SECURITY INFOWATCH.COM

ACCESS & IDENTITY

What Zero Trust Means for Physical Security Systems

Embracing Zero Trust is not just a cybersecurity imperative but a fundamental guide for the safeguarding of physical assets

Jason Beers, Jeremy Freeze-Skret

Forrester Research analyst John Kindervag may have popularized the term in 2010, but Zero Trust in cybersecurity has existed since the 1990s. Fast-forward to today, faced with persistent and growing cyber threats, President Joe Biden issued the Executive Order on Improving the Nation's Cybersecurity in May 2021, effectively shifting U.S. government agencies toward Zero Trust by 2027.

But there still might be confusion around what the term means in the broader physical security realm.

The concept of Zero Trust is a transition from perimeter access control with free movement within the secured area (trust after authenticated entry) to an architecture of continuous monitoring of people and resources (data in this case), restricted movement to only specifically authorized areas (never trust, always verify).

Zero Trust Evolves

As the norm for government changes, the agencies and departments are developing plans and strategies to meet the goal over the next several years. Most areas are based on the Cybersecurity & Infrastructure Security Agency's (CISA) Zero Trust Maturity Model 2.0 and stemming from the National Institute of Standards Special Publication 800-207. It articulates the five pillars of achieving Zero Trust:

- **Identity**: An attribute or set of attributes uniquely describing an agency *user or entity*, including non-person entities. Enforce user and entity access to the right resources at the right time for the right purpose without granting excessive access. Integrate identity, credential, and access management solutions, enforce strong authentication, grant tailored context-based authorization, and assess identity risk for agency users and entities.
- **Devices:** Any asset, including its hardware, software, and firmware, which can connect to a network, including servers, desktop and laptop machines, printers, mobile phones, Internet of Things devices, networking equipment, and more. Secure all devices and prevent unauthorized devices from accessing resources. Device management includes maintaining a dynamic inventory of all assets including their hardware, software, and firmware, along with their configurations and associated vulnerabilities as they become known.
- **Networks:** An open communications medium including typical channels such as agency internal networks, wireless networks, and the Internet and other potential channels such as cellular and application-level channels used to transport messages. Shift *from* perimeter-focused security and permit agencies to manage internal and external traffic flows, isolate hosts, enforce encryption, segment activity, and enhance enterprise-wide network visibility. Implement security controls closer to the applications, data, and other resources and augment traditional network-based protections to improve defense-in-depth.
- **Applications and workloads:** This includes agency systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments. Continuously authorize application access, incorporating real-time risk analytics and factors such as behavior or usage patterns.
- **Data:** All structured and unstructured files and fragments that reside or have resided in federal systems, devices, networks, applications, databases, infrastructure, and backups, including on-premises and virtual environments, as well as the associated metadata. Following federal requirements, data should be protected on devices, applications, and networks. Agencies should inventory, categorize, and label data,

protect data at rest and in transit, and deploy mechanisms to detect and stop data exfiltration.

There are also three foundational elements practitioners need to consider when implementing their strategy, including:

- **Visibility and analytics:** Visibility refers to the observable artifacts that result from the characteristics of and events within enterprise-wide environments. The focus on cyber-related data analysis can help inform policy decisions, facilitate response activities, and build a risk profile to develop proactive security measures before an incident occurs.
- **Automation and orchestration:** Zero Trust fully uses automated tools and workflows that support security response functions across products and services while maintaining oversight, security, and interaction of the development process for such functions, products and services.
- **Governance:** Governance refers to the definition and associated enforcement of agency cybersecurity policies, procedures, and processes, within and across pillars, to manage an agency's enterprise and mitigate security risks in support of zero trust principles and fulfillment of federal requirements.

Building a Better Solution

> *"Physical security systems already incorporate the principles of Zero Trust in their design and implementation, especially in the highest-security systems in the Departments of Defense and Energy.*

Closed-loop systems with no outside connections; fixed design with tested components tuned to a validated Physical Security Information Management (PSIM) software, operated by fully vetted and specifically authorized users. These systems are custom-built "wooden shoes," acquired in a lengthy process and operated for years before being upgraded by a complete system refresh.

