PROMETHEUS™
SECURITY GROUP GLOBAL

A Zero Trust Architecture for the Physical Security Equipment Industry

A Practical Guide for Architects, Engineers, OEMs, Integrators/Tech Providers and End Users

EXECUTIVE SUMMARY

Zero Trust Architecture (ZTA), first defined by John Kindervag in 2010[1], has transformed security mindsets by replacing static perimeter defense strategies with continuous verification and authentication of all devices. Until recently, physical security equipment (PSE) couldn't align with these principles. Prometheus Security Group (PSG) has closed that gap — introducing the industry's first unified Zero Trust technology stack that extends protection across legacy infrastructures to *any* third-party far-edge input/output (I/O) device, including readers, sensors, cameras, door locks and any switched power device.

PSG's Zero Trust platform is proven, open, and federally certified, deployed in the most demanding environments.

Information Technology (IT) focuses on managing data, software, and communication networks, prioritizing confidentiality and security, while Operational Technology (OT) controls security and access control equipment, physical machinery, and industrial processes, prioritizing safety and real-time availability. The threat landscape has shifted from IT to OT, including physical security equipment (PSE). Operational Technology targets are now prime targets for nation-states, ransomware groups, supply-chain compromise and insider threats. Mandates such as Executive Order 14028[2] and NIST SP 800-207[3] make Zero Trust required for government systems, with critical infrastructure markets tracking very close behind. For commercial and industrial organizations, operating without Zero Trust leaves core business processes vulnerable to spoofing, replay attacks, lateral movement, credential abuse, and other preventable threats — risks that can adversely impact continuity, public perception and financial performance.

Industrial automation and control include the supervisory control components typically found in process industries[4]. It also includes SCADA (supervisory control and data acquisition) systems that are commonly used by organizations that operate in critical infrastructure industries. These include a) electricity transmission and distribution b) gas and water distribution networks c) oil and gas production operations d) gas and liquid transmission pipelines [4].

PSG's Zero Trust solution is a federally certified, field proven open-architecture platform deployed in the most demanding environments, including Protection Level 1 Nuclear (PL1N) programs under the DoD and DOE. The technology interfaces with any reader, any sensor, any camera, and control point, video management system or command and control platform. It retrofits existing analog infrastructure to strong, modern cybersecurity Zero trust principles without rip-and-replace efforts. Developed over eight years, PSG's unified platform for access, intrusion, and video is the only physical-security system certified by the U.S. Air Force for deployment in PL1N environments.

Why Zero Trust Matters for Physical Security

As end users recognize that data is the new oil, IT security expectations for OT space are accelerating. Yet most OT systems still rely on "security through obscurity" leaving critical exposure points: unidentified endpoints, unproven, untested and proprietary protocols, unauthenticated and unencrypted analog signals, and *totally unprotected control outputs*. Physical security can evolve from a cost center to a value center by generating authenticated data for Artificial Intelligence (AI) and digital-twin applications. A digital twin is a dynamic, virtual replica of a physical object, process, or system that remains synchronized using real-time data from sensors and Internet of Things (IoT) devices. By leveraging AI and simulation, it allows for analysis, monitoring, and optimization without risking the physical asset. Bringing PSE security up to the level of the assets it safeguards is an immediate mission and business imperative — far too important to wait for regulatory mandates or crisis-driven responses from incidents to force the issue.

PSG's Core Value Proposition:

- **Establishes** strong cryptographic identities for Industrial Internet of Things (IIoT) endpoints which are traditionally unidentified, unauthenticated and unencrypted.
- **Eliminates** cyber vulnerabilities inherent in legacy analog inputs and control outputs by continuously authenticating and verifying devices and data.
- **Elevates** physical security to the same cybersecurity standards as IT through proper application of Zero Trust principles.
- **Enables** AI and digital twins with authenticated edge-to-enterprise data.
- **Creates** new OEM supply chain authenticity and revenue opportunities via the **DESI controller**, which can be licensed and embedded in edge devices or integrated into existing systems and devices to enhance security.

PSG'S MISSION: to drive a unified Zero Trust architecture standard across the PSE industry — bridging IT and OT with an open architecture, scalable, mission-proven option built on enforced micro-segmentation and hardware-anchored attestation.

