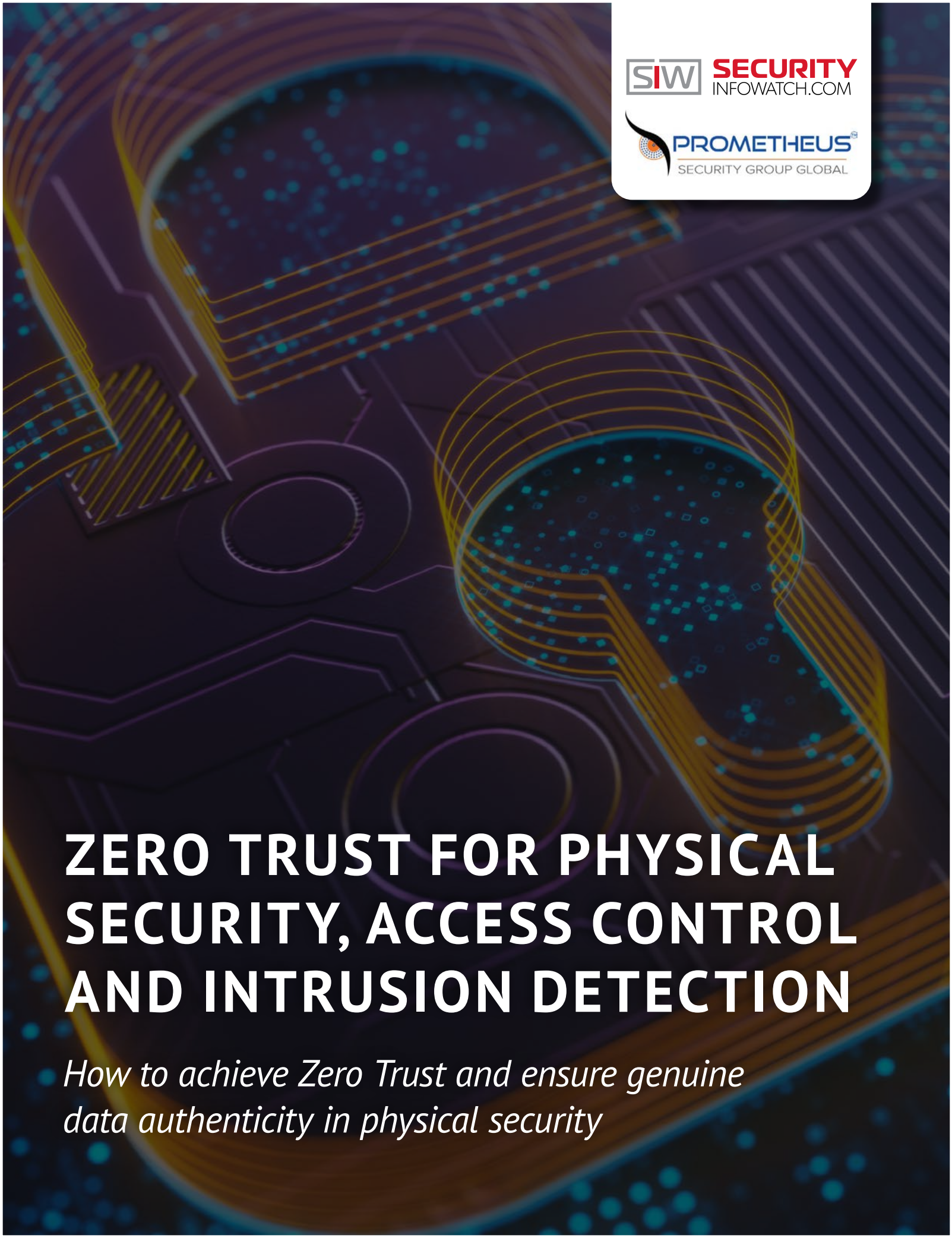

SECURITY INFOWATCH.COM

PROMETHEUS SECURITY GROUP GLOBAL

ZERO TRUST FOR PHYSICAL SECURITY, ACCESS CONTROL AND INTRUSION DETECTION

How to achieve Zero Trust and ensure genuine data authenticity in physical security

