NIST SPECIAL PUBLICATION 1800-35A

Implementing a Zero Trust Architecture

Volume A:
Executive Summary

Alper Kerman
Murugiah Souppaya
National Institute of Standards and Technology
Gaithersburg, Maryland

Parisa Grayeli
Susan Symington
The MITRE Corporation
McLean, Virginia

December 2022

SECOND PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

As enterprise data and resources become distributed across on-premises environments and multiple clouds, protecting them has become increasingly challenging. Many users need access from anywhere, at any time, from any device to support the organization's mission. Data is created, stored, transmitted, and processed across different organizations' environments, which are distributed across on-premises and multiple clouds to meet ever-evolving business use cases. It is no longer feasible to simply protect data and resources at the perimeter of the enterprise environment or to assume that all users, devices, applications, and services within it can be trusted.

A zero-trust architecture (ZTA) enables secure authorized access to assets—machines, applications and services running on them, and associated data and resources—whether located on-premises or in the cloud, for a hybrid workforce and partners based on an organization's defined access policy. For each access request, ZTA explicitly verifies the context available at access time—this includes both static user profile information or non-person entity information such as the requester's identity and role; and dynamic information such as geolocation, the requesting device's health and credentials, the sensitivity of the resource, access pattern anomalies, and whether the request is warranted and in accordance with the organization's business process logic. If the defined policy is met, a secure session is created to protect all information transferred to and from the resource. A real-time, risk-based assessment of resource access and access pattern anomaly detection with continuous policy evaluation are performed to establish and maintain the access. A ZTA can also protect organizations from non-organizational resources that their users and applications may connect to, helping to stop threats originating from outside of the organization's control.

This guide summarizes how the National Cybersecurity Center of Excellence (NCCoE) and its collaborators are using commercially available technology to build interoperable, open standards-based ZTA implementations that align to the concepts and principles in NIST Special Publication (SP) 800-207, *Zero Trust Architecture* to protect conventional, general-purpose enterprise information technology (IT) infrastructure. As the project progresses, this second preliminary draft will be updated, and additional volumes will also be released for comment.

CHALLENGE

Organizations would like to adopt a ZTA, but they have been facing some challenges which may include:

- Lack of adequate asset inventory and management needed to fully understand the business applications, assets, and processes that need to be protected, with no clear understanding of the criticality of these resources
- Lack of adequate digital definition, management, and tracking of user roles across the organization needed to enforce fine-grained, need-to-know access policy for specific applications and services
- Ever-increasing complexity of communication flows and distributed IT components across the environments on-premises and in the cloud, making them difficult to manage consistently
- Lack of visibility of the organization's communications and usage patterns—limited understanding of the transactions that occur between an organization's subjects, assets,

applications, and services, and absence of the data necessary to identify these communications and their specific flows

- Lack of awareness regarding everything that encompasses the organization's entire attack surface. Organizations can usually address threats with traditional security tools in the layers that they currently manage and maintain such as networks and applications, but elements of a ZTA may extend beyond their normal purview. False assumptions are often made in understanding the health of a device as well as its exposure to supply chain risks.
- Lack of understanding regarding what interoperability issues may be involved or what additional skills and training administrators, security personnel, operators, end users, and policy decision makers may require; lack of resources to develop necessary policies and a pilot or proof-of-concept implementation needed to inform a transition plan
- Leveraging existing investments and balancing priorities while making progress toward a ZTA via modernization initiatives
- Integrating various types of commercially available technologies of varying maturities, assessing capabilities, and identifying technology gaps to build a complete ZTA
- Concern that ZTA might negatively impact the operation of the environment or end-user experience
- Lack of a standardized policy to distribute, manage, and enforce security policy, causing organizations to face either a fragmentary policy environment or non-interoperable components
- Lack of common understanding and language of ZTA across the community and within the organization, gauging the organization's ZTA maturity, determining which ZTA approach is most suitable for the business, and developing an implementation plan
- Perception that ZTA is suited only for large organizations and requires significant investment rather than understanding that ZTA is a set of guiding principles suitable for organizations of any size
- There is not a single ZTA that fits all. ZTAs need to be designed and integrated for each organization based on the organization's requirements and risk tolerance, as well as its existing invested technologies and environments.

OUTCOME

The outcome of this project is to develop example solutions, demonstrate them to support various scenarios, and publish the findings in this practice guide, a NIST SP 1800 that is composed of multiple volumes targeting different audiences.