01/

ZERO TRUST ARCHITECTURE – PRINCIPLES FOR PHYSICAL SECURITY EQUIPMENT INDUSTRY ADOPTION

Zero Trust means no device, user, or data flow is trusted by default - trust must be verified at every point, continuously.

Edge devices are now a primary attack surface. Sensors, door hardware, cameras, power control outputs, and readers are especially vulnerable because they sit at the far edge and lack modern cybersecurity protection. Many legacy systems rely on the assumption that once inside the protected perimeter, they are safe. This false sense of trust creates exposure, allowing attackers to bypass inadequate authentication, exploit weak protocols, tamper analog signals and harvest unencrypted communications. Properly applied, Zero Trust principles eliminate these risks.

> ***"Resilience must be built in. Systems should maintain secure operation even during attacks, outages, or degraded network conditions."***

Every event, connection, and action must be confidential, authenticated and verified. Device identity and authenticity must be established and cryptographically validated before any data is accepted. Authentication and interrogation must be continuous, not a one-time check or worse passively waiting for information. If a device fails verification, access is revocable immediately. Likewise, every action must be explicitly authorized. Devices and users operate only within defined roles and established corporate policies; duties are segmented. Dynamic, role-based access reduces risk by adapting privileges to context, while static permissions invite exploitation.

Hardware enforcement with strong root chains of custody is essential to achieve this. Inline security controls at the edge must block unverified data before it enters the network. Software-only enforcement is insufficient, and adversaries increasingly target firmware and embedded operating systems. Trusted hardware modules create secure boundaries and prevent protocol misuse, securing data even at rest.

Edge devices must communicate only through explicitly authorized protocols, enforcing strict least-privilege principles and denying any unauthorized or unexpected commands by default. This approach stops lateral movement and command injections before they start.

Data integrity must be verified before upstream consumers — whether human operators, AI analytics, or machine learning models — act on it. AI models and digital twins fundamentally depend on authenticated, verified data — without it, insights become distorted or outright wrong. False or manipulated data doesn't just mislead algorithms; it can send response force to the wrong location, consuming critical time and opening gaps an adversary can exploit. Continuous verification ensures these upper-level systems can operate on clean, accurate inputs. Every transaction must be logged and tamper evident. All access attempts, data flows, and enforcement actions should be recorded and retained for audit. Without complete, immutable records, attacks go undetected and liabilities are not exposed.

Finally, resilience must be built in. Systems should maintain secure operation even during attacks, outages, or degraded network conditions. Fail-secure modes prevent unsafe states, and recovery must be rapid, controlled, and verifiable.

