Agentless Zero-Trust:

Clientless SASE over 5G for Secure IoT/OT at Scale

Presented by:
Milind Gunjan

Disclaimer

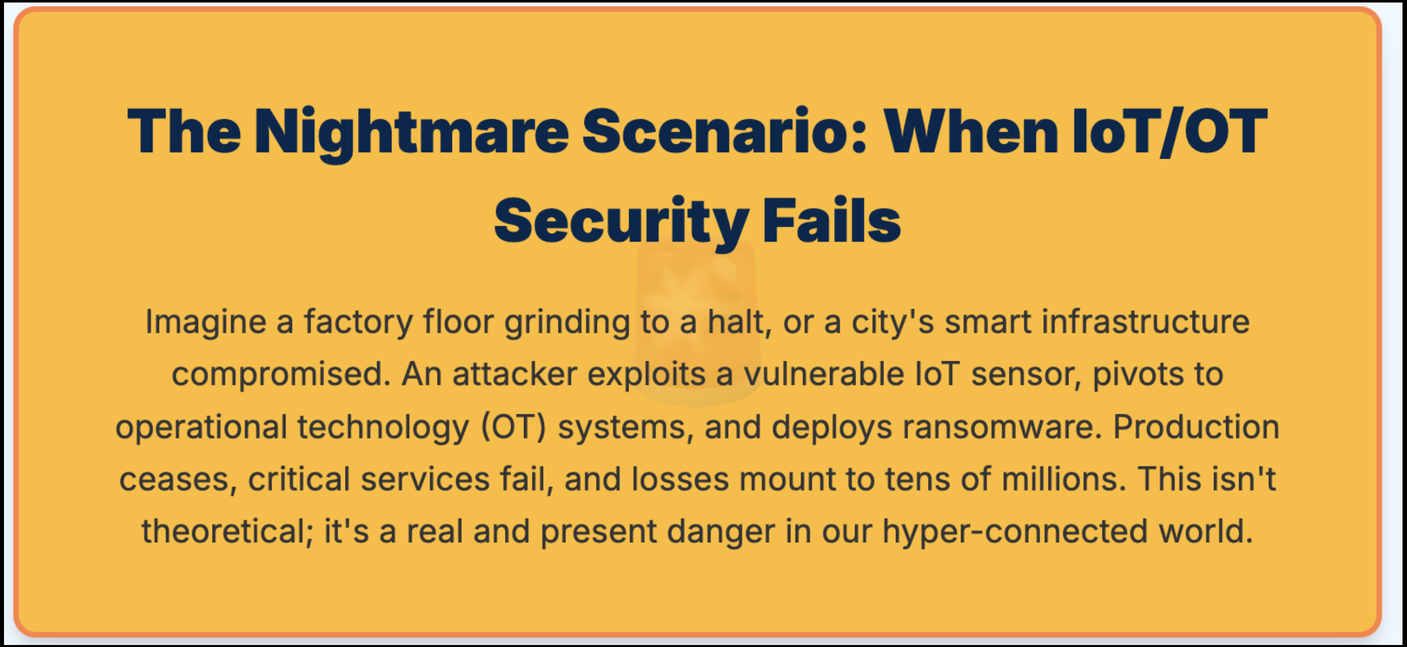
This presentation represents my own research and professional insights.
It is presented in a personal capacity and does not represent the views, positions, or endorsements of AWS or any other organization.

$whoami

- A seasoned telecom and cloud-native security Architect
- Recognized member of the Forbes Technology Council, advising on 5G security, zero trust, and IoT protection.
- Holds multiple patents in SIM-driven zero-trust and 5G-smart SASE architectures—including dynamic policy-driven threat mitigation for cellular IoT—that have enabled real-world defense of critical infrastructure and industrial metaverse environment.

