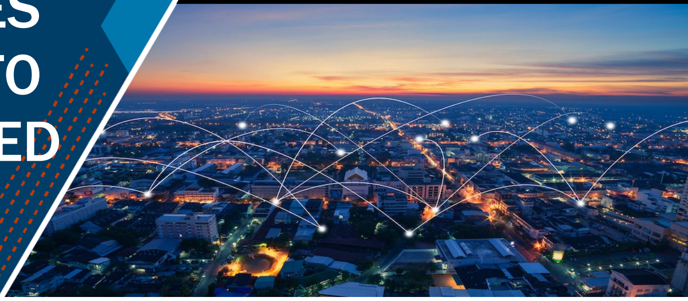
CONNECTED COMMUNITIES GUIDANCE: ZERO TRUST TO PROTECT INTERCONNECTED SYSTEMS



OVERVIEW

Increasingly, localities in the United States are implementing smart, emerging, and connected technologies across critical infrastructure sectors, seeking cost-savings and enhanced quality-of-life for their citizens. These localities, otherwise known as connected communities or "smart cities," are urban, suburban, and rural government entities that utilize a confluence of several technological applications such as cloud computing, Internet of Things, and artificial intelligence. Connected communities use these technologies to interconnect infrastructure systems to provide more efficient, innovative, and sustainable services.

> *"In today's interconnected society, our Nation faces a wide array of serious risks from many threats, all with the potential for significant consequences that can impact our critical national functions. These functions are built as "systems of systems" with complex designs, numerous interdependencies, and inherent risks."* – CISA Director Jen Easterly's April 2023 testimony *"CISA 2025: The State of American Cybersecurity from CISA's Perspective"*

The process of securing critical infrastructure in connected communities requires addressing more technology types across sectors, ranging from energy to clean water and even emergency services. As a result of the increased interconnectedness within connected communities, traditional perimeter-based security measures are no longer sufficient to protect networks from intrusion and secure critical infrastructure data.

Multiple U.S. government agencies have developed frameworks and strategies to apply zero trust principles across federal networks. However, there is a lack of guidance for State, Local, Tribal, and Territorial (SLTT) governments, specifically within connected communities. The purpose of this document is to explain the concept of zero trust as an effective approach to protect interconnected critical infrastructure systems within connected communities.

RISKS TO CONNECTED COMMUNITIES AND INTERCONNECTED SYSTEMS

Connected communities may create safer, more efficient, resilient communities through technological innovation and data-driven decision-making; however, the integration of smart technologies also introduces potential vulnerabilities that, if exploited, could impact economic security, public health and safety, and critical infrastructure operations. Cyber threat activity against operational technology (OT) systems is increasing globally, and the interconnection between OT systems and smart city infrastructure increases the attack surface and heightens the potential consequences of compromise across these environments.[1]

Connected communities are an attractive target for criminals and cyber threat actors to exploit vulnerable systems to steal critical infrastructure data and proprietary information, conduct ransomware operations, or launch destructive cyberattacks. Successful cyberattacks against smart cities could lead to disruption of infrastructure services, significant financial losses, exposure of citizens' private data, erosion of citizens' trust in the smart systems themselves, and physical impacts to infrastructure that could cause physical harm or loss of life.[2]

[1] Cybersecurity Best Practices for Smart Cities. April 2023. https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf.
[2] Ibid.

Additionally, as connected communities continue integrating more systems and increasing connectivity between networks, network administrators and security personnel may lose visibility into collective system risks. With the emergence of hybrid workforces and accelerating cloud migration, applications and users are becoming decentralized with users expecting access from any location on any device. This potential loss of visibility also includes components owned and operated by vendors providing their infrastructure as a service to support integration.[3] The implied trust of years past, in which being physically present in an office provided some measure of user authentication, can no longer be sustained. Interconnected systems bring to bear a level of complexity that requires a higher level of security that is applied consistently across all network environments and user interactions.

The increased use of smart city technologies—including big data, cloud computing, and sensors that inform city operations—creates new attack opportunities for adversarial state and non-state cyber actors to gain access to or carry out disruptive attacks against local government and critical infrastructure networks. For more from the Homeland Threat Assessment 2024, visit https://www.dhs.gov/publication/homeland-threat-assessment.

ZERO TRUST FOR INTERCONNECTED SYSTEMS

What is Zero Trust?

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 provides the following definitions for zero trust and zero trust architecture (ZTA):[4]

Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

ZTA is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies.

NIST's SP 800-207 also outlines seven basic tenets of zero trust and ZTA:[5]

- All data sources and computing services are considered resources.
- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy—including the observable state of client identity, application/services, and the request asset—and may include other behavioral and environmental attributes.
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
- The enterprise collects information about the current state of assets, network infrastructure and communications, and uses it to improve its security posture.

[3] Cybersecurity Best Practices for Smart Cities. April 2023. https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf.
[4] NIST SP 800-207: Zero Trust Architecture. August 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.
[5] Ibid.