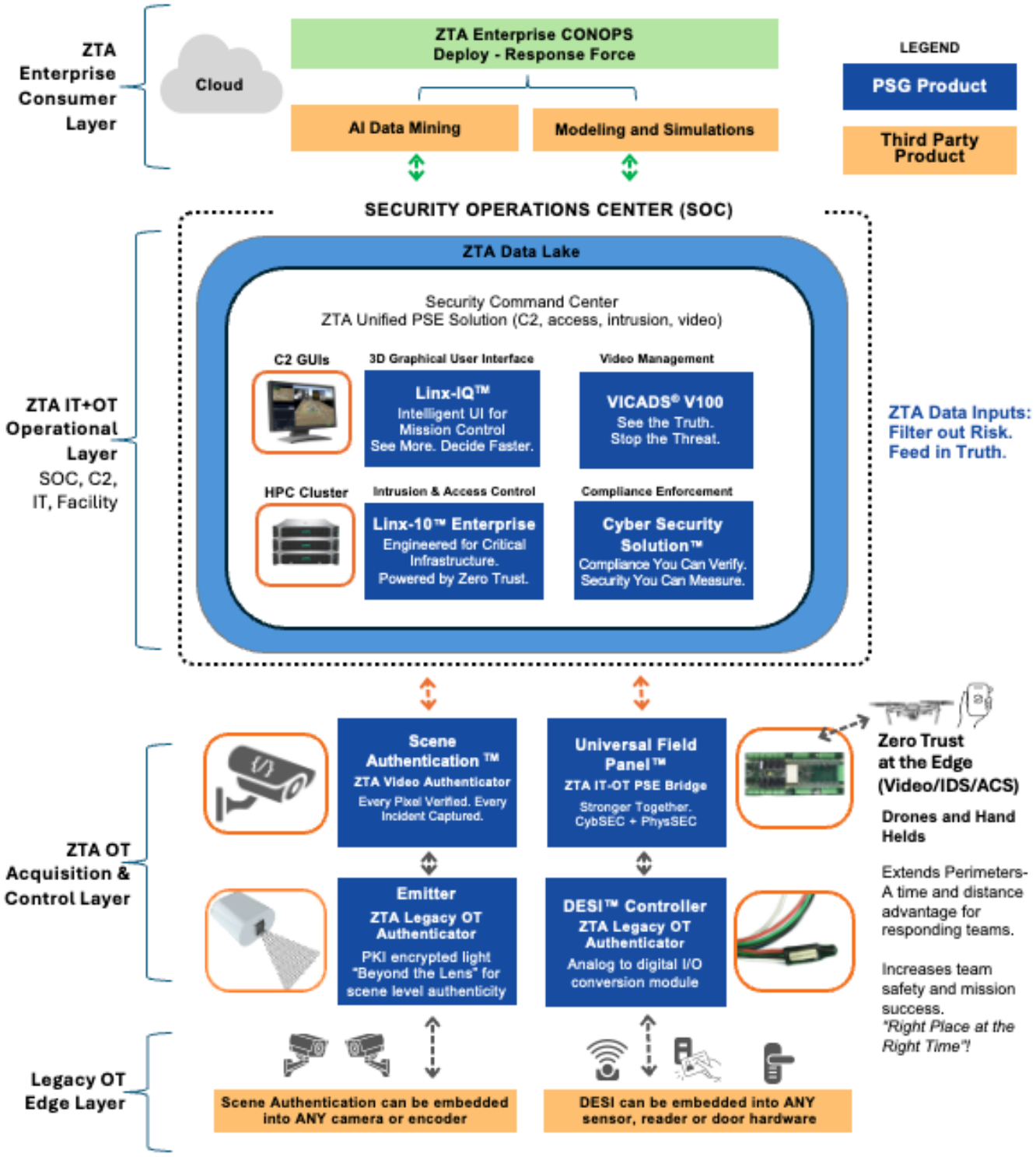
Today, Zero Trust principles can - and must - be applied to all Operational Technology including physical security devices. Implementing Zero Trust practices at every edge device makes security enforceable, auditable, and defensible, meeting the same rigorous standards now expected across all critical-infrastructure and IT systems.

02/

PSG PROVIDES A STANDARD ARCHITECTURE IMPLEMENTING ZERO TRUST FOR OPERATIONAL TECHNOLOGY

Prometheus Security Group (PSG) extends Zero Trust enforcement from the command center to the farthest edge device. Every product in the PSG suite applies authenticated access, deterministic authorization, comprehensive logging, protocol governance, and resilient operation—forming a standard for a unified Zero Trust platform for physical security. PSG's architecture allows organizations to extend the protected perimeter beyond the traditional fence line – bridging from IT to OT to include remote sensors, drones, and handhelds into a single Zero Trusted operational environment instead of ignoring that these vulnerabilities exist.

PROMETHEUS
TECH STACK: ZERO TRUST ARCHITECTURE
AUTHENTICATED AND VERIFIED (A-V) EDGE TO ENTERPRISE



ZTA for the Acquisition & Control Layer - Universal Field Panel™ an IT to OT ZTA Bridge for PSE

The **Universal Field Panel (UFP)** is the foundation for ZTA for access control and intrusion detection. It establishes the interface boundary between the Acquisition and Control and the Security Operations Center (SoC) layers as well as providing the same for the edge layer. It delivers a clear migration path from legacy analog I/O to digital communications, hardware-anchored cryptographic identities and modern Zero Trust enforcement, all while reusing existing sensors and wiring.

Technical Security Benefits:

- **Strong cybersecurity:** Cryptographic identities for endpoints, hardware root of trust, secure boot, device authentication & encrypted communication
- **Multiple paths to adopt ZTA:** Open Architecture platform with standards-based protocols, modern API, reference designs and third-party application container options on a secure host
- **High density:** each panel supports up to 128 inputs, 64 outputs and 16 readers reducing total cost per input, output and access control door
- **Extended protection:** perimeter coverage bridges from IT to OT and removes "Security through protocol Obscurity" that pervades the industry today.
- **Role-based access, least privilege** and **inline protocol control** at the edge

The UFP authenticates each session, restricts communication to authorized protocols, enforces least privilege, blocks unauthorized commands, and continuously verifies device identities. Secure, distributed edge processing reduces risk, improves performance, and enhances resilience.

