eBook

Top 10 Edge Security Threats and How Operational Zero Trust Alleviates Them

FREEWAVE

FREEWAVE

In the rapidly evolving landscape of Operational Technology (OT) and Industrial Internet of Things (IIoT), edge environments are increasingly vulnerable to sophisticated cyber threats that can disrupt operations, compromise safety, and incur significant financial losses. Traditional security models, reliant on perimeter defenses, fall short in addressing the distributed nature of modern industrial systems. This paper explores the top 10 edge security threats facing OT and IIoT, drawing from industry insights and real-world incidents, and demonstrates how FreeWave's Operational Zero Trust™ (OZT) principles, implemented through FreeWave Zentry™ security solutions, provide a robust, scalable defense.

By adopting the Zentry security architecture, organizations can eliminate exposed attack surfaces, enforce least-privilege access, and achieve rapid deployment without disrupting existing operations.

The convergence of IT and OT has transformed industrial operations, enabling real-time data analytics, remote monitoring, and automation. However, this integration has expanded the attack surface, particularly at the edge where devices like PLCs, sensors, and gateways interface with the physical world. In industrial operations the stakes are high: a single breach can halt production, endanger lives, or expose sensitive data, and cost millions.

According to the 2023 Verizon Data Breach Investigations Report, OT systems are increasingly targeted, with 80% of incidents involving credential abuse or exploitation of remote services [1]. Ransomware attacks on industrial sectors rose by 87% in 2022, per Dragos' Year in Review [2]. These statistics underscore the need for a paradigm shift from traditional firewalls to identity-centric models like Operational Zero Trust.

The practice of OZT reframes IoT and IIoT security by assuming no implicit trust: authenticating before connecting, micro segmenting by default, and eliminating persistent access paths. The Zentry solution embodies these principles, offering outbound-only connections, device-level identity enforcement, and deterministic logging. This paper outlines the top threats, how Zentry security controls mitigate them, and implementation strategies, positioning Zentry security capabilities as an essential tool for decision-makers evaluating security investments.

FREEWAVE

Top Edge Security Threats in OT and IIoT

Edge environments in OT and IIoT are prime targets due to their distributed architecture and legacy components. Below, we detail the top 10 threats:

1.Expanding Attack Surface at the Edge

Industrial environments now rely on thousands of distributed edge devices such as PLCs, sensors, cameras, and controllers. Every new device increases the number of potential entry points attackers can target. Traditional perimeter security was never designed to protect this level of distribution.

Why it matters: A larger attack surface increases the likelihood of unauthorized access and undetected compromise.

How FreeWave solves it:
The Zentry solution enforces identity at the device level. Every device must authenticate before any connection is allowed. If a device is not explicitly trusted, it is invisible and unreachable. Operational Zero Trust reduces the attack surface by design rather than attempting to monitor it after exposure.

2.Legacy Devices Without Built In Security

Many OT devices were engineered for uptime and longevity, not cybersecurity. They often lack authentication, encryption, or patching capabilities, making them easy targets.

Why it matters: Legacy equipment becomes a weak entry point that attackers can exploit to access the broader environment.

How FreeWave solves it:
FreeWave Zentry zero trust overlay applies security at the network and session layer without requiring agents. Identity based access and encryption are enforced externally, allowing legacy devices to participate in a Zero Trust model without modification.

3. Insecure Remote Access Paths

VPNs and remote access tools typically require inbound ports, static IPs, or shared credentials. These methods expose systems directly to the internet and are frequently abused.

Why it matters: Remote access is one of the most common entry points for ransomware and OT intrusions.

How FreeWave solves it:
The Zentry solution uses outbound only connections with authenticate before connect enforcement. There are no open inbound ports and no static tunnels. Unauthorized users cannot even see the environment, let alone access it.

4. Ransomware Targeting Operational Systems

Ransomware attacks increasingly target OT environments because downtime directly impacts revenue and safety. Once inside, attackers often move laterally across flat networks.

Why it matters: A single compromised device can shut down production lines or critical services.