The Unseen Risk: A Hyper-Connected World

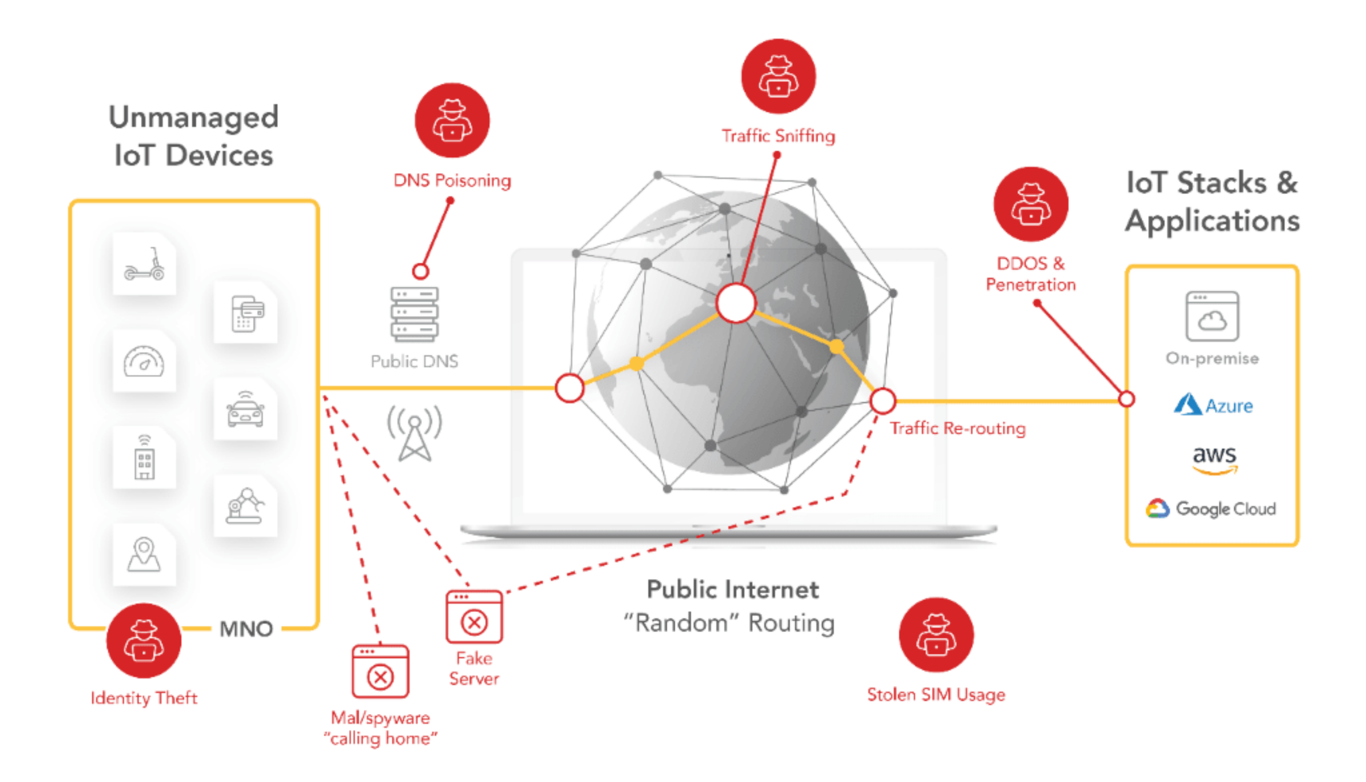
The number of connected devices is skyrocketing, creating a massive, often invisible, attack surface.



The Nightmare Scenario: When IoT/OT Security Fails

Imagine a factory floor grinding to a halt, or a city's smart infrastructure compromised. An attacker exploits a vulnerable IoT sensor, pivots to operational technology (OT) systems, and deploys ransomware. Production ceases, critical services fail, and losses mount to tens of millions. This isn't theoretical; it's a real and present danger in our hyper-connected world.

