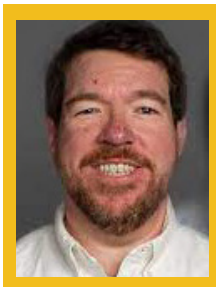
# NIST Q&A on Zero Trust

Scott Rose, NIST's Zero Trust subject matter expert, answers some common questions about Zero Trust.

**Scott Rose**
Computer Scientist, Information Technology Lab
National Institutes of Standard and Technology (NIST)



Zero Trust refers to an evolving set of security paradigms that narrows defenses from wide network perimeters to individual or small groups of resources. Its focus on protecting resources rather than network segments is a response to enterprise tends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary.

ZTA strategies are already present in current federal cybersecurity policies and programs, though the document includes a gap analysis of areas where more research and standardization are needed to aid agencies in developing and implementing ZTA strategies. Additionally, this document establishes an abstract definition of Zero Trust and ZTA as well as general deployment models, use cases where ZTA could improve an enterprise's overall IT security posture, and a high-level roadmap to implementing a ZTA approach for an enterprise. (Source: NIST)

**Q.** *Zero Trust is a journey and can be a complex process for many organizations, especially the smaller ones. If an organization is beginning this journey, what's your advice about how best to get started and what are some of the first steps to take that make the best impact up front?*

**A.** **Scott Rose:** The first, and possibly biggest step an organization takes when migrating to a Zero Trust architecture is cultural in nature. Organizations need to understand their core business processes and the risks associated with those processes. This is where an organization's security planners, workflow owners, and resource owners need to work together to conduct a comprehensive risk analysis. This comprehensive risk analysis relies on cybersecurity teams and operation teams working together to discover, audit, and monitor all aspects of the organization: identities, data, assets and data flows. A successful migration to Zero Trust requires cooperation and communication from all components in the organization. Unfortunately, just relying on documentation is often not enough as there is often a separate "oral history" and tacit knowledge of infrastructure operations that is not written down. Any cultural stovepipes between security teams and administrators and operators need to be broken down because Zero Trust relies on communication between these teams to succeed.

This knowledge of the organization needs to include monitoring current activity as well. Any audit of an organization's resources will become out of date quickly unless it includes a continuous monitoring program. Zero Trust relies on having robust monitoring in place to react quickly to changing network

Zero Trust relies on having robust monitoring in place to react quickly to changing network conditions or newly discovered threats.

conditions or newly discovered threats. Many attacks could be quickly identified and mitigated it they are discovered in the early phase of infiltration and before the exploitation phase.

Zero Trust cannot be "bolted on" to an existing IT infrastructure, but also requires a change in how cybersecurity is discussed in the organization. Simply adding common Zero Trust elements such multifactor authentication or microsegmentation will not result in a Zero Trust enterprise if the policies used to deploy and operate these elements are not updated.

**Q.** *NIST is famous for its Cyber Security Framework and the collaborative way that NIST reached out to partners across government, industry, academia and non-profits in order to develop a solid framework that is nationally and internationally recognized and accepted as the gold standard. How can the same set of organizations get involved in order to make this Zero Trust effort just as collaborative and inclusive?*

**A.** **Scott Rose:** The tenets described in NIST SP 800-207 are a conceptual framework and are slightly different than the Cyber Security Framework (CSF). The tenets are meant to be a set of guiding principles used with tools such as the CSF or the NIST Risk Management Framework to develop and implement an IT security architecture. The concepts in NIST SP 800-207 will shape future deeper dives into specific facets of Zero Trust like identity governance, internet of things (IoT) deployments in a Zero Trust enterprise, etc.

These future works will follow the usual process of NIST consulting with, and soliciting comments from, the public and private sectors and other stakeholders. Some of this work may add to or refine the existing tenets to support a specific use case or industry need. These improvements may feed a revision of SP 800-207. The Special Publication is seen as the initial work. We anticipate further refinement and improvement as the community learns more about the challenges and opportunities surrounding implementing Zero Trust architectures.

**Q.** *How is the National Cybersecurity Center of Excellence going to be involved in the Zero Trust effort and how can organizations gain awareness and insight into what's happening there? How can organizations get involved?*

**A.** **Scott Rose:** The National Cybersecurity Center of Excellence (NCCoE) is currently starting a project in policy-based resource access in a Zero Trust architecture. The project will demonstrate example implementations of a Zero Trust architecture using vendor technology designed using the approaches and models described in NIST SP 800-207. The abstract architecture in NIST SP 800-207 was used to describe the functional component requirements that can be satisfied using commercially available and open source products. The project Zero Trust Architecture builds will be used to perform a set of scenarios of resource access (e.g., employee access to resources, remote employee access to resources) The lessons learned from the builds and example implementations will be documented and used to identify areas for further work and refinement of Zero Trust definitions and concepts.