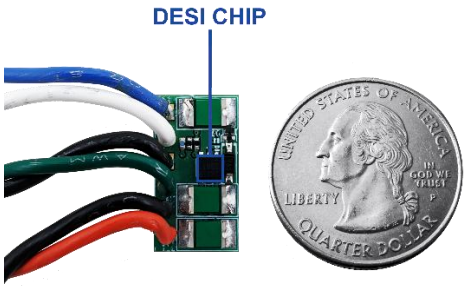
Cost and Operational Benefits:

- **Reduced SoC hardware, power, and cooling requirements** — lowering operational costs and simplifying infrastructure footprints without sacrificing security performance.
- **Faster edge-level data collection and analysis for accelerated incident response** — enabling earlier detection, quicker decision-making, and reduced dwell time for threats.
- **Increased processing speed and overall system responsiveness** — improving operator effectiveness and system reliability in time-sensitive PSE environments.
- **Extended boundary protection through remote and mobile edge devices** — expanding the security perimeter and delivering coverage in locations where traditional legacy infrastructure cannot reach.
- **Cost Effective Migration** Upgrade from legacy infrastructure to modern ZTA input by input without costly rip and replace new infrastructure requirements.

Combines CybSEC and PhysSEC with enforced cybersecurity safeguards—including Trusted Platform Module (TPM), secure boot, encrypted root file systems, and verified firmware—to ensure stronger system integrity and tamper resistance.

PSG offers access to technology through **OEM licensing agreements** and embraces a **Modular Open Systems Approach** for flexible integration. Multiple paths exist for OEMs, Integrators and End Users **to adopt ZTA:** Open Architecture platform with standards-based protocols, modern API, reference designs for hardware level integrations and third-party application container hosting options in a Zero Trust enabled environment.

ZTA for the Acquisition & Control Layer — Digital Encrypted Security Interface Controller a ZTA Authenticator for Legacy OT Edge I/O Devices



The **DESI controller**, small enough for insertion into existing physical security equipment devices, enables legacy analog devices to achieve digital conversion. It converts legacy analog input signals and totally unprotected control signals into digital **PKI endpoints over *existing infrastructure AND with existing devices*. Once encrypted and authenticated**, it prevents attackers from bypassing or injecting false signals into vulnerable and exploitable infrastructure.

- **Extends** Zero Trust to legacy OT equipment: emergency signals, door locks, sensors, access control devices, readers, process controls and building automation devices without replacing wiring or communication infrastructure
- **Provides** a strong cryptographic identity that continuously validates each device: inputs before acceptance AND outputs before command execution
- **Easily** installs in the sensor device or at the output device, replacing vulnerable and outdated end-of-line resistors and implementing protection where none exists today — delivering stronger tamper detection, enhanced system resilience, and faster identification of faults and unauthorized activity.
- **Provides** a new level of supply chain traceability and security to OEMs and End Users allowing verification of genuine devices
- **Requires** far less infrastructure at the edge AND at the panel for new installations, drastically reducing the cabling infrastructure and costs required to install PSE systems. For example, an access control door's request to exit, lock control, door position and reader/lock tampers can all be picked up over a single pair of wires to the door reducing cabling infrastructure by over half.

By enabling manufacturers signed device authentication and seamless end user validation, OEMs can ensure every PSE device enters the security ecosystem with guaranteed provenance and trusted genuine identity. These block common supply chain compromise scenarios, including counterfeit devices entering inventory, firmware modified en route, or unauthorized hardware swapped during distribution. This capability not only strengthens customer confidence but also differentiates OEM products in a market increasingly driven by Zero Trust requirements.

Future device lines will ship fully ZTA ready out of the box, empowering OEMs to deliver "greenfield ready" solutions that accelerate deployment, reduce integration overhead, and minimize support costs. Manufacturers

gain faster time to market, simplified compliance with evolving security standards, and a compelling competitive advantage by offering devices that customers can adopt securely and instantly — from day one.