IoT Security Challenges

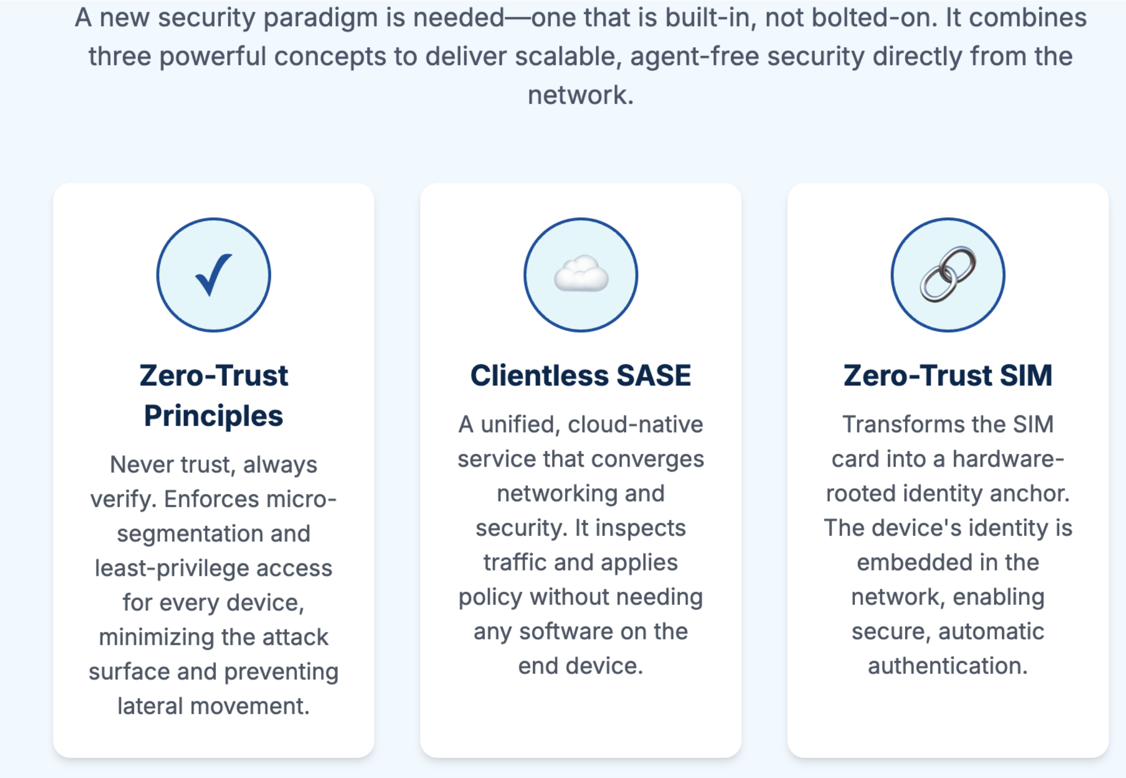


Why Traditional Security Fails

Legacy security models like VPNs and agent-based software are fundamentally incompatible with the diverse, resource-constrained, and distributed nature of modern IoT/OT devices, leaving them vulnerable.

Category	Traditional Security (VPNs/Agents)	Clientless SASE & Zero-Trust SIM
Security Model	Perimeter-based (trusts anything inside)	Identity-driven ("never trust, always verify")
Agent Requirement	Dependent on installing software clients	Agentless by design for IoT/OT
Scalability	Struggles with scale; creates bottlenecks	Cloud-native and highly scalable
Visibility	Limited, disruptive, or impossible on IoT	Unified, real-time, non-disruptive
Policy Enforcement	Broad and static (e.g., full network access)	Granular, dynamic, and context-aware

The Agentless Zero-Trust Revolution



A new security paradigm is needed—one that is built-in, not bolted-on. It combines three powerful concepts to deliver scalable, agent-free security directly from the network.

Zero-Trust Principles

Never trust, always verify. Enforces micro-segmentation and least-privilege access for every device, minimizing the attack surface and preventing lateral movement.