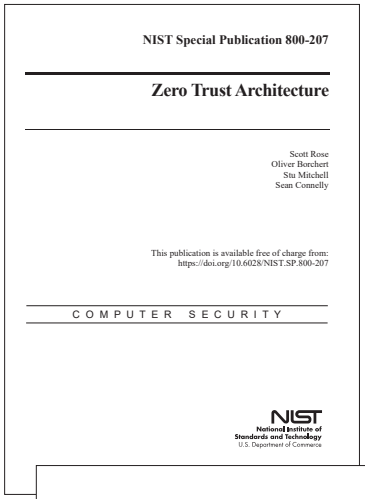
Vendor collaborators for the current NCCoE Zero Trust project have been selected and announced on the NCCoE's ZTA page (see https://www.nccoe.nist.gov/zerotrust for more information). However, there are other ways for individuals and organizations to get involved and stay informed such as joining the NCCoE Zero Trust Architecture community of interest. The community of interest is how the project will communicate updates about the project as well as announcements about NCCoE events or work related

*Continued on page 46*

## NIST Talks Zero Trust

*Continued from page 9*

to zero trust. There is also an email address on the NCCoE project page that can be used to send feedback to the project team. This address as well as information about the community of interest are both listed on the NCCoE ZTA project page.


NIST Special Publication 800-207

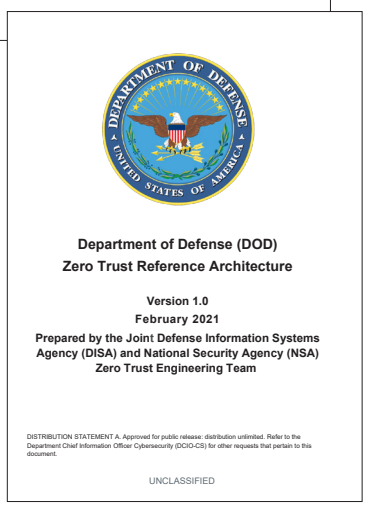
Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce


Department of Defense (DOD)
Zero Trust Reference Architecture

Version 1.0
February 2021
Prepared by the Joint Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. Refer to the Department Chief Information Officer Cybersecurity (DCIO-CS) for other requests that pertain to this document.

UNCLASSIFIED

**Q.** *We understand NIST's core and functional components of Zero Trust. How would you assess the state of the art in terms of where each component stands today? Which components are more advanced and which ones need more development in order to achieve the desired capabilities?*

**A.** **Scott Rose:** Of all the functional components described in NIST SP 800-207, the policy engine component will likely see the greatest advancement in functionality. As Zero Trust sees wider deployment and experience, we anticipate improvements in how the policy engine uses information about the organization and environment to make access request decisions. We are also seeing the start of how machine learning and artificial intelligence can be applied to the work of the policy engine and how these technologies can be used to automate cybersecurity policy checks, enforcement, and responses. As technology advances, the policy engine may become a partner to the human administrators of the organization's infrastructure more than just a tool used to operate the infrastructure.

We also may see new standards or protocols for the communication between functional components. One of the concerns we frequently heard from agencies was the risk of vendor "lock-in" based on a specific technology. There was the desire for a more "open" Zero Trust based on an open set of standards that would allow policy engines, policy administrators and policy enforcement points from different vendors to work together in a single solution or as a federated deployment in a coalition. This is not possible with a single protocol but will likely be some sort of framework using various standards that would allow for interoperability between components and between components and information feeds (e.g., logs, threat intelligence, etc.). ■

ON THE FrontLines MAGAZINE

TREZZA Media Group
Connecting Partners Through Mindshare Media

Publisher
**Tom Trezza Jr.**
President
Trezza Media Group
3101-So. Ocean Drive Unit 1803
Hollywood, Fl. 33019
ttrezza@trezzamediagroup.com
201-757-7405

Public Sector COMMUNICATIONS

Editor
**Jeff Erlichman**
Managing Partner
Public Sector Communications
Louisville, CO
djerlichman@comcast.net

Art Direction
**Reuter & Associates**, bill@reuter.net