Guidehouse

DC Chapter Sponsored Training

January 29 | 12:00 PM – 12:30 PM

AGA WASHINGTON D.C. CHAPTER

Guidehouse
Outwit *Complexity*

Introduction to Zero Trust Architecture

Christine Owen, Director
Advanced Solutions – Cybersecurity Team

January 2022

©2022 Guidehouse Inc. All rights reserved. Proprietary and competition sensitive. For internal use only.

Agenda

- Defining Zero Trust
- ZTA Overview
- Regulatory Requirements
- Q&A

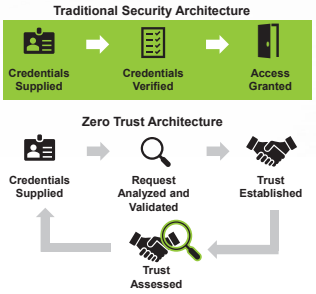
©2022 Guidehouse Inc. All rights reserved. Proprietary and competition sensitive. For internal use only.

What is Zero Trust Architecture (ZTA)?

Zero Trust is based on the idea of never trusting, always validating a user.

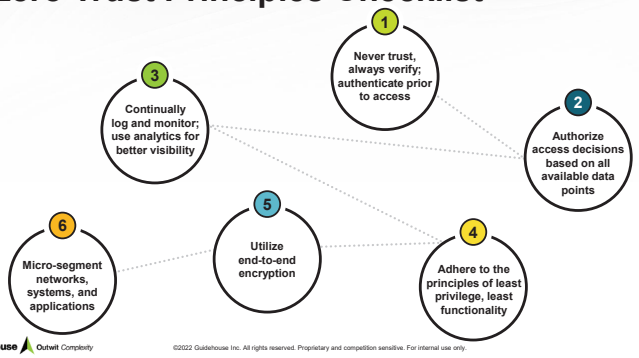
ZTA monitors the entire network by continually recording, authenticating, and verifying an identity as it accesses organizational resources.

Multiple data points throughout an organization create a detailed picture of the network, identities accessing the network, and the activities occurring on the network.



©2022 Guidehouse Inc. All rights reserved. Proprietary and competition sensitive. For internal use only.

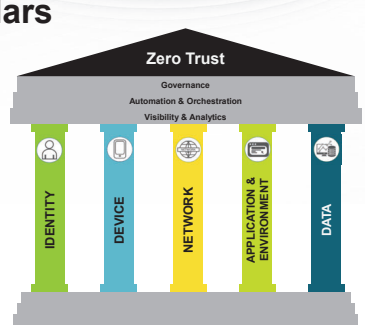
Zero Trust Principles Checklist



©2022 Guidehouse Inc. All rights reserved. Proprietary and competition sensitive. For internal use only.

CISA's Zero Trust Pillars

ZTA unifies security tools across multiple domains (Hardware, Network, Data, and Application domains) to create an active security posture within the network perimeter.



©2022 Guidehouse Inc. All rights reserved. Proprietary and competition sensitive. For internal use only.

ZTA Overview: Access Control

To supplement credentials, Access Control Policies are configured to examine the identity, device, and other attributes, such as the IP address, time of day, hardware used, and prior authorizations to create context for an access decision.

A risk assessment algorithm evaluates the user's attributes; once evaluated, a risk score is assigned. The risk score facilitates a decision, based on the amount of risk an organization will allow.

Data points such as:

- **Attribute-Based Access Control**
- **Principles of Least Privilege, Least Access**
- **Lateral Movement is Restricted**

support authorizations and credentials. Zero Trust methodology strengthens non-repudiation.

©2022 Guidehouse Inc. All rights reserved. Proprietary and competition sensitive. For internal use only.

ZTA Overview: Networks

Segmented Network

The network should be segmented into the smallest possible groupings (i.e., at the app level) or enclaves. Ideally, applications are isolated from each other. Users must be authenticated for each access request. Segmentation removes the ability for unauthorized users to laterally move throughout the systems.

End-to-End Encryption

All communication in the ZT network is encrypted, including back-end access decision communication.

©2022 Guidehouse Inc. All rights reserved. Proprietary and competition sensitive. For internal use only.