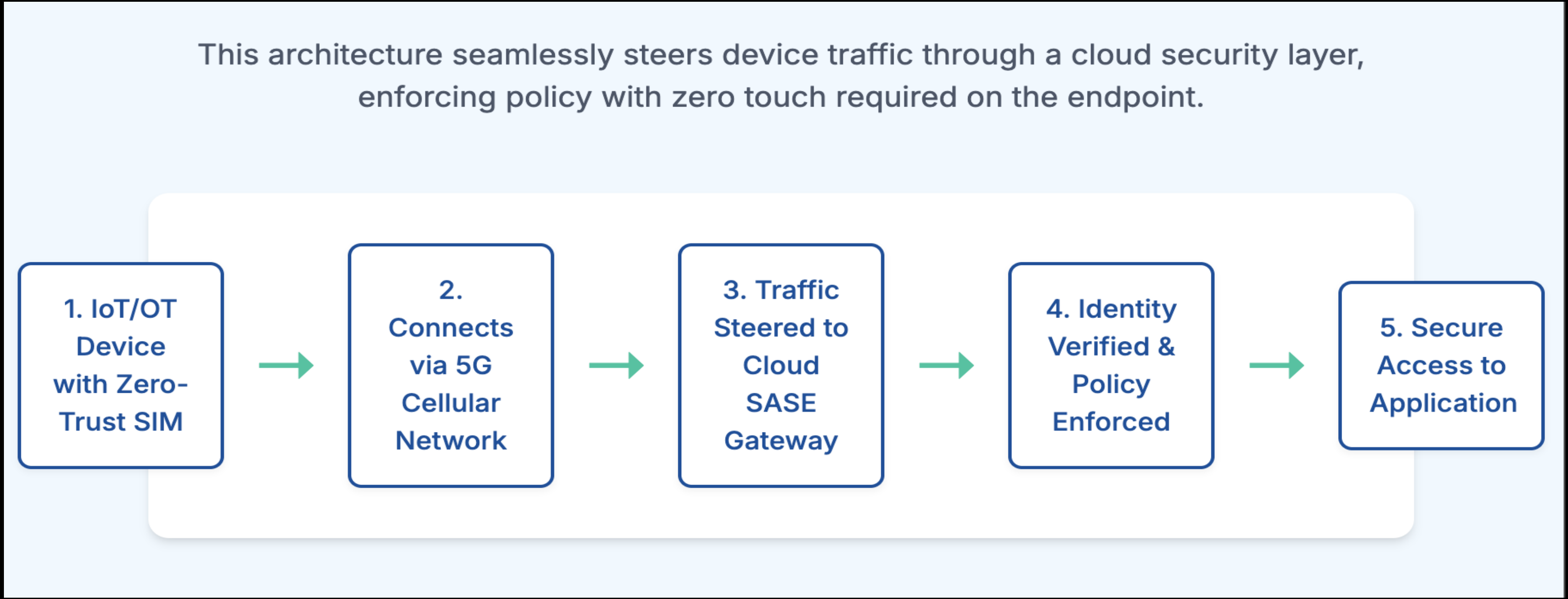
Clientless SASE

A unified, cloud-native service that converges networking and security. It inspects traffic and applies policy without needing any software on the end device.

Zero-Trust SIM

Transforms the SIM card into a hardware-rooted identity anchor. The device's identity is embedded in the network, enabling secure, automatic authentication.

How It Works: Security Embedded in the Network

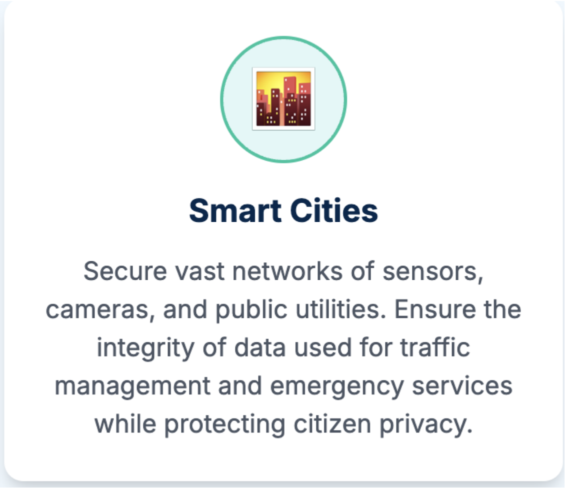


This architecture seamlessly steers device traffic through a cloud security layer, enforcing policy with zero touch required on the endpoint.