It's quite a different world we live in today. Advancements in digital technologies and the Internet of Things (loT) have created more opportunities to blur the lines between what's real and what's fake. With aging sensor technologies used in physical security systems and insecure and unencrypted protocols utilized in the systems supporting access control, intrusion detection, and video assessment, the system's efficacy comes into question. Susceptibility to spoofing, tampering, and false identification raises the risk of human or automatic intervention based on inadvertently trusting "bad data" and can have significant consequences. We have all seen video and audio deepfakes that look convincing and seem authentic. Tampering of critical systems and sensors from outside and inside threats providing unauthenticated access is a genuine concern. According to the Department of Homeland Security, these threats are only increasing and becoming more sophisticated.

Lessons learned include a Chinese company that handed over $25 million in a successful phishing attempt leveraged via a spoofed video of the company's CFO—which proved later to be a deep fake. In other examples, stolen identity by siphoning unencrypted data both at rest and in transit has been utilized to implement methods to bypass access controls and detection meant to keep the unauthorized and unauthenticated out. These techniques threaten the foundational effectiveness of physical security systems that many organizations rely upon.

WHAT IS ZERO TRUST?

Zero Trust is a strategy and concept that implements a "do not trust by default" approach with no implicit trust granted to any user or system, assuming threats exist internally and externally. It is a complementary security principle to the widely adopted "least privilege" principles. While least privilege focuses on minimizing access rights, Zero Trust supplements this and furthers security by continuously verifying and validating every subsequent access request, providing a more robust security posture.

The recent executive order EO 14028 will have widespread consequences for the industry in government procurement and critical infrastructure protection (CIP), utilities, industrial, and local government agencies. Issued in May 2021, the EO requires U.S. government agencies to implement Zero Trust mechanisms starting in 2024 and no later than 2027. Still, these requirements are also expected to filter to other industries and markets. As such, many organizations are scrambling to facilitate Zero Trust infrastructure — fearing costly PACS and other system replacements to meet its requirements of trusted and verified data continuously monitored throughout the enterprise.

FIVE PILLARS OF ACHIEVING ZERO TRUST

Designed to improve the nation's cybersecurity, EO 14028 "establishes baseline security standards for developing software for the government, including requiring developers to maintain greater visibility into their software and making security data publicly available," according to the General Services Administration (GSA). The next several years will be critical as government agencies and departments strategize how to meet the established requirements and goals. Many of the guidelines for Zero Trust come from the Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Maturity Model 2.0 and the National Institute of Standards Special Publication 800-207.

The five pillars of Zero Trust detailed by CISA include but are not limited to:

1. **User Identity:** Utilize robust authentication methods to verify identity before granting access to resources; perform continuous monitoring and validation of identified users.
2. **Device Security:** Validate devices against trusted policy; perform a continuous assessment of device security posture.
3. **Network Security:** Enforce logical/physical segmentation to minimize risks of active/passive lateral movement within the network; utilize strong encryption protocols to protect data in transit.
4. **Application Security:** Control and monitor access to applications, ensuring only authorized use; implement secure development to implementation practices and runtime protection to safeguard applications from threats.
5. **Data Security:** Maintain data integrity and accessibility by authorized users; implement use of strong encryption and access controls to ensure the integrity of data at rest and in transit.

WHY IS IT IMPORTANT?

Zero Trust is essential because it fundamentally changes how organizations approach security to adapt to the ever-evolving threat landscape. In the physical security sector, protected assets are high-value and high-consequence, including the safety of human life. The systems, sensors, and software suites utilized for driving actions and decision-making must be authentic and trustworthy, even at the level of the most minor input/output components.

The implementation of Zero Trust drives data surety in systems and devices from the cloud to the edge, ensuring every part of the system is embedded with cyber security controls, and has become a necessity in achieving physical security and cyber-secure premises.

In a practical example, least privilege ensures that a user's permissions are minimal based on where they need to be or what they need to access to do their job. However, implementing only that approach has inherent flaws, which will become evident as we explain the transition to Zero Trust and why it's vital in the digital age.