How FreeWave solves it:
The FreeWave Zentry solution enforces strict micro segmentation and session level policy. Devices and users only connect to exactly what they are authorized to access. Lateral movement is blocked by default, limiting the blast radius of any compromise.

FREEWAVE

5. Lack of Visibility Into Edge Activity
Many organizations have limited insight into what devices are connected, how they communicate, and when access occurs.

Why it matters: Without visibility, attacks often go unnoticed until damage is already done.

How FreeWave solves it:
The Zentry solution produces clean, deterministic logs for every access decision and session. These logs integrate with SIEM platforms, giving security and operations teams clear visibility into who connected, when, and to what.

6. Weak or Missing Authentication
Default credentials, shared passwords, or no authentication at all remain common in OT environments.

Why it matters: Attackers can gain access with minimal effort using credential stuffing or brute force techniques.

How FreeWave solves it:
Operational Zero Trust requires explicit authentication for every device and user. The Zentry solution enforces identity verification before any connection is established, eliminating anonymous or implicit trust.

> **When you compare the FreeWave Zentry zero-trust based solution to traditional alternatives like VPNs, the return on investment becomes clear**

7. Shadow OT Devices and Unmanaged Assets
Untracked devices are often deployed in the field without security oversight. These devices frequently operate outside monitoring and policy controls.

Why it matters: Unknown devices create blind spots that attackers can exploit.

How FreeWave solves it:
Only enrolled and authenticated devices can communicate through the Zentry system. If a device is not known, it cannot connect. This eliminates shadow OT by enforcing policy at the point of connection.

8. Insecure Legacy Protocols
Industrial protocols such as Modbus and DNP3 were not designed with security in mind. They often transmit data in clear text and trust the network implicitly.

Why it matters: Attackers can inject commands or manipulate data without detection.

How FreeWave solves it:
The Zentry solution encrypts all data in motion and enforces identity-based session control regardless of protocol. Even legacy communications are protected by Operational Zero Trust controls.

9. Third Party and Vendor Risk
Vendors and contractors often require access to OT systems for maintenance and support. Traditional access methods grant broad permissions that are difficult to control or audit.

Why it matters: Third party access increases the risk of accidental or malicious misuse.

How FreeWave solves it:
The FreeWave Zentry solution provides just in time, least privilege access for vendors. Access is identity based, time limited, and fully logged, ensuring vendors only access what they need and nothing more.

10. Misconfiguration and Human Error
Complex security stacks increase the likelihood of misconfigurations such as exposed ports or overly permissive rules.

Why it matters: Misconfigurations are one of the leading causes of security incidents.

How FreeWave solves it:
The Zentry solution simplifies secure connectivity through centralized policy and automation. Operational Zero Trust reduces reliance on manual configuration by enforcing consistent controls everywhere.

These threats are interconnected, often escalating from a single-entry point to systemic compromise. In sectors where remote assets are common, exposure to internet-facing devices heightens these risks.

Implementation and Benefits of Zentry in IT/OT Environments

Deploying Zentry zero-trust security solutions in converged IT/OT environments is remarkably straightforward for security leaders and engineering teams. Installation typically completes in minutes, and it can be validated during a low-risk 30-day field proof-of-value (POV) to validate performance in your specific operating conditions. Scaling across the network requires no modifications to existing firewall rules, enabling rapid enterprise-wide adoption without disrupting operations.

FreeWave OZT and the Zentry solution deliver several critical attributes that address the unique challenges of industrial networks:

- Elimination of lateral movement: Attackers cannot traverse the network even if an initial compromise occurs.
- Invisible security posture: Devices and assets are hidden from unauthorized discovery, significantly reducing the attack surface.
- Built-in automation: Policy enforcement and key management are automated, minimizing configuration errors that often introduce vulnerabilities.

