eBook

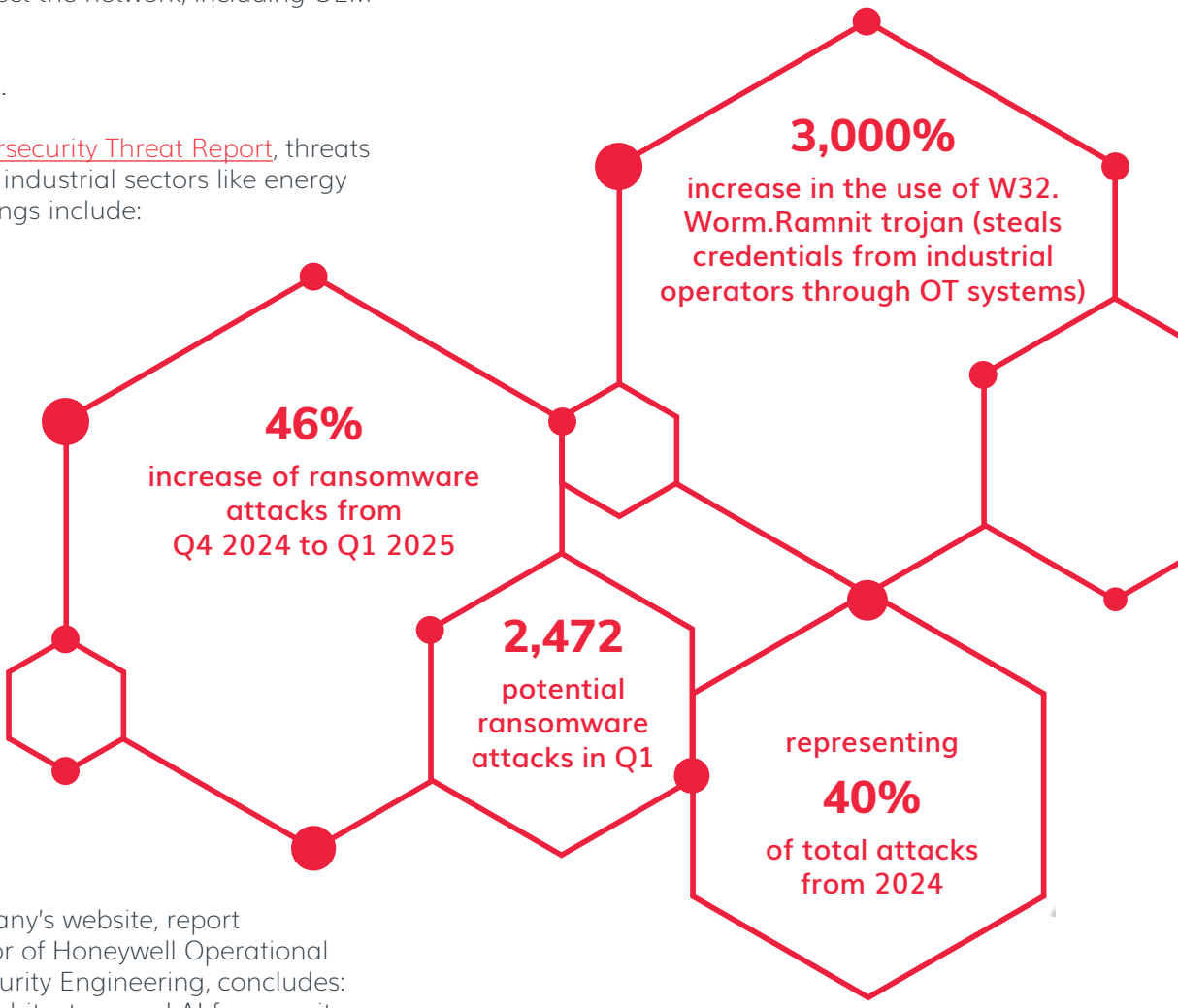
How Integrating Network Security into OEM Solutions Adds Product Value

Most cellular gateway and edge compute devices from original equipment manufacturers (OEMs) don't play in the network security space. They don't identify with security because it's "not native to the device or what we sell." Instead, they're in the business of delivering reliable and robust connectivity solutions. This is true – in part.