While effective, these systems have significant limitations in an ever-evolving threat landscape. They are mostly reactive, only "plug and play" with the components they are developed and certified with. New technology is difficult to integrate, often leaving these solutions years behind the state of the industry in many cases. The closed loop shuts off the ability to easily share data with larger complexes, installations, or enterprises. Data is the area where competition and advantage can be gained in business security operations, warfare, and physical security systems.

Recognizing this is the Data Age – or Data Revolution (in keeping with the agricultural – industrial – digital path), Zero Trust must have confidence in the data input to provide an advantage in data aggregation. The generation, analysis, and correlation of data from historically disparate streams offer an exciting promise of pushing physical security closer to the anticipation of and early response to threats while orchestrating a complete understanding of the holistic threat picture:

- High-security systems data fused with facilities control systems and geographic information systems to correlate events in real places at real points in real-time.
- Access control measures integrated with human resource and IT systems instantaneously.
- AI-enabled analytics can monitor trends from extranet sources in real-time, increasing the security team's overall awareness.

Enhancing Technology Migration

Beyond data, Zero Trust principles are the only sound architecture for physical security systems. This transition will require a concerted focus on the multitude of devices at the boundaries and extremities to enforce these principles through expectations codified in

requirements. A network structure that prevents devices that cannot cryptographically verify themselves, continuously inventories and monitors the data of all connected devices can bring the perimeter more under control. An expectation of modular open architecture standards-based non-proprietary solutions will accept new sensors, cameras, or access control technology without requiring extensive testing – provided these elements meet Zero Trust architecture requirements. Proprietary data sets and solutions will be much less attractive to enterprise customers.

> *"Alongside the opportunities of Zero Trust for Physical Security Systems, there are also many challenges. The first two are intricately linked– evolving policies and standards and cost-risk decisions to meet Zero Trust requirements."*

Departments and agencies are embarking on a path to achieve Zero Trust, but this will take many years and billions of dollars to materialize. Standards and definitions, such as where the Zero Trust boundary is set and its minimum requirements, will shift over time. Solutions that can move agencies toward Zero Trust without massive "rip and replace" actions will be extremely attractive in the near term.

Cloud-based services – massive infrastructure integration with micro-segmentation into discrete networks or services is the path of many agencies and will certainly shape the acquisition policies of most requests. Certain entities – notably in the Departments of Defense and Energy – will need hybrid infrastructure solutions (cloud and on-prem) for continuous, uninterrupted operations and mission assurance. These systems must also adhere to the Zero Trust requirements and will increase their value and effectiveness through a sound, secure path to share data with the larger data cloud.

How Zero Trust Will Evolve

Continuous device, user, and data monitoring is a significant challenge that will not have a silver bullet solution. It will require solutions providers to be knowledgeable and proactive cyber citizens to realize the architecture and push the borders of what's possible. Physical security systems must incorporate artificial intelligence (AI) tools to achieve this like IT networks will. Data itself also poses a myriad of challenges. Cloud-based, plug-and-play architecture requires common storage, monitoring, analytics, and data standards.

AI tools that monitor the system's data flows and sensor feeds can automate monitoring to significantly ease the burden on the human in the loop, even to the point of automated response and dispatch. U.S. government agencies also desire the transition to cloud-based services – Physical Security Systems as a Service is an attractive alternative to the current practice of *Requirements Development – Solicitation – Buy – Own & Operate, Rinse and Repeat in five years* for some agencies.

The amount of data that can be used to build an all-encompassing security picture incorporating (human resources, user network activities, physical security, facilities, weather, local news and more) is staggering and beyond the means of a human to process. Zero Trust will require "data on data" for system health monitoring and "data assurance."

Adopting Zero Trust principles marks a pivotal shift in physical security systems, propelling them beyond traditional perimeter-based approaches toward a more dynamic and resilient framework. As government agencies and enterprises navigate the complexities of this transition, they must confront both the challenges and opportunities it presents, from evolving policies and integration hurdles to the promise of enhanced data-driven insights and proactive threat mitigation.

By embracing Zero Trust as not just a cybersecurity imperative but a fundamental philosophy guiding the safeguarding of physical assets, organizations can forge a path toward greater resilience, agility, and confidence in an ever-evolving threat landscape.