NIST emphasizes that the goal of zero trust is to, "prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible."[6] Similarly, the National Security Telecommunications Advisory Committee (NSTAC) describes zero trust as, "a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur, and therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be continually verified."[7] Every access request must be evaluated in real time based on access policies and the current state of credentials, device, application, and service, as well as other observable behavior and environmental attributes before access may be granted.[8]

CISA's Zero Trust Maturity Model (ZTMM), which serves as an industry-backed approach for zero trust implementation, provides additional context to NIST's zero trust tenets. CISA describes five pillars that entities should account for when adopting zero trust principles: devices, networks, applications, workloads, and data. The model also introduces the following cross-cutting capabilities that support the interoperability of the pillars, namely: visibility and analytics; automation and orchestration; and governance. CISA's ZTMM is one of many paths to support the transition to zero trust.[9]

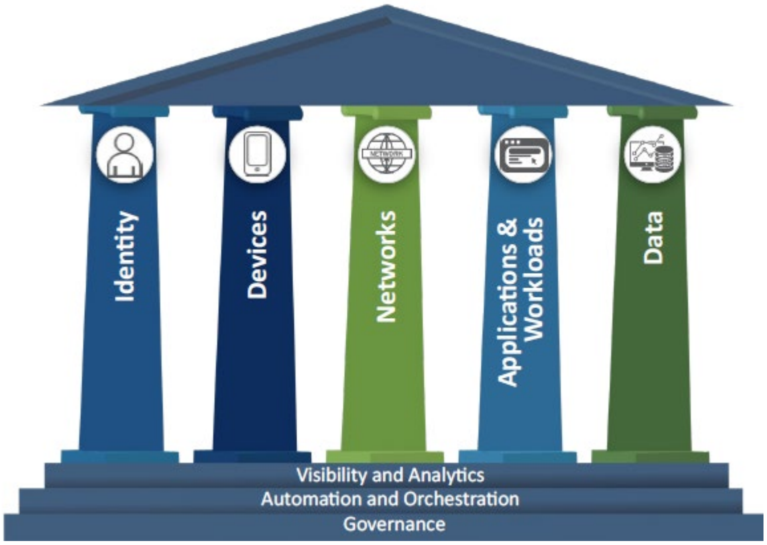
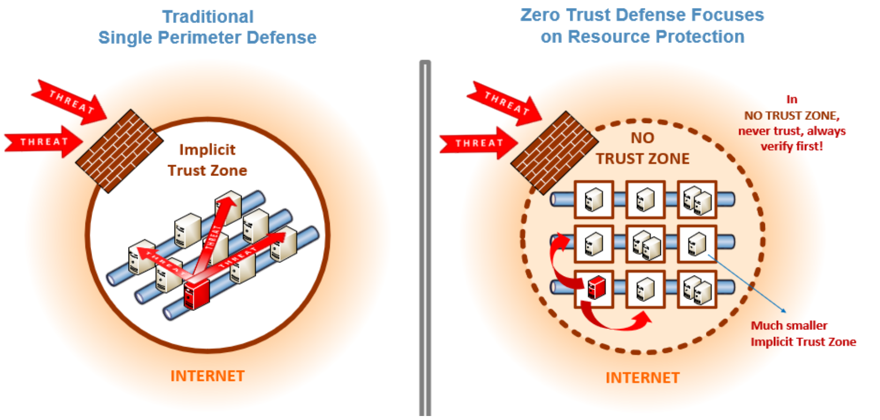


Figure 1: **Zero Trust Maturity Model Pillars**

Essentially, zero trust presents a shift from a location-centric model to an identity, context, and data-centric approach with fine-tuned security controls between users, systems, applications, data, and assets that change over time. While significant, this shift from location-centric to data-centric provides the visibility needed to support the development, implementation, enforcement, and evolution of security policies necessary to protect interconnected critical infrastructure systems.[10]

[6] NIST SP 800-207: Zero Trust Architecture. August 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.
[7] The President's National Security Telecommunications Advisory Committee. Report to the President on Zero Trust and Identity Management. February 2022. https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf.
[8] Zero Trust Cybersecurity: 'Never Trust, Always Verify.' October 2020. https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify.
[9] Zero Trust Maturity Model 2.0. April 2023. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.
[10] Ibid.

Why Zero Trust?



A zero trust approach, at its most basic level, is centered on eliminating implied trust and increasing authentication. Zero trust authentication, such as the principle of least privilege, can be an effective tool for municipalities implementing smart, emerging, and connected technologies to limit risk within interconnected critical infrastructure environments. Connected communities should utilize a holistic approach by applying zero trust concepts across interconnected systems. This includes ensuring that each user be authenticated, every access request be validated, and all activities be continuously monitored to mitigate the risks associated with an expanded attack surface.

Zero trust is more than just “locking things down” as it also provides connected communities with a framework for providing consistent security across interconnected systems and a homogenous experience for users wherever they are. Whether a user is at home, a coffee shop, or in the office, their access is treated in a uniform manner from a security and risk perspective.