Additional value benefits for OEMs include:

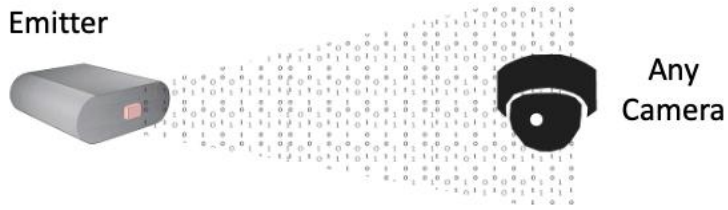
- **Stronger** brand reputation through built in, verifiable security.
- **Provides** streamlined supply chain validation with cryptographically anchored device identity to OEMs and End Users
- **Greater** customer retention through devices that slot seamlessly into modern Zero Trust ecosystems
- **Lower** long term engineering burden by standardizing on a future proof security model
- **Reduced** return rates and warranty claims due to more secure, consistent onboarding

ZTA for the Acquisition & Control Layer — Scene Authentication™ a ZTA Authenticator for Legacy OT Edge Video Devices

PSG's standard architecture extends Zero Trust into the **scene itself** –" Beyond the Lens" through its patented **Scene Authentication™** technology.

- **Emitter** injects PKI encrypted light pulses into the 'scene' for an immutable fingerprint that continuously verifies and authenticates the live video scene from edge to enterprise
- **Receiver** can verify that footage is authentic, live, and location specific.
- **Prevents** spoofing, replay, and video looping attacks that bypass frame-signing methods
- **Prevents** tampering with evidence and video storage
- **Open Architecture** SDK/API integration for any third-party camera or Video Management System and deployable over plug in architectures for devices supporting on-device application development ecosystems

If the light pattern is interrupted, the system automatically triggers an alarm, confirming tampering or obstruction. Scene Authentication fulfills the Zero Trust requirement for **authenticated, encrypted and verified data streams** feeding analytics, AI, and digital twins. When viewed at an operator workstation the emitter pulses are filtered from view, so the insider does not know the signal has tamper protection or where the emitter is located.



ZTA for the IT + OT Operational Layer —

VICADS® V100 ZTA Video Management

PSG's **VICADS® V100** integrates Scene Authentication into a fully operational Zero Trust video management system (VMS).

- **Ensures** only **authenticated and encrypted video** feeds reach the SOC operator and video storage back ends
- **Supports** both analog and IP video, enabling **gradual migration and modernization**
- **Insider Threat** aware at the operator workstation, emitter pulses are invisible, preventing insiders from detecting that tamper protection is active
- **Provides** multiple federal certifications from third party evaluators for performance (PL1-PL4) and compliance Risk Management Framework Authority To Operate (RMF ATO) supporting use in nuclear and critical-infrastructure environments
- **Enforces** Zero Trust principles of "continuously validated and confidential data flow" supporting higher quality inputs to AI and digital twin applications

Technology Note: Scene Authentication is an open architecture and can be integrated with **any camera or VMS**, VICADS is one implementation, Axis ACAP is another; PSG's VMS is not a requirement. PSG is **OEM licensing this technology** for direct integration and can support hardware-based integration on other OEM platforms.

ZTA for the IT + OT Operational Layer —

Cyber Security Solution (CSS) ZTA Management & Compliance Enforcement

The **Cyber Security Solution (CSS)** provides continuous cyber compliance and management of the ZTA subsystems at all layers. Hardware enforcement with strong root chains of custody is essential. CSS facilitates authenticated operations by supplying the root chain of trust for the security devices. Inline security controls at the edge must block unverified data before it enters the network. Software-only enforcement is insufficient, and adversaries increasingly target firmware and embedded operating systems. Trusted hardware modules create secure boundaries and prevent protocol misuse.

It provides a centralized management approach for PSE Industrial Internet of Things (IIoT) devices including but not limited to baseline auditing and verification, vulnerability scanning and patching, ensuring that edge devices communicate only through explicitly authorized protocols, enforcing strict least-privilege principles and denying any unauthorized or unexpected commands by default.

It allows for separation duties and supports micro-segmentation by preventing devices from operating until their cryptographic identities have been validated and authorized, with the approval workflow optionally distributed across multiple administrators. When incidents occur, it provides a place for rapid revocation and remediation.

