

NIST SPECIAL PUBLICATION 1800-35A

Implementing a Zero Trust Architecture

Volume A:
Executive Summary

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

Dr. Parisa Grayeli
Susan Symington
The MITRE Corporation
McLean, Virginia

June 2022

PRELIMINARY DRAFT

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



1 Executive Summary

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

9 A zero-trust architecture (ZTA) enables secure authorized access to each individual resource, whether
10 located on-premises or in the cloud, for a hybrid workforce and partners based on an organization's
11 defined access policy. For each access request, ZTA explicitly verifies the context available at access
12 time—this includes the requester's identity and role, the requesting device's health and credentials, and
13 the sensitivity of the resource. If the defined policy is met, a secure session is created to protect all
14 information transferred to and from the resource. A real-time and continuous policy-driven, risk-based
15 assessment is performed to establish and maintain the access.

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

21 CHALLENGE

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

- 23 ▪ Leveraging existing investments and balancing priorities while making progress toward a ZTA
- 24 ▪ ZTA deployment requiring leveraging integration of many deployed existing technologies of
25 varying maturities and identifying technology gaps to build a complete ZTA
- 26 ▪ Concern that ZTA might negatively impact the operation of the environment or end-user
27 experience
- 28 ▪ Lack of common understanding of ZTA across the organization, gauging the organization's ZTA
29 maturity, determining which ZTA approach is most suitable for the business, and developing an
30 implementation plan

This preliminary practice guide can help your organization:

- **Identify milestones for gradually integrating ZTA into your environment**, based on the demonstrated examples and using a risk-based approach, to:
 - **Support teleworkers** with access to resources regardless of user location or user device (managed or unmanaged)
 - **Protect resources regardless of their location** (on-premises or cloud-based)
 - **Limit the insider threat** (insiders are not automatically trusted)

This preliminary practice guide can help your organization:

- **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, and how resources are accessed and protected
- **Real-time and continuous policy-driven, risk-based assessment of resource access**

31 SOLUTION

32 NCCoE is collaborating with ZTA technology providers to build several example ZTA solutions and
 33 demonstrate their ability to meet the tenets of ZTA. The solutions will enforce corporate security policy
 34 dynamically and in near-real-time to restrict access to authenticated, authorized users and devices while
 35 flexibly supporting a complex set of diverse business use cases involving a remote workforce, use of the
 36 cloud, partner collaboration, and support for contractors. The example solutions are designed to
 37 demonstrate the ability to protect against and detect attacks and malicious insiders. They showcase the
 38 ability of ZTA products to interoperate with existing enterprise and cloud technologies with only minimal
 39 impact on end-user experience.

40 The project can help organizations plan how to evolve their existing enterprise environments to ZTA,
 41 starting with an assessment of their current resources and setting milestones along a path of continuous
 42 improvement, gradually bringing them closer to achieving the ZTA goals they have prioritized based on
 43 risk, cost, and resources. We are using a phased approach to develop example ZTA solutions that is
 44 designed to represent how we believe most enterprises will evolve their enterprise architecture toward
 45 ZTA, i.e., by starting with their already-existing enterprise environment and gradually adding or adapting
 46 capabilities. Our first implementations are crawl versions of the enhanced identity governance (EIG)
 47 deployment because EIG is seen as the foundational component of the other deployment approaches
 48 utilized in today's hybrid environments. Our initial EIG implementations use the identity of subjects and
 49 device health as the main determinants of access policy decisions.

50 Depending on the current state of identity management in the enterprise, deploying EIG solutions is an
 51 initial key step that will be leveraged to support micro-segmentation and software-defined perimeter
 52 (SDP) deployment approaches, which will be covered in the later phases of the project. Our strategy is to
 53 follow an agile implementation methodology to build everything iteratively and incrementally while
 54 adapting or adding more capabilities to evolve to a complete ZTA. We are starting with the minimum
 55 viable EIG solution that allows us to achieve some level of ZTA, and then we will gradually deploy
 56 additional functional components and features to address an increasing number of ZTA requirements,
 57 progressing the project toward demonstration of more robust micro-segmentation and SDP deployment
 58 options.

Collaborators

Appgate
AWS

IBM
Ivanti

Ping Identity
Radiant Logic

Collaborators		
Broadcom Software	Lookout	SailPoint
Cisco	Mandiant	Tenable
DigiCert	Microsoft	Trellix
F5	Okta	VMware
ForeScout	Palo Alto Networks	Zimmerium
Google Cloud	PC Matic	Zscaler

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

65 HOW TO USE THIS GUIDE

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

70 **Technology, security, and privacy program managers** who are concerned with how to identify,
 71 understand, assess, and mitigate risk can use *NIST SP 1800-35B: Approach, Architecture, and Security*
 72 *Characteristics* once it is available. It will describe what we built and why, including the risk analysis
 73 performed and the security/privacy control mappings.

74 **IT professionals** who want to implement an approach like this can make use of *NIST SP 1800-35C: How-*
 75 *To Guides* once it is available. It will provide specific product installation, configuration, and integration
 76 instructions for building this project's example implementations, allowing them to be replicated in
 77 whole or in part.

78 SHARE YOUR FEEDBACK

79 You can view or download the preliminary draft guide at the [NCCoE ZTA project page](#). NIST is adopting
 80 an agile process to publish this content. Each volume is being made available as soon as possible rather
 81 than delaying release until all volumes are completed. Work continues on implementing the example
 82 solution and developing other parts of the content. As a preliminary draft, this volume will have at least
 83 one additional draft released for public comment before it is finalized.

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

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

91 **COLLABORATORS**

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

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