PROMETHEUS™
SECURITY GROUP GLOBAL

Zero Trust Architecture for the Physical Security Equipment (PSE) Industry

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

EXECUTIVE SUMMARY

Zero Trust Architecture (ZTA), first defined by John Kindervag in 2010, has transformed IT security by replacing perimeter defenses with continuous verification. 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 to *any* third-party far-edge device, including readers, sensors, cameras, and controllers across analog and digital infrastructures.

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

The threat landscape has shifted from IT networks to OT environments, including physical security edge devices. Physical security systems are now prime targets for nation-states, ransomware groups, and insider threats. Mandates such as Executive Order 14028 and NIST SP 800-207 make Zero Trust required for government systems, with critical infrastructure markets very close behind. Every day without Zero Trust leaves operations vulnerable to spoofing, replay, lateral attacks, and more.

PSG's Zero Trust platform is proven, open, and federally certified, deployed in the most demanding environments, including Protection Level 1 Nuclear (PL1N) programs under the DoD and DOE. The technology interfaces with any reader, sensor, camera, controller, VMS, or C2 system and can retrofit existing analog infrastructure without rip-and-replace efforts. Developed over eight years, PSG's unified platform for access, intrusion, and video secures two-thirds of U.S. nuclear assets and is the only physical-security system certified by the U.S. Air Force for employment in PL1N environments.

Why Zero Trust Matters for Physical Security

As end users recognize that data is the new oil, IT and OT convergence is accelerating. Physical security can evolve from a cost center to a value center by generating authenticated data for AI and digital-twin applications. Yet most systems still rely on unauthenticated analog signals, leaving critical exposure points.

PSG's Core Value Proposition:

- **Eliminates** cyber vulnerabilities inherent in analog devices by continuously authenticating and verifying data through converting analog signals to digital signals.
- **Elevates** physical security to the same trust standards as IT through Zero Trust principles.
- **Enables** AI and digital twins with authenticated edge-to-cloud data.
- **Creates** new OEM revenue opportunities via the **DESI chip**, which can be licensed and embedded in edge devices.

PSG's mission: to unify IT and physical security under a single Zero Trust architecture that is open, scalable, and already proven in the nation's most secure environments.

01/

ZERO TRUST ARCHITECTURE – PRINCIPLES FOR THE PHYSICAL SECURITY EQUIPMENT (PSE) INDUSTRY.

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, controllers, and readers are especially vulnerable because they sit at the far edge and often lack modern security protections. Many legacy systems rely on the assumption that once personnel are inside the perimeter, they are safe. This false sense of trust creates exposure, allowing attackers to exploit weak signals, unencrypted communications, and inadequate authentication. Zero Trust principles eliminate this risk.

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 authenticated and verified (A-V). Device identity must be cryptographically validated before any data is accepted. Authentication must be continuous, not a one-time check. If a device fails verification mid-session, access is revoked immediately. Likewise, every action must be explicitly authorized. Devices and users operate only within defined roles and established corporate policies. Dynamic, role-based access reduces risk by adapting privileges to context, while static permissions invite exploitation.

Every transaction must also 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.

Hardware enforcement is essential. 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. Edge devices must communicate only through approved, whitelisted protocols; unauthorized or unexpected commands should be denied by default. This approach stops lateral movement and command injection before they start.

Data integrity must be verified before analytics. AI systems and digital twins depend on authenticated, verified inputs - if data isn't trusted, the insights derived are unreliable. Verification ensures analytics operate on clean, accurate information.

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.

