INDUSTRY INFLUENCER Q&A

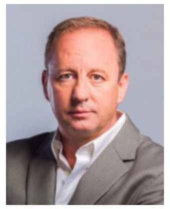
Sponsored By PROMETHEUS SECURITY GROUP GLOBAL

Incorporating Zero Trust in Corporate Security

Long used by government entities, Zero Trust principles are making their way to the mainstream in a big way

© Gorodenkoff / 312879613/Adobe Stock

The rise of connectivity – even across federal government agencies – is dominating the world of security and as the need to protect data continues to be at the forefront, long-established cybersecurity principles, such as Zero Trust, are making their way into physical security. In this exclusive industry influencer sponsored by Prometheus Security Group, President & CEO Rick Gross discusses the effect this will have on corporate security teams moving forward.



Rick Gross

What is Zero Trust?

Zero Trust principles, originally developed for cybersecurity, can be described as 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, data, and resources, resulting in restricted movement to only specifically authorized areas (in short, never trust, always verify). More simply put, Zero Trust means that no device, user, or system within a network should be trusted by default, regardless of whether it's inside or outside the corporate network perimeter.

Originally, the concept was developed in the early 1990s, and took hold across the federal government and its agencies, but more recently, 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.

Why is Zero Trust being incorporated into corporate security?

In essence, the extremely secure nature of security when applying Zero Trust principles is what's guiding enterprise and corporate security teams to adopt this methodology. The adoption of 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 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.

What are some of the benefits of Zero Trust for physical security?

Zero Trust principles applied to physical security enhance an organization's security posture by consistently applying measures across the network, reducing the risk of unauthorized access. This strategy involves implementing defense in depth with multiple security layers, including stringent user and device authentication for physical space access. Granular access controls ensure that only authorized individuals with specific permissions can enter certain areas or access assets, while the adaptable nature of Zero Trust frameworks accommodates evolving threats and technologies. By mitigating insider threats through continuous authentication, organizations can maintain compliance with regulatory standards, while also enabling quick detection and response to security incidents through continuous monitoring and anomaly detection mechanisms.

What are the foundational elements of Zero Trust implementation?

The foundational elements of Zero Trust implementation encompass visibility and analytics, automation and orchestration, and governance. Visibility and analytics involve gaining insights into the organization's security landscape, enabling proactive threat detection and response. Automation and orchestration streamline security processes, allowing for swift and effective actions in the face of potential threats. Governance establishes the framework for managing security policies and procedures, ensuring consistency and compliance across the organization. Together, these elements form the backbone of a robust Zero Trust strategy, bolstering the organization's resilience against evolving cyber threats.

What are the key pillars of achieving Zero Trust in cybersecurity?

The five pillars of Zero Trust include identity, devices, networks, applications and workloads, and data. Identity focuses on ensuring that only authorized users and entities access resources, employing strong authentication and context-based authorization. Devices entail securing all hardware and software connecting to networks, maintaining an inventory and managing vulnerabilities. Networks shift away from perimeter-based security to manage traffic flows and enhance visibility. Applications and workloads are continuously authorized with real-time risk analytics. Finally, data protection involves inventorying, categorizing, and labeling data, along with mechanisms to detect and prevent data exfiltration.

What challenges come with implementing Zero Trust in physical security systems?

Implementing Zero Trust in physical security systems presents several challengesk, including keeping up with evolving policies and standards, making cost-risk decisions regarding investment, seamlessly integrating cloud-based services, ensuring continuous monitoring capabilities, and addressing compatibility issues with legacy systems. Additionally, human factors such as organizational culture and employee education play a crucial role in successful implementation. Overcoming these challenges requires strategic planning, ongoing commitment, and investment in both technology and human resources.

How will artificial intelligence (AI) play a role in Zero Trust implementation in the future?

AI will play a pivotal role in implementing Zero Trust by automating monitoring and response processes within physical security systems. These AI tools will leverage machine learning algorithms to analyze vast amounts of data in real-time, identifying patterns and anomalies indicative of potential security threats. By automating these tasks, AI not only helps alleviate the burden on human operators but also enables faster and more accurate threat detection and response. Additionally, AI-powered solutions can adapt and learn from evolving threats, enhancing the overall effectiveness and resilience of Zero Trust security measures. ⛊

For more information visit:
https://psgglobal.net/
Phone: (512) 247-3700
Email: sales@psgglobal.net