1. IoT/OT Device with Zero-Trust SIM → 2. Connects via 5G Cellular Network → 3. Traffic Steered to Cloud SASE Gateway → 4. Identity Verified & Policy Enforced → 5. Secure Access to Application

Securing the Future: Real-World Applications

- From factory floors to smart cities, agentless Zero Trust provides the foundational security needed to enable the next wave of innovation safely.



Smart Cities

Secure vast networks of sensors, cameras, and public utilities. Ensure the integrity of data used for traffic management and emergency services while protecting citizen privacy.

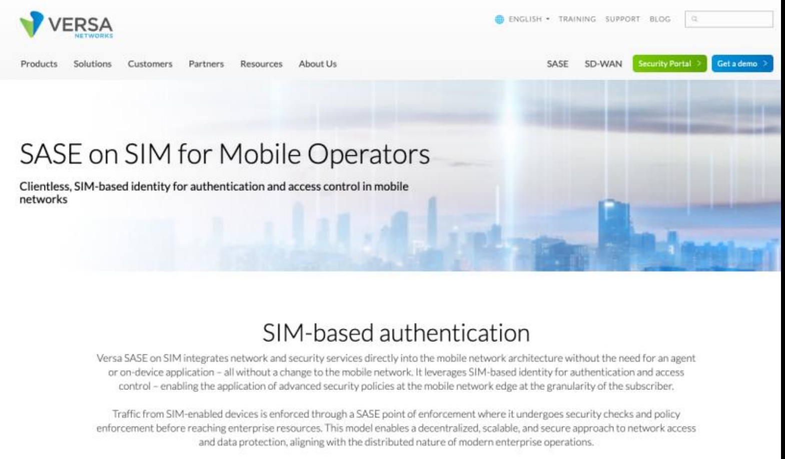
Industrial Metaverse

Provide the trusted, low-latency connectivity required for real-time digital twins and remote-operated machinery, enabling innovation without compromising security.

Critical Infrastructure

Protect power grids, manufacturing plants, and logistics. Isolate OT systems to prevent lateral movement and ensure operational uptime and physical safety, even for legacy equipment.

Competitive landscape



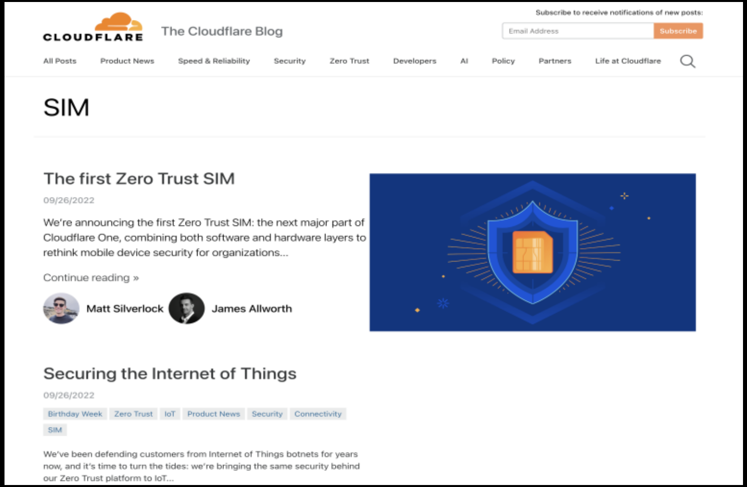
SASE on SIM for Mobile Operators

Clientless, SIM-based identity for authentication and access control in mobile networks

SIM-based authentication

Versa SASE on SIM integrates network and security services directly into the mobile network architecture without the need for an agent or on-device application – all without a change to the mobile network. It leverages SIM-based identity for authentication and access control – enabling the application of advanced security policies at the mobile network edge at the granularity of the subscriber.

Traffic from SIM-enabled devices is enforced through a SASE point of enforcement where it undergoes security checks and policy enforcement before reaching enterprise resources. This model enables a decentralized, scalable, and secure approach to network access and data protection, aligning with the distributed nature of modern enterprise operations.



SIM

The first Zero Trust SIM

09/26/2022

We're announcing the first Zero Trust SIM: the next major part of Cloudflare One, combining both software and hardware layers to rethink mobile device security for organizations...

