTA respects that real-world operational needs are sometimes messy and complex, and that a too-rigid approach to credential management can inhibit legitimate transactions. Working with stakeholders at all levels, Guidehouse helps organizations create privilege and exception policies that support operational goals without critically compromising the concepts of zero trust and least privilege. Because legacy applications and user directories are often deeply embedded, a right-sized zero trust architecture may require a hybrid approach. This brings together the best of cloud identity access management with entrenched on-premise controls, minimizing disruption for authorized users and protecting existing investments while still moving in the direction of ZTA principles.

# Core Functional Components of Zero Trust



## Abbreviations

- IdP:** Identity Provider
- EDR:** Endpoint Detection and Response
- ZT:** Zero Trust
- SOC:** Security Operations Center
- PDP:** Policy Decision Point
- PEP:** Policy Enforcement Point
- PAM:** Privilege Access Management
- SaaS:** Software-as-a-Service
- IaaS:** Infrastructure-as-a-Service
- Authn:** Authentication



## ZTA and the National Cybersecurity Strategy

In May 2021, the Executive Order on Improving the Nation’s Cybersecurity was issued, spelling out federal priorities to modernize and strengthen cybersecurity standards, improve software supply chain security, and improve response to cybersecurity incidents. A January 2022 [memorandum](#) from the Office of Management and Budget (OMB) established a requirement for all federal agencies to implement ZTA by the end of fiscal year 2024, a position reiterated by the [National Cybersecurity Strategy](#) in March 2023. The latter document states: “The OMB zero trust architecture strategy directs FCEB [federal civilian executive branch] agencies to implement multi-factor authentication, encrypt their data, gain visibility into their entire attack surface, manage authorization and access, and adopt cloud security tools.”

The implications of this policy are clear and wide-ranging for federal agencies. In addition to the ZTA target of 2024, agencies are also directed to completely eliminate non-ZTA-compliant legacy solutions within a decade.

Large commercial organizations should also heed this guidance. Although the strategy is specifically binding for federal agencies, it aims to shore up other parts of the US critical infrastructure as well. Any company materially operating in the energy, financial, or healthcare sectors should consider itself part of critical infrastructure and therefore likely to come under the scrutiny of relevant federal agencies that are themselves on a fast track to ZTA. Beginning a ZTA evolution now, rather than under active federal pressure, can promote a smoother transition—and one that can be managed on an organization’s own terms rather than the failsafe dictates of a regulatory or oversight body.

## Applying Existing Skills to Zero Trust Architecture

As with any significant evolution in process and technology, ZTA requires some upskilling and retraining to be most effective. But ZTA does not require a complete reboot or housecleaning. Many of the core practices behind zero trust represent normal cybersecurity hygiene put into sharp focus and applied with breadth and precision. Identity verification is nothing new, nor is the idea that an authorized user of one application is not necessarily entitled to access a second application. Similarly, the continuous logging of authorized user activity and the active analysis of those logs are established best practices in any setting. Security professionals who understand the importance of these practices and are interested in new ways to apply them will do well adapting to the new architecture.

One key evolution that may require retraining and rethinking is the closer alignment of access controls among the internal workforce and by external users such as partners and customers. Most organizations today consider these to be different problems, and most split ultimate responsibility for these user groups into separate tiers. This structure assumes that an employee (or more specifically, someone using an employee’s credentials) is inherently more trustworthy than an outside user.

ZTA applies greater scrutiny to all access, so governance should be merged to cover all types of users seeking access. Understanding the needs of different user audiences is still a specialized skill, but security teams will need to bridge gaps between teams to apply zero trust principles correctly for all.

Data science also grows in importance in a zero trust architecture. Developing greater analytical skills among the security team and involving data science generalists in the regular review of access and anomaly logs can help. Machine learning models may also be needed to address the ever-growing volume of suspicious and unidentified traffic seeking access. These tools can perform the brute-force analysis at high volume, leaving human experts to flag the highest risks and to recommend policy adjustments.



## Ongoing Care and Diligence in the ZTA World

Strong and sustained executive commitment from the CIO and CISO are just the start of a ZTA journey. It takes a cross-functional team of identity, networking, infrastructure, business, and application experts to create and implement a ZTA framework. A team of subject matter experts across those disciplines as well as the broader user community will need to continue collaborating in order to keep the zero trust architecture healthy and aligned. The team will also need to review capability gaps on a rolling basis.

Because ZTA is a significant departure from traditional security management, expect the transition to present substantial challenges, setbacks, and even failures. Experienced ZTA practitioners, such as those at Guidehouse, can help transition teams better respond to these setbacks, and enable users and technologists to get back on course.

The work of blending legacy systems into a zero trust architecture is not a one-time event. Each change in identity management or credential issuance may require further adjustments to support a key legacy data source or application. And keep in mind that today's cutting-edge solutions are inevitably tomorrow's legacy technology. ZTA infrastructure updates will be just as necessary as the maintenance and replacement of applications and data sources are today.

### Conclusion

By judging the context of each and every request for access, zero trust architecture puts security into its proper context: as central to the health and smooth operation of any organization. Because ZTA affects every aspect of the technology stack, it requires careful planning for smooth implementation and on-track evolution.

Guidehouse is a strong partner for ZTA initiatives, born out through significant and successful ZTA engagements with both federal agencies and large commercial entities. Our professionals are experienced in sophisticated identity access management; proficient with a wide spectrum of multi-vendor data sources, applications, and network technologies across both on-premise and cloud data centers; and possess deep expertise in cybersecurity strategy communication.


Contact Guidehouse to discuss your current readiness for zero trust and to learn more about your options.

### Contacts

Amanda Kane, Partner  
Technology Advisory  
Cybersecurity  
[amkane@guidhouse.com](mailto:amkane@guidhouse.com)

### About Guidehouse

At Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures, focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 16,500 professionals in over 55 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit [guidehouse.com](https://guidehouse.com).

 [guidehouse.com/services/cybersecurity](https://guidehouse.com/services/cybersecurity)

 [@GHTechSolutions](https://twitter.com/GHTechSolutions)

 [linkedin.com/showcase/guidhouse-technology-solutions/](https://linkedin.com/showcase/guidhouse-technology-solutions/)