Once deployed, it becomes the central point for continuous updates, patching, and vulnerability management, keeping the system secure and current.

ZTA for the IT + OT Operational Layer —

Linx-10 Enterprise & Linx™ IQ ZTA Intrusion Detection & Access Control with a modern three-dimensional Security Operations user interface for enhanced situational awareness

Linx™ 10 Enterprise and Linx™ IQ unify command and control functions across intrusion, access, and video, delivering a consolidated view of situational awareness and ensuring that only verified, trusted data reaches the Security Operations Center. Linx IQ introduces a modern three-dimensional situational awareness plane that presents environments more realistically, creating a more immersive and intuitive operator experience. By more closely mirroring the real world, the system enables faster understanding, better decisions, and improved response speed. When operator commands are executed the continuous verification chain occurs in reverse, ensuring that the C2 platform passes cryptographic tests to execute commands and effect change, thus completing the chain of custody and protection.

03/

ZERO TRUST ARCHITECTURE PRACTICAL IMPLEMENTATION AND MIGRATION OF THE OT EDGE

In today's OT environments, the landscape is dominated by long lived legacy equipment, aging infrastructure, and devices that were never designed with modern cybersecurity in mind. Any effective security strategy must recognize this reality. Approaches that assume instant modernization—or ignore the need for gradual migration—inevitably fall short due to the significant economic and operational constraints that industrial operators face.

Likewise, strategies that require entirely new infrastructure or demand wholesale replacement of existing systems are destined to fail. The cost, downtime, and rework associated with such disruptive changes make them impractical for most facilities.

ZTA Standard Architecture Brownfield Advantage

PSG's reference architecture features products that extend Zero Trust into legacy OT environments by securing existing infrastructure with minimal disruption. DESI controllers replace legacy end-of-line resistors and switched power outputs while reusing existing wiring, instantly converting analog loops to digital encrypted and authenticated ZTA control signals. Scene Authentication software can be loaded onto deployed cameras, with emitters added to the field of view and beyond the camera lens, giving operators ZTA verified video without replacing infrastructure. These measures extend the life of brownfield investments while mitigating vulnerability gaps inherent in legacy that attackers target, delivering Zero Trust protection at lower cost and with minimal downtime.

A successful path forward must instead emphasize the deployment of modern cybersecurity controls as close to the operational edge as possible, while still allowing seamless integration with the existing infrastructure exactly as it stands today. Supporting "attach as is" deployment makes this possible. It enables teams to layer modern defenses directly onto existing environments, preserving uptime and minimizing implementation complexity. By avoiding large scale infrastructure replacements, organizations can accelerate security modernization, reduce exposure, and demonstrate responsible stewardship of both risk and resources. This approach aligns enhanced protection with business continuity—delivering resilience without compromise.

From there, the migration to digitally enabled, Zero Trust capable devices can occur progressively — aligned with maintenance windows, budget cycles, and operational priorities. This incremental evolution avoids disruption, preserves capital investment, and ultimately delivers a more secure and resilient OT architecture over time.

This approach delivers three business outcomes executives care about most:

- Reduced risk exposure without operational disruptions
- Preservation of existing capital investment while extending asset life
- A financially sustainable path to achieving Zero Trust across the OT environment

In short, the winning strategy for OT ZTA implementation is not rip and replace. It is evolution, not revolution — a phased, economically responsible journey that strengthens security while protecting uptime and productivity. Zero Trust at the edge requires inline enforcement, continuously authenticated and verified data pipelines from edge to enterprise. PSG's architecture delivers this through a layered design built around its product suite.

04/

ZERO TRUST ARCHITECTURE AI READINESS AND IMPLEMENTATION FROM SPECIFICATION

In a greenfield environment, architects and engineers have a unique advantage: the chance to design systems the right way from the start. Modern cybersecurity isn't an added design burden, it's a set of design principles that prevents painful rework, costly retrofits, and operational bottlenecks later. When security is treated as foundational, teams gain more control over the architecture, reduce long term complexity, and avoid being forced into reactive fixes down the road. Relying on legacy or analog assumptions might seem easier in the moment, but it creates technical debt that will slow future innovation. Building with current cybersecurity realities in mind protects both the system's integrity and the team's ability to adapt and scale with confidence.