ZERO TRUST FOR PHYSICAL SECURITY AND CRITICAL INFRASTRUCTURE PROTECTION SYSTEMS

As digital technologies advance and proliferate, the adoption of Zero Trust enhances the security principle of "least privilege." Presidential Executive Order (EO) 14028 is now driving the move to Zero Trust frameworks in physical security, including access, perimeter control, and intrusion detection. It's a blended physical security and cybersecurity approach that goes beyond the traditional "trust but verify" and believes all networks and communications contain inherent possible threats.

The EO represents a monumental shift in the security and access control industry, where every action is *continuously* monitored. The five pillars provide the framework to connect to Zero Trust architecture. It is necessary to ensure **all** data, including from the scene or sensor and command and control signals back to devices, are authentic and verified processes and network structures.

Many believe that their physical security systems are verified and encrypted. Still, many systems have an inadequate border at the server or monitoring center level and few at the data acquisition level. The question can be asked: where is the ultimate edge? Most agree that this may be the data acquisition device, such as an IP camera or card reader, but consider the real-world sources that those devices are intended to interact with. This pushes the edge to the scenes and sensing devices that are dynamic and susceptible to human intelligence.

Applying Zero Trust principles to physical security means that entry to buildings or sensitive areas is not automatically granted based on physical credentials alone. Instead, individuals must be continuously verified, often through biometric data and real-time authentication. Did that access control reader output valid data? Is the sensor on the door in the expected state, or has an insider tampered with the wires in an inconspicuous closet, making it appear closed? What about the reverse direction? Did that command sent to the access control system come from a valid command and control system or a man-in-the-middle? Did the system operator initiate the vehicle gate opening, or did the maintenance crew purposely cross some wires?

Constant real-time verification and authentication error detection, as well as encryption of data across the entire system from the scene to the enterprise command center, provide a more robust, trusted dataset that not only contributes to more secure systems but also provides better fuel for advanced artificial intelligence (AI) and machine learning (ML) to yield more accurate results from data analysis.

Organizations must have the infrastructure to ensure data is valid when generated, collected, and then safeguarded when that information is stored. Data surety and Zero Trust are all about data that can be correlated and interfaced with other information. This ***requires*** scalable public key cryptography and modern authentication methods to be applied to ALL nodes within the system. Devices are authenticated with a certificate-based identity, much like a human with an access credential or biometric, ensuring devices can't just access systems without proper authorization. When placed into service within the system, the information being generated can be cryptographically verified from that device, at that place, and at that point in time. Pertinent data is collected, correlated, and protected — with encryption; it can't be modified in transit or at rest without notice, alert, or exceptions generated.

The application of Zero Trust in these critical systems requires a structure built to gather, transmit, and store data in a trusted manner and then use it appropriately in the physical security world. For example, with this data, users can gather information on personnel files, an employee's access history, their account access, and attempted actions to ensure that what they are doing is compliant with policy.

It does no good to leverage Artificial Intelligence or Machine Learning (AI/ML) tools on a data pool that can't inherently be trusted down to every piece of stored information — because, in essence, it will only base its conclusions or inferences and alert on inherently flawed data. Advanced tools are worthless if you can't fully trust the data across the enterprise. When trusted, valid data is in place, it enables speed of decisions, superior correlation of events, and identification of physical security trends.

Today's critical infrastructure protection must establish a broader perimeter of data trust and move more devices toward achieving Zero Trust's goal. Zero Trust provides confidence in data, and trusted data feeds into trusted data storage, whether local or cloud. It starts with Zero Trust by design, which means devices that incorporate requirements (authentication, encryption, and validation) are built to be integrated into the network. We know that the IoT and operational technologies are not necessarily built on the same cybersecurity framework as networks, and the transition of those devices into physical security is also a concern.

UFP, DESI, AND SCENE AUTHENTICATION

PSG recognizes the importance of Zero Trust in the physical security sector and operates with the mindset of continuous innovation and development to contribute and align with Zero Trust strategies. An immediate rip-and-replace approach to the current access control and intrusion detection system is not usually feasible or cost-effective. Still, it does benefit

from a migration-over-time approach. Therefore, optimizing compatibility and interoperability while providing Zero Trust-compatible infrastructure for system upgrades in phases is essential.