Zero trust concepts can also be applied to more than the users themselves. The principles can be applied to cloud workloads and infrastructure components like OT devices and network nodes. Continuous monitoring and authentication of devices provide additional controls with the zero trust model. The elevated scrutiny of users and devices is a critical security control mechanism that prevents lateral movement across interconnected systems by malicious actors.[11]

RECOMMENDATIONS FOR CONNECTED COMMUNITIES

Zero trust design principles create a more secure network environment that requires authentication and authorization for each new connection with a layered, defense-in-depth approach to security. However, the path to zero trust is an incremental process that may take years to fully implement. It is important to understand that zero trust is no singular product or application; rather, zero trust is a journey that connected communities need to take and maintain. Going from a traditional network architecture to zero trust, especially those with interconnected critical infrastructure systems, is not going to be a “one-and-done” effort.

The zero trust principles detailed below can provide connected communities with a framework of essential activities to achieve greater visibility into network activity, trend identification through analytics, issue resolution through automation and orchestration, and more efficient network security governance.[12] Connected communities should consider the following:

- **Create an asset inventory:** An asset inventory establishes a visibility baseline for all assets on a given network. When developing the inventory, connected communities should prioritize high-risk and high-exposure assets, particularly new devices, including but not limited to, “bring your own devices” (BYODs). BYODs include personal smartphones, laptops, MiFi devices, and tablets employees use to access an organization’s network.
    - NIST SP 1800-5 – IT Asset Management provides more information on how connected communities can create or augment their asset inventory.

[11] Zero Trust Cybersecurity: ‘Never Trust, Always Verify.’ October 2020. https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify.
[12] Cybersecurity Best Practices for Smart Cities. April 2023. https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf.

- **Control access to data**: Ensure multi-factor authentication (MFA) policies are up-to-date, apply MFA multiple times during any single session, and add access controls around the most sensitive data. With zero trust, users should only access what they are supposed to access and nothing more. Connected communities must enforce the zero trust principle of least privilege and deploy authentication mechanisms to consider both identity and context.
  - For more information on MFA and authentication best practices, please refer to CISA's Capacity Enhancement Guide: Implementing Strong Authentication, NSA's Cybersecurity Information on Selecting Secure Multi-factor Authentication Solutions, and NIST SP 800-63B – Digital Identity Guidelines: Authentication and Lifecycle Management.
- **Assess security protocols**: Create and implement policies governing who has access to what data, when, and clearly define the processes to ensure compliance. Zero trust principles reinforce the practice of integrating security through the entire cybersecurity lifecycle process.
  - For additional best practices to protect interconnected systems, see CISA's Cybersecurity Advisory *Weak Security Controls and Practices Routinely Exploited for Initial Access*.
- **Network segmentation**: Zero trust encourages the practice of micro-segmentation. Connected communities should segment networks into subnetworks to create smaller, more manageable surfaces to protect. Should a malicious actor gain access, micro-segmentation helps to minimize lateral movement, contains the threat, and restricts malware from spreading across the entire environment.
  - CISA's Layering Network Security Through Segmentation infographic illustrates the level of effort needed for attackers to breach and navigate an unsegmented network versus a highly segmented network. NIST explains the "building blocks" of network segmentation in their Cybersecurity White Paper (CSWP) 28 – Security Segmentation in a Small Manufacturing Environment.
- **Sustain and streamline resourcing efforts**: Connected communities should establish consistent budget line items for long-term refreshes of hardware and software and replace legacy systems. It is important to consider technical debt, or reliance on legacy technology, and develop ZTA from the ground up. Layering security on top will likely do more harm, introduce additional security misconfigurations or vulnerabilities, and create greater complexities for effectively managing security.
  - For more information on system life cycle and risk management processes, please see NIST SP 800-160 Vol. 2 Rev. 1 - Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.
- **Identify and prioritize low-user impact security enhancements to gain early buy-in:** Disrupting users' day-to-day experience is the fastest way to nullify a zero trust transition. Thus, connected communities should prioritize efforts that clearly benefit the workforce and can be easily accomplished to maximize buy-in and commitment for a comprehensive ZTA. When ZTA is deployed properly, authentication and access will be seamless, and users will be more likely to embrace zero trust.
  - The Information Systems Audit and Control Association (ISACA) developed their Top Management Considerations for Zero Trust, which includes additional information on strategic implementation, end-user training, and change management.
- **Centralized visibility and orchestration:** Implement security orchestration to connect different technologies, bridge visibility gaps, and automate repetitive tasks required for authenticating users at multiple access levels.[13]
  - CISA's Orchestration of Information Technology Automation Frameworks White Paper provides organizations with more information on how Security Orchestration, Automation, and Response (SOAR) and IT Automation frameworks combine to mitigate cyber risks.

For more information or to seek additional help, contact us at Connected.Communities@CISA.DHS.GOV.

[13] "Never Trust, Always Verify": Federal Migration to ZTA and Endpoint Security. June 2022. https://www.csis.org/analysis/never-trust-always-verify-federal-migration-zta-and-endpoint-security.