Major entities are recognizing the need for a successful Zero Trust model and adopting it into their culture and implementations ratifying new standards such as ANSI/ISA-62443-4-2-2018, Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components[5] and the Department of Defense (DoD), Zero Trust Reference Architecture Version 2.0, July 2022[6].

ZTA Standard Architecture Greenfield Advantage

PSG's reference architecture features products built with Zero Trust from the start, embedding identity, verification, and enforcement into every layer of a new system. Systems can be specified as required to implement ZTA digital authentication and verification from installation day one. DESI modules are designed to fit nearly any installation; the single controller density paired with DESI's dramatic cabling reduction offers increased security and a significantly lower cost compared to traditional analog systems. Scene Authentication software can be preloaded on new cameras, with emitters integrated into the design, so authenticity is enforced without retrofit cost. By integrating these controls at design time, systems are lower cost to secure, faster to certify, and cyber resilient for the long term.

Modern cybersecurity isn't a constraint on innovation either — it's what keeps advanced models, sensitive datasets, and high value simulations safe, reliable, and trustworthy. Designing with current security principles early on prevents data integrity issues, model tampering risks, and system disruptions that can undermine results and slow mission progress. By embedding contemporary security practices upfront, teams ensure their Artificial Intelligence, Automation and Modeling and Simulation systems remain resilient, adaptable, and fully capable.

The PSG ZTA approach requires significantly less infrastructure at both the edge and the panel for new installations, dramatically reducing the cabling and associated costs of deploying PSE systems. By consolidating multiple door level functions—such as request to exit, lock control, door position monitoring, and reader or lock tamper signals—onto a single pair of wires, the system eliminates the need for traditional multi conductor runs. In a typical access control deployment, these signals can all be supported over one twisted pair, reducing cabling requirements by more than half while simplifying installation, minimizing panel side terminations, and lowering overall project complexity and cost.

By consolidating multiple door level functions onto a single pair of wires, this approach drastically reduces both edge and panel infrastructure, enabling far faster and more cost-effective PSE designs and installations. This combined with the dramatic increase in per panel density (128 sensor inputs / 64 control outputs on a single board) not only slashes material and labor costs but also simplifies troubleshooting, minimizes panel congestion, and eliminates many of the wiring complexities that traditionally slow projects down. For teams tasked with delivering reliable PSE system designs on tight schedules and budgets, this architecture removes unnecessary overhead and creates a cleaner, more scalable design with fewer points of failure.

05/
ZERO TRUST ARCHITECTURE PROVEN PERFORMANCE

PSG's complete ZTA product suite has been **tested and validated in DoD and DOE programs** and is **certified at the highest levels** of nuclear and critical-infrastructure security. PSG's ZTA suite is commercial ready, it transforms years of complex compliance requirements into a turnkey, commercial-ready capability that any customer can adopt with minimal effort. Each component enforces Zero Trust directly at the device level, integrating seamlessly into a unified, open architecture.

Legacy OT Edge: Physical Layer

At the device level, all sensors, readers, and cameras are considered untrusted until proven otherwise. For Zero Trust compliance all data flows originating at edge devices must be cryptographically bound to a trusted identity at the inception. DESI Controllers provide this binding for legacy analog inputs and switched control outputs, while UFP panels deliver a modern cybersecurity profile and capability set. Cameras are configured with Scene Authentication software and paired with Emitters to embed ZTA cryptographic scene verification for video. These technologies convert legacy infrastructures **over *existing infrastructure AND with existing devices*.**

ZTA OT Acquisition & Control: I/O Enforcement Layer

The UFP sits in line at the Edge providing the bridge between the IT and OT boundary as the enforcement point. A Zero Trust policy enforcement component must inspect, validate, and authorize all traffic across trust boundaries. The UFP enforces this through protocol allowlisting, continuous device authentication, and session-by-session reauthorization. This ensures that no command, data stream, or device can bypass Zero Trust validation.

ZTA OT Acquisition & Control: Video Enforcement Layer

ZTA principles suggest visual data streams must be continuously validated against source identity to prevent spoofing or replay. PSG's Scene Authentication fulfills this requirement by injecting encrypted light pulses into camera fields of view (beyond the camera lens), which the VICADS V100 verifies in real time. This guarantees the authenticity of video data before it is displayed or stored.