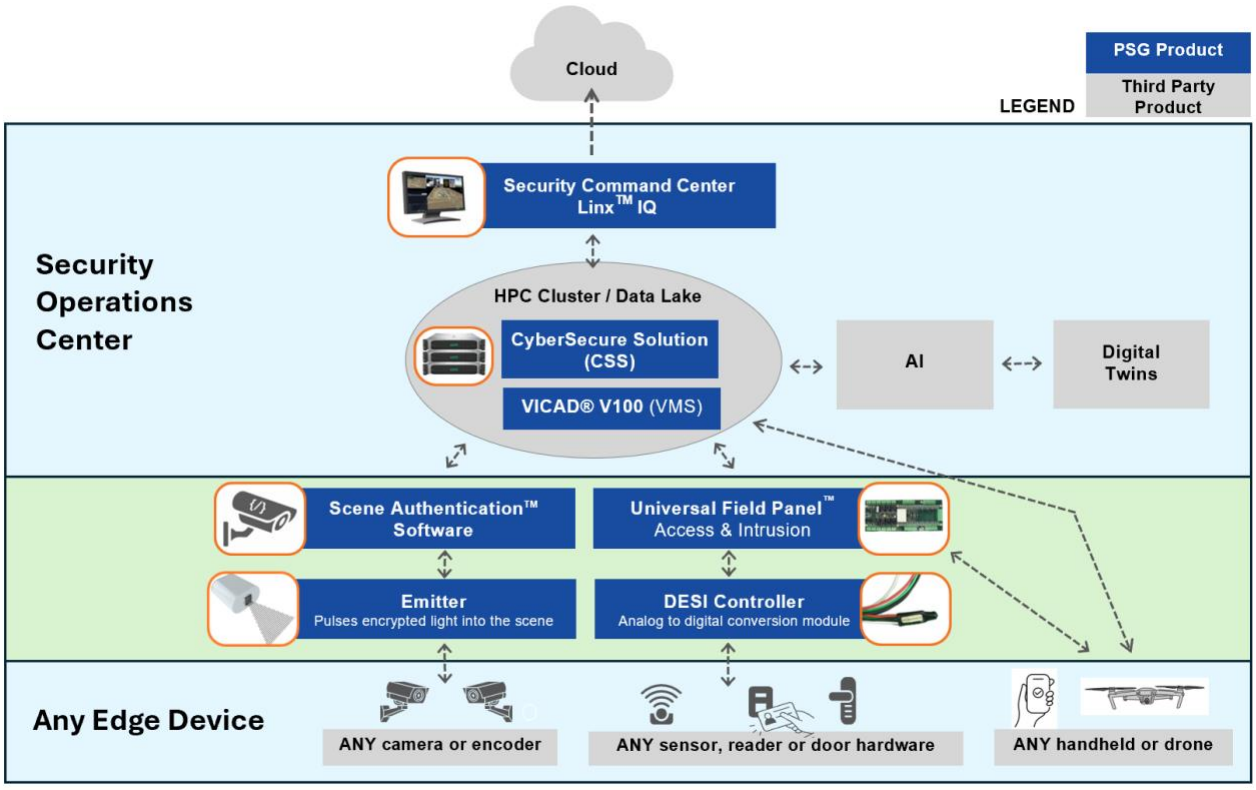
Today, Zero Trust principles can - and must - be applied to all physical security devices, including any intrusion sensor, access reader, or video camera. Implementing ZTA practices at every edge device makes security enforceable, auditable, and defensible, meeting the same rigorous standards now expected across all critical-infrastructure and IT systems.

02/

PSG PROVIDES A TOTAL ZERO TRUST ARCHITECTURE (ZTA) APPROACH

Prometheus Security Group (PSG) delivers Zero Trust enforcement from the command center to every edge device. Each product in PSG's suite applies the core principles of authentication, authorization, logging, protocol control, and resilience, forming a unified Zero Trust platform for physical security.

PSG's architecture allows organizations to extend the protected perimeter hundreds or even thousands of feet beyond the traditional fence line - integrating remote sensors, drones, and handhelds into a single trusted environment.



ZTA for Sensors/Readers - Universal Field Panel™ (UFP)

The **UFP** is the foundation for access control and intrusion protection. It supports both digital and analog inputs, enabling reuse of legacy sensors and wiring while simultaneously implementing modern Zero Trust protections.

- **Role-based access** and **inline protocol control** at the edge
- **Docker container support** for rapid edge processing
- **High input density:** each panel supports up to 16 doors and 128 inputs, reducing total cost per sensor
- **Extended protection:** perimeter coverage can expand hundreds to thousands of feet beyond the physical fence line

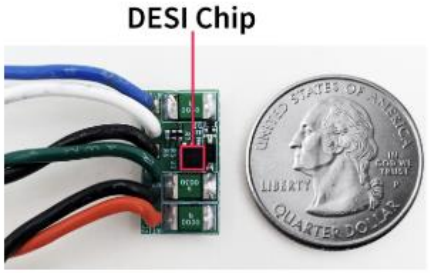
The UFP authenticates every session, applies protocol allowlists, and continuously re-verifies device identity. Data management can be securely distributed across the network, with processing occurring directly at the edge for greater efficiency and resilience.

Cost and Operational Benefits:

- Reduced SOC hardware, power, and cooling requirements
- Faster data collection and analysis at the edge
- Increased processing speed and system responsiveness
- Extended boundary protection using remote and mobile edge devices

PSG supports **OEM panel licensing agreements** and embraces a **Modular Open Systems Approach (MOSA)** for flexible integration.

ZTA for Legacy Devices — Digital Encrypted Security Interface (DESI) Controller



The **DESI controller** converts legacy analog signals into **PKI-encrypted, authenticated digital data**, preventing attackers from bypassing or injecting false signals into older infrastructure.

- Extends Zero Trust to legacy sensors and readers without replacing wiring or communication infrastructure
- Cryptographically validates each input before acceptance
- Installs at the sensor, replacing legacy **End-of-Line (EOL) resistors**
- Designed to cover the full PSE voltage range while maintaining signal integrity

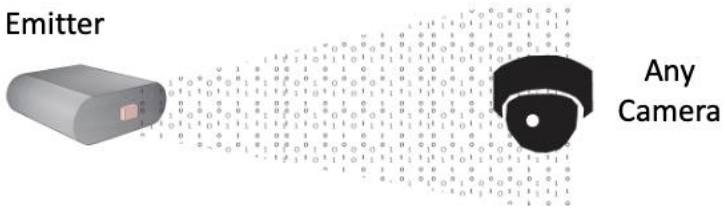
The **DESI PKI chip**, smaller than a pencil eraser, enables analog devices to achieve digital trust. PSG is licensing this patented chip to **OEM sensor, reader, and door hardware manufacturers**, allowing Zero Trust capabilities to be embedded at the factory level.
Future devices will ship **ZTA-ready out of the box**, making new ("greenfield") installations fully compliant from day one.