The resulting benefits are both immediate and strategic:

- Operational Resilience: By containing threats such as ransomware at the point of entry, the solution minimizes costly downtime and maintains continuous production.
- Cost Efficiency: Organizations can avoid layered, complex security stacks. The streamlined model reduces both capital expense and ongoing management overhead.
- Regulatory Compliance: Full support is provided through comprehensive logs that simplify reporting and audits.
- Enhanced Vendor Management: Time-bound, granular access controls improve third-party accountability while reducing risks associated with external connections.

Real-world deployments in comparable industrial environments have demonstrated up to a 90% reduction in exposed attack surfaces [9]. When integrated with existing FreeWave wireless infrastructure, the Zentry overlay enables organizations to achieve a robust zero-trust posture that not only strengthens security but also delivers a measurable competitive advantage through improved reliability and reduced operational risk.

Challenges and Considerations

As with any new integration, encountering challenges when adopting OZT particularly in established OT environments may include cultural shifts. These often arise as teams move away from long-standing legacy mindsets that rely on implicit trust and perimeter-based defenses. Integrating Zentry security capabilities into brownfield sites, with their mix of aging infrastructure and existing workflows, can also require careful planning.

These hurdles are manageable. Comprehensive training programs help your teams embrace the identity-first approach, while phased rollouts allow you to deploy Zentry security controls incrementally, minimizing disruption to ongoing operations. Starting with a low-risk 30-day proof-of-value (POV) lets you validate performance in your specific environment before broader commitment, and scalable pricing models align costs with your deployment pace. FreeWave's award-winning support organization and staff are there to help you every step of the way.

When you compare the FreeWave Zentry zero-trust based solution to traditional alternatives like VPNs, the return on investment becomes clear: the Zentry solution prevents incidents upfront through design rather than reacting after a breach, reducing both direct recovery costs and operational downtime [10].

Aspect	Traditional Security	FreeWave OZT
Exposure	Inbound ports open	Nothing exposed
Deployment Time	Weeks or more	Minutes
Lateral Movement	Possible	Blocked by default
Visibility	Limited	Deterministic logging

References
[1] Verizon. (2023). Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/
[2] Dragos. (2023). OT Cybersecurity Year in Review. https://www.dragos.com/year-in-review/
[3] NIST. (2022). SP 800-82r3: Guide to Operational Technology (OT) Security. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf
[4] SANS Institute. (2023). ICS/OT Cybersecurity Survey. https://www.sans.org/reading-room/whitepapers/ICS/
[5] CISA. (2021). Colonial Pipeline Cyber Incident. https://www.cisa.gov/news-events/alerts/2021/05/10/colonial-pipeline-cyber-incident
[6] FireEye. (2020). SolarWinds Supply Chain Compromise. https://www.mandiant.com/resources/solarwinds-supply-chain-compromise
[7] MITRE. (2023). ATT&CK for ICS. https://collaborate.mitre.org/attackics/
[8] IEC. (2021). 62443: Security for Industrial Automation and Control Systems. https://webstore.iec.ch/publication/7029
[9] Forrester. (2022). The Total Economic Impact of Zero Trust. https://www.forrester.com/report/The-Total-Economic-Impact-Of-Zero-Trust/
[10] Gartner. (2023). Market Guide for Zero Trust Network Access. https://www.gartner.com/en/documents/4012345

Empowering Your Network, Securing Your Investments

Edge security threats in OT and IIoT demand advanced solutions like Operational Zero Trust. The FreeWave Zetry solution empowers CISOs, operational owners, and engineering managers to make informed procurement decisions, reducing risks while enhancing efficiency. By implementing Zentry security strategies, organizations can achieve a secure, modern industrial edge.

Test is out, contact us to start your own 30-day POV to experience these benefits firsthand. Or ask for a 1:1 OZT workshop to uncover the weaknesses in your network, today.

Invest in FreeWave today to protect tomorrow's operations.

FREEWAVE CORPORATE HEADQUARTERS

5395 Pearl Parkway
Boulder, CO 80301

Toll Free +1 866.923.6168
Local +1 303.381.9200

www.freewave.com/zentry
FW_10ZentryEB_1225