This second preliminary practice guide can help your organization:

- **Develop an implementation plan and identify milestones for gradually integrating ZTA into your environment,** based on the demonstrated examples and using a risk-based approach, to:
  - **Support user access to resources** regardless of user location or user device (managed or unmanaged)

- **Protect business assets and processes regardless of their location** (on-premises or cloud-based)
- **Limit the insider threat** (insiders—both users and non-person entities—are not automatically trusted)
- **Limit breaches** (reduce attackers' ability to move laterally in the environment)
- **Protect sensitive corporate information** with data security solutions
- **Improve visibility** into the inventory of resources, what configurations and controls are implemented, all communications and their specific flows, and how resources are accessed and protected, and then use this understanding to formulate and enforce a useful and complete security policy
- **Perform real-time and continuous monitoring and logging, and policy-driven, risk-based assessment and enforcement** of resource access

SOLUTION

The NCCoE is collaborating with ZTA technology providers to build several example ZTA solutions and demonstrate their ability to meet the tenets of ZTA described in NIST SP 800-207. The goal of the solutions is to enforce corporate security policy dynamically and in near-real-time to restrict access to authenticated, authorized users, devices, and non-person entities while flexibly supporting a complex set of diverse business outcomes involving both remote and on-premises workforces, use of the cloud, partner collaboration, and support for contractors. The example solutions are designed to demonstrate the ability to protect against and detect attacks and malicious insiders. They showcase the ability of ZTA products to interoperate with existing enterprise and cloud technologies while trying to minimize impact on end-user experience.

The project can help organizations plan how to evolve their existing enterprise environments to ZTA, starting with an assessment of their current resources, strengths, and weaknesses, and setting milestones along a path of continuous improvement, gradually bringing them closer to achieving the ZTA goals they have prioritized based on risk, cost, resources, and their unique mission. The goal is to enable organizations to thoughtfully apply ZTA controls that best protect their business while enabling them to operate as they need to. We are using a phased approach to develop example ZTA solutions that is designed to represent how we believe most enterprises will evolve their enterprise architecture toward ZTA, i.e., by starting with their already-existing enterprise environment and gradually adding or adapting capabilities. Our first implementations focus on the enhanced identity governance (EIG) deployment because EIG is seen as the foundational component of ZTA. The identity-based controls provided by EIG are needed to secure and monitor administrative access to the ZTA infrastructure itself. Our EIG implementations use the identity of subjects and device health as the main determinants of access policy decisions, and we provide support for device discovery and protecting access to cloud-based resources.

Depending on the current state of identity management in the enterprise, deploying EIG solutions is an initial key step that may be enhanced with the addition of identity protection solutions to monitor for identity compromise or misuse and that will be leveraged to support micro-segmentation and software-defined perimeter (SDP) deployment approaches. The remaining deployment models will be covered in the later phases of the project. Our strategy is to follow an agile implementation methodology to build everything iteratively and incrementally while adapting or adding more capabilities to evolve to a complete ZTA. We started with the minimum viable EIG solution that allowed us to achieve some level of ZTA, and then began gradually deploying additional functional components and capabilities to address an increasing number of ZTA requirements, progressing the project toward demonstration of more robust micro-segmentation, SDP, or holistic deployment options.

Collaborators

- Appgate
- AWS
- Broadcom Software
- Cisco
- DigiCert
- F5
- Forescout
- Google Cloud
- IBM
- Ivanti
- Lookout
- Mandiant
- Microsoft
- Okta
- Palo Alto Networks
- PC Matic
- Ping Identity
- Radiant Logic
- SailPoint
- Tenable
- Trellix
- VMware
- Zimperium
- Zscaler

While the NCCoE is using a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Business decision makers, including chief information security and technology officers can use this part of the guide, *NIST SP 1800-35A: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-35B: Approach, Architecture, and Security Characteristics*, which describes what we built and why. Also, *NIST SP 1800-35E: Risk and Compliance Management,* maps logical components of the general ZTA reference design to security characteristics listed in various cybersecurity guidelines and recommended practices documents.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-35C: How-To Guides,* which provides critical steps for product installation, configuration, and integration instructions for building this project's example implementations, allowing them to be replicated in whole or in part. Also, you can use *NIST SP 1800-35D*: *Functional Demonstrations,* which provides the use cases that have been defined to showcase ZTA security capabilities and the results of demonstrating them with each of the example implementations.

SHARE YOUR FEEDBACK

You can view or download the second preliminary draft guide at the NCCoE ZTA project page. NIST is adopting an agile process to publish this content. Each volume is being made available as soon as possible rather than delaying release until all volumes are completed. Work continues on implementing the example solutions and developing other parts of the content. As a second preliminary draft, this volume is subject to additional draft releases that will be made available for public comment.

Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. As example implementations continue to be developed, you can adopt this solution for your own organization. If you do, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and recommended practices for transforming the processes associated with implementing this guide.

To provide comments, join the community of interest, or learn more by arranging a demonstration of these example implementations, contact the NCCoE at nccoe-zta-project@list.nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.