ZTA Overview: Monitoring

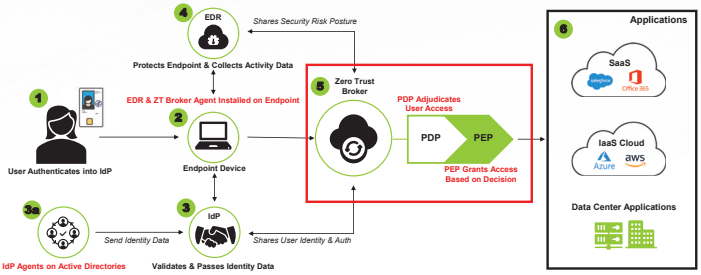
Zero Trust emphasizes enhanced security throughout the network using the principles of Observability and Monitoring.

Monitoring
Advanced automated monitoring and alerts to identify types of attacks and abuse.

Observability
Accurate and detailed information collection on **users, devices, data and applications** for analysis and prevention of unknown types of attacks.

©2022 Guidehouse Inc. All rights reserved. Proprietary and competition sensitive. For internal use only.

ZTA Overview: User Access Flow



©2022 Guidehouse Inc. All rights reserved. Proprietary and competition sensitive. For internal use only.

Zero Trust Regulatory Requirements

The recent Presidential Executive Order to improve the nation's cybersecurity infrastructure, mandated the transition traditional perimeter security to a Zero Trust security architecture.

Access to the Agency network and applications will be policy and identity-driven, while analyzing full device, user, and network health.

The OMB's draft Federal Zero Trust Strategy (the "OMB Draft") requires government agencies to achieve specific Zero Trust security goals by the end of Fiscal Year 2024.

Federal Information Security Act **(FISMA)**	Homeland Security Presidential Directive 12 **(HSPD-12)**	Federal Information Processing Standard **(FIPS 201)**	National Institute of Standards and Technology **(NIST)**
FISMA mandates that all federal agencies maintain a level of security for their information systems proportional to the system or data's level of sensitivity as well as adhere to NIST standards	HSPD-12 dictates the common identification standards required for all federal employees and contractors which uses smart card credentialing to secure access to federal facilities and resources	FIPS 201 outlines the Personal Identity Verification (PIV) standards for federal employees and contractors including identity credentials, physical smart card, and interfaces	NIST provides the cybersecurity standards and best practices for federal agencies to apply based on federal policies and executive orders

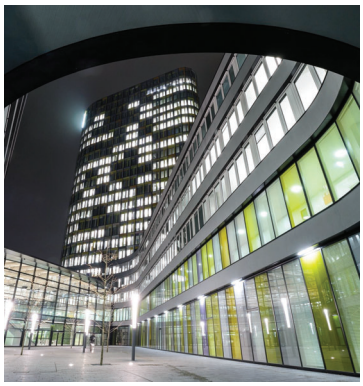
©2022 Guidehouse Inc. All rights reserved. Proprietary and competition sensitive. For internal use only.

Zero Trust Additional Materials

- DOD Zero Trust Reference Architecture
- OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credentialing, and Access Management
- OMB M-19-18, Federal Data Strategy – A Framework for Consistency
- NIST SP 800-162, Attribute Based Authentication Controls (ABAC)
- NIST SP 800-63, Digital Identities Guidelines
- NIST SP 800-37, Risk Management Framework for Information Systems and Organizations
- NIST SP 800-207, Zero Trust Architecture

©2022 Guidehouse Inc. All rights reserved. Proprietary and competition sensitive. For internal use only.

Questions



©2022 Guidehouse Inc. All rights reserved. Proprietary and competition sensitive. For internal use only.

Your Cybersecurity Guides

Christine C. Owen
Director, Advanced Solutions
cowen@guidehouse.com
(202) 294-6029

Amanda Kane
Director, Advanced Solutions
amkane@guidehouse.com
(703) 772-4242

Marianne Bailey
Partner, Advanced Solutions
mbailey@guidehouse.com
(443) 535-1698

Guidehouse
Outwit Complexity

©2022 Guidehouse Inc. All rights reserved. Proprietary and competition sensitive.
This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.