Continue reading »

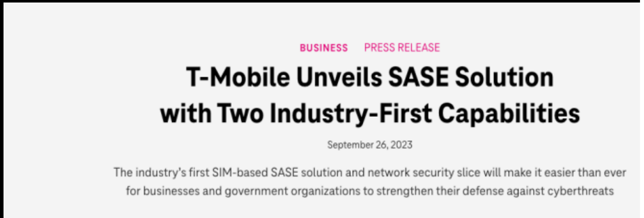
Matt Silverlock James Allworth

Securing the Internet of Things

09/26/2022

Birthday Week · Zero Trust · IoT · Product News · Security · Connectivity · SIM

We've been defending customers from Internet of Things botnets for years now, and it's time to turn the tides: we're bringing the same security behind our Zero Trust platform to IoT...

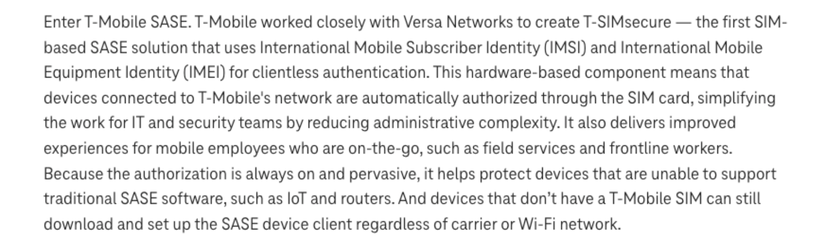


BUSINESS PRESS RELEASE

T-Mobile Unveils SASE Solution with Two Industry-First Capabilities

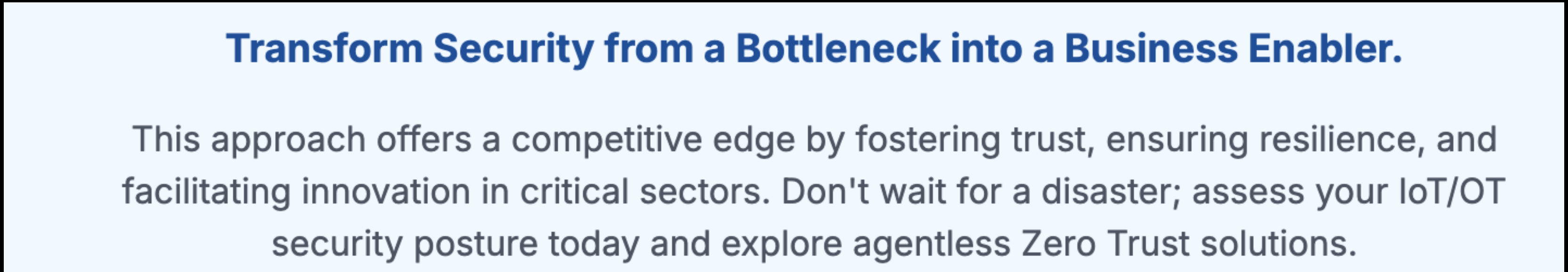
September 26, 2023

The industry's first SIM-based SASE solution and network security slice will make it easier than ever for businesses and government organizations to strengthen their defense against cyberthreats



Enter T-Mobile SASE. T-Mobile worked closely with Versa Networks to create T-SIMsecure — the first SIM-based SASE solution that uses International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) for clientless authentication. This hardware-based component means that devices connected to T-Mobile's network are automatically authorized through the SIM card, simplifying the work for IT and security teams by reducing administrative complexity. It also delivers improved experiences for mobile employees who are on-the-go, such as field services and frontline workers. Because the authorization is always on and pervasive, it helps protect devices that are unable to support traditional SASE software, such as IoT and routers. And devices that don't have a T-Mobile SIM can still download and set up the SASE device client regardless of carrier or Wi-Fi network.

Embrace the Future of Built-In Security



Transform Security from a Bottleneck into a Business Enabler.

This approach offers a competitive edge by fostering trust, ensuring resilience, and facilitating innovation in critical sectors. Don't wait for a disaster; assess your IoT/OT security posture today and explore agentless Zero Trust solutions.