ZTA for Video Cameras - Scene Authentication™

PSG extends Zero Trust into the **scene itself** - beyond the camera lens - through its patented **Scene Authentication™** technology.

- Injects **encrypted light pulses** into the live video scene to verify that footage is authentic, live, and location-specific
- Prevents spoofing, replay, and video looping attacks that can bypass traditional frame-signing methods
- Provides **SDK/API integration** for any third-party camera or VMS

If the light pattern is interrupted, the system automatically triggers an alarm, confirming tampering or obstruction. Scene Authentication fulfills the Zero Trust requirement for **verified, trustworthy data streams** feeding analytics, AI, and digital twins.



ZTA for Video Management - VICADS® V100

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
- Supports both analog and IP video, enabling gradual modernization
- Provides **federal certifications** supporting use in nuclear and critical-infrastructure environments
- Directly supports the Zero Trust principle of "validated data flow" for AI and digital twin applications

Note: Scene Authentication can be integrated with **any camera or VMS**, VICADS is one implementation, not a requirement. PSG is open to **OEM agreements** for direct integration.

Cyber Security Solution (CSS) and Linx™ IQ

The **Cyber Security Solution (CSS)** provides continuous cyber compliance and management of authenticated data, while **Linx™ IQ** unifies command-and-control functions across intrusion, access, and video. Together, they consolidate situational awareness and ensure that only **verified and trusted data** reaches the Security Operations Center (SOC).

PSG's complete 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. Each component enforces Zero Trust directly at the device level, integrating seamlessly into a unified, open architecture.

PSG Brownfield Advantage

PSG products extend Zero Trust into legacy environments by securing existing infrastructure with minimal disruption. DESI modules replace legacy end-of-line resistors, instantly converting analog loops to digitally signed signals while reusing existing wiring. Scene Authentication software can be loaded onto deployed cameras, with emitters added to the field of view and beyond the camera lens, giving operators verified video without replacing infrastructure. These measures extend the life of legacy investments while closing the gaps that attackers target, delivering Zero Trust protection at lower cost and with minimal downtime.

03/

ZERO TRUST EDGE ARCHITECTURE USING PSG COMPONENTS

Zero Trust at the edge requires inline enforcement, continuous authenticated and validated (A-V) data pipelines from device to enterprise. PSG's architecture delivers this through a layered design built around its product suite.

PSG Greenfield Advantage

PSG products build Zero Trust from the start, embedding identity, verification, and enforcement into every layer of a new system. DESI modules can be specified as direct replacements for end-of-line resistors, ensuring analog inputs are digitally signed from installation day. 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 cheaper to secure, faster to certify, and resilient for the long term.

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 earliest possible point. DESI Controllers provide this binding for legacy analog inputs, while UFP panels natively authenticate digital inputs. Cameras are configured with scene authentication software and paired with ZTA Emitters to embed cryptographic scene verification for video.

Enforcement Layer

The UFP sits in line at the Edge -IT 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.

Video 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 VICADS V100 verifies in real time. This guarantees the authenticity of video data before it is displayed or stored.

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. UFP and VICADS outputs feed securely into Security Operations Centers (SOC), SIEMs, and cloud platforms, ensuring higher-level systems operate on verified inputs. PSG's CyberSecure Solution (CSS) and Linx IQ extend this by providing compliance enforcement, central logging, and cross-domain visibility.

High Performance Computing (HPC) – Supercomputer Architecture

At the core of this architecture is PSG's **HPC Zero Trusted Data Lake**, a high-performance computing cluster (HPC), utilizes a supercomputer architecture as a repository designed to securely store and process all edge activity data (intrusion, access, and video) locally on-premises.

For government networks, this architecture requires and achieves Authority to Operate (ATO) 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.

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 that Zero Trust principles can extend all the way to the far edge - to every sensor, reader, and camera.

As IT and OT converge, authenticated data has become the **new currency of trust**. PSG 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 make physical security as trusted, intelligent, and interoperable as IT and proven in the nation's most secure environments and ready for yours.

PSG's team is ready to help design, integrate, and scale Zero Trust protection across your enterprise. We stand ready to help you apply Zero Trust principles to your complex operating environment!

Key Outcomes

01/ Cyber Resilience
Eliminates vulnerabilities in analog and hybrid systems.

02/ Data Integrity
Cryptographically verifies every signal and frame from edge to cloud.

03/ AI Readiness
Supplies authenticated data streams for analytics, automation, and digital twins.

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

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 at *www.psgglobal.net*, tel: 512.247.3700.

References

[1] John Kindervag, *Build Security into Your Network's DNA: The Zero Trust Network Architecture*, Forrester Research, 2010.