The Universal Field Panel (UFP), along with the Digital Encryption Security Interface (DESI), takes an existing installed 1940s analog sensor circuit technology and introduces it to the modern digital age of Public Key Infrastructure (PKI) encryption and authentication. It is enhancing its capability to become more trustworthy in gathering data and verifying control signals without a complete system overhaul. It's an end-to-end, secure, open architecture platform offering a safe computing environment with robust encryption that carries data from edge sensors to control centers digitally and closes the vulnerability gap of legacy line-supervised analog circuits. The UFP and DESI enable the alignment with Zero Trust cybersecurity pillars by using modern authentication and encryption methods to provide device and data security.

DESI is an edge-to-enterprise command center encryption module that pushes the analog to digital conversion to the edge, minimizing the attack surface and providing an authentication and encryption capability to data ingested from edge devices like sensors and detectors while utilizing the existing cabling infrastructure, offering a low-cost, practical and effective approach to Zero Trust. DESI also simultaneously provides the same authentication and encryption capabilities for ingested sensors AND control mechanisms such as relays and other critical outputs, which is a massive win for access control systems. This technology updates and replaces legacy analog end-of-line (EOL) resistors with sealed digital microchips. DESI gathers data cost-effectively from intrusion detection, access control, and industrial controls and can be adapted for other OT/IOT devices like building control systems.

DIGITAL REAL-TIME CONTINUOUS SCENE AUTHENTICATION

PSG has also developed a digital Scene Authentication capability that combines raw camera feeds in real-time with an injected encrypted algorithm source overlay to provide real-time validation of the source video scene and its authenticity. This goes beyond the standard OEM encryption of data egressing from the camera by providing an encrypted digital pulse into the camera scene for processing. The signal source in the scene utilizes both the visible and non-visible light spectrum to convey the messages, providing real-time authentication.

Scene Authentication is a tamper-proof, verifiable video data solution that provides proof the viewed imagery was from a specific paired camera and point in time, meeting the zero-trust pillar of data security and giving nonrepudiation evidence of events. This video image fingerprinting is patented video technology that meets strict critical asset specifications for anti-spoofing, tampering, and sabotaging camera scenes. Scene Authentication complies with Federal Information Processing Standards (FIPS) approved cryptography and is GSA-approved.

This tool is applicable whenever trusted, verified video is required. A new trusted digital scene can use AI and ML

intrusion detection and assessment capabilities to provide the first clue that something abnormal is occurring, with object or activity recognition—using trusted video as a sensor for early detection. It can also be deployed in police interview rooms and courtrooms for high-ranking government officials to determine the validity of news reports, eliminate questions about whether the video is authentic, and scour out deep fake videos.

HOW TO ENABLE ZERO TRUST WITH PSG

With the current mandate, it's unclear what exactly constitutes the absolute edge, but PSG's approach to technology development is to push data collection and encryption out to the furthest edge possible, including stepping off the wire and into the scenes, sensors, and control devices. From pushing sensor processing to the limits of the physical edge to implementing strategies for the authentication of source data, these methods contribute greatly to the implementation and enforcement of Zero Trust within the physical security enclave.

Zero Trust is an urgent need and costly mandate intersecting physical security and cybersecurity. Getting trusted data is crucial in meeting new Zero Trust requirements in government and adjacent markets. PSG technology can make significant strides across multiple industries today, with the architecture and tools to cost-effectively implement Zero Trust from the edge to the enterprise without a total rip-and-replace. Zero Trust is available now, and we can help you implement a successful methodology to meet the executive order and beyond.

PROMETHEUS SECURITY GROUP GLOBAL

SIW SECURITY INFOWATCH.COM

READY TO ENHANCE YOUR SECURITY FRAMEWORK WITH ZERO TRUST PRINCIPLES?

Visit our **website** or reach out to our experts to schedule a consultation and take the first step towards a more secure future.

sales@psgglobal.net

(512) 247-3700

LinkedIN