ZTA IT + OT Operations: Operational Layer

At the core of this architecture is PSG's HPC Zero Trust Data Lake — a supercomputer class, high performance computing (HPC) platform engineered to securely store and process all edge generated activity data, including intrusion events, access logs, and video, directly on premises. This hardened data lake delivers ultra-high throughput, exceptional resiliency, and always on availability, adding a powerful layer of protection against cyberattacks. Even under hostile conditions, catastrophic events or partial system failures, the HPC cluster supports degraded yet uninterrupted operations, ensuring continuous system function.

UFP and VICADS outputs feed securely into Security Operations Centers, Security Information and Event Management systems, and cloud platforms, ensuring higher-level systems operate on verified inputs. PSG's Cyber Security Solution and Linx IQ extend this by providing compliance enforcement, central logging, and cross-domain visibility. Faster response times and real time insights thanks to on premises data processing results in enhanced safety and operational continuity in critical environments.

ZTA Enterprise Consumers: Enterprise Integration Layer

Once data is authenticated and validated at the enforcement layer, it can be safely forwarded to enterprise systems. Zero Trust principles require that only trusted OT data should be consumed by analytics, digital twins, or AI models.

For government networks, this architecture requires and achieves Authority to Operate certifications, proving it meets the strictest standards. The HPC cluster functions as the "engine" for trusted data, ensuring that when AI and Digital Twin applications are introduced, they draw only from authenticated, verified ZTA data streams, guarantying that advanced analytics (AI) and Modeling utilize a foundation of Zero Trust integrity.

References

[1] John Kindervag, *Build Security into Your Network's DNA: The Zero Trust Network Architecture*, Forrester Research, 2010.
[2] Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," issued on May 12, 2021
[3] NIST, *NIST Special Publication 800-207: Zero Trust Architecture*, August 2020
[4] ISA-62443-1-1-2007, *Security for industrial automation and control systems, Part 1-1: Terminology, concepts, and models.*
[5] ANSI/ISA-62443-4-2-2018, *Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components*
[6] Department of Defense (DoD), *Zero Trust Reference Architecture Version 2.0*, July 2022

SUMMARY

Prometheus Security Group (PSG) unifies access, intrusion, and video under one proven Zero Trust platform - already deployed across the most critical U.S. defense and energy sites. With federal certifications including Protection Level 1 Nuclear (PL1N). PSG demonstrates with its ZTA Architecture standard for PSE that Zero Trust principles can be bridged across IT to OT boundaries at the edge – for every sensor, reader, camera and I/O device.

As IT and OT converge, ZTA authenticated, confidential data has become the new currency of **secure, reliable operations**. PSG's revolutionary technology turns legacy systems into secure digital assets, giving organizations verified data they can use for AI, digital twins, and operational intelligence. The result: physical security evolves from a **cost center to a value center**.

PSG's mission: to drive a unified Zero Trust architecture standard across the PSE industry—bridging IT and OT to make physical security as intelligent and interoperable as IT.

PSG's team is ready to help design, integrate, embed and scale Zero Trust protection across your enterprise either directly or through your favorite solution provider.

We stand ready to help you bring Zero Trust to your complex operating environment—strengthening protection, improving resilience, and enabling confident operations. It is proven in the nation's most secure environments and ready for yours!

Key Outcomes

01/ Cyber Resilience
Eliminates vulnerabilities in analog and hybrid systems with an open architecture, scalable, mission proven platform built on enforced micro segmentation

02/ Data Integrity
Cryptographically identifies and verifies every endpoint from edge to enterprise with hardware anchored attestation.

03/ Modernization Without Rip-and-Replace
Upgrades reusing existing infrastructure investments through DESI, UFP, and Scene Authentication technologies.

04/ AI Readiness & Implementation from Specification
"Security from the Start" supplies ZTA data inputs for analytics, automation, and digital twins. Designed from inception.

05/ Proven Performance
Secures two-thirds of U.S. nuclear assets across DoD and DOE - and the only PL1N-certified system in the industry.

For consultation or integration support, contact the PSG Zero Trust Solutions team. *www.psgglobal.net*, Tel: 512.247.3700