While some OEMs may have security fabrics, usually there's another vendor or specialist swimming in the cybersecurity lane to protect the network, including OEM devices.

Yet, the world is changing.

In Honeywell's 2025 Cybersecurity Threat Report, threats have escalated for critical industrial sectors like energy and manufacturing. Findings include:



In an article on the company's website, report author Paul Smith, director of Honeywell Operational Technology (OT) Cybersecurity Engineering, concludes: "Leveraging Zero Trust architecture and AI for security analysis can speed detection and enable smarter decision making and proactive defense in an increasingly complex digital landscape."

That's one reason future-ready OEMs are modernizing IIoT portfolios by integrating security into edge, connectivity, and compute devices. They're pulling away from the pack – and making resilience part of their value proposition.

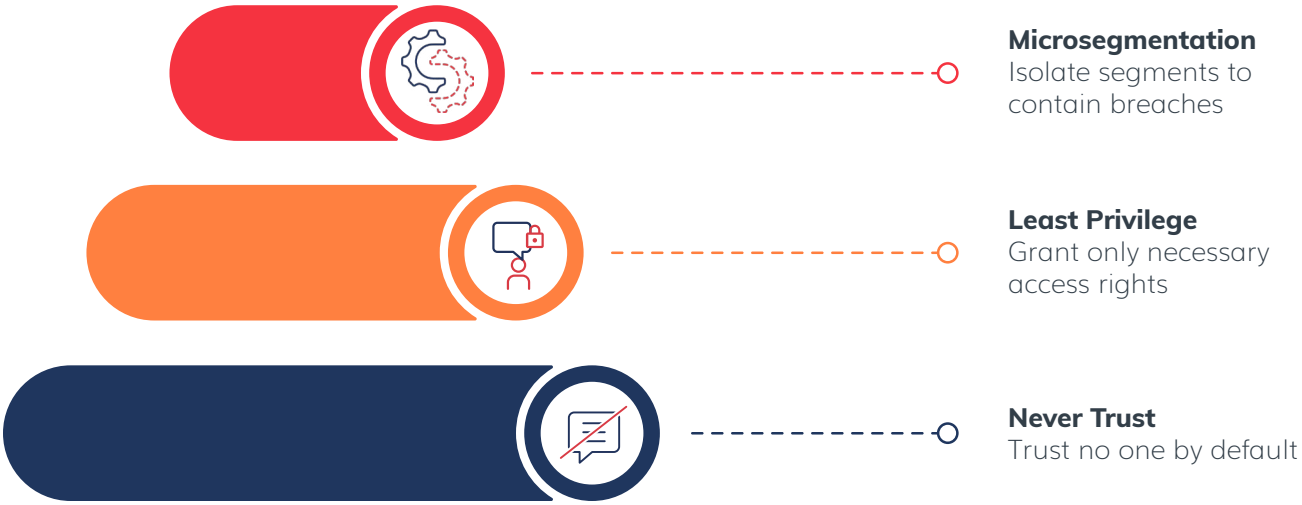
FREEWAVE

Network Security Starts with Zero Trust

To understand zero trust, we turn to the National Institute of Standards and Technology (NIST). NIST defines zero-trust architecture as securing "authorized access to enterprise resources that are distributed across on-premises and multiple cloud environments, while enabling a hybrid workforce and partners to access resources from anywhere, at any time, from any device in support of the organization's mission." In other words, zero trust provides unprecedented security with agility.

Scott Alldridge, author of "The Visible OPS Cybersecurity: Enhancing Your Cybersecurity Posture with Practical Guidance," points out that the fundamental difference between traditional security models and zero trust is "continuous validation of user identities and device integrity" versus one-time verification.

Zero Trust Security Pyramid



Microsegmentation
Isolate segments to contain breaches

Least Privilege
Grant only necessary access rights

Never Trust
Trust no one by default

FREEWAVE

Rethinking the Value Proposition for OEMs

In today's world, top leaders – CEOs, CIOs, CISOs, and CFOs – are oftentimes liable for compliance. Failing penetration testing (PEN testing) can lead to vulnerabilities and rising insurance premiums. The pressure of thwarting security breaches and hacks demand a robust solution that lowers costs and increases network security without complex solutions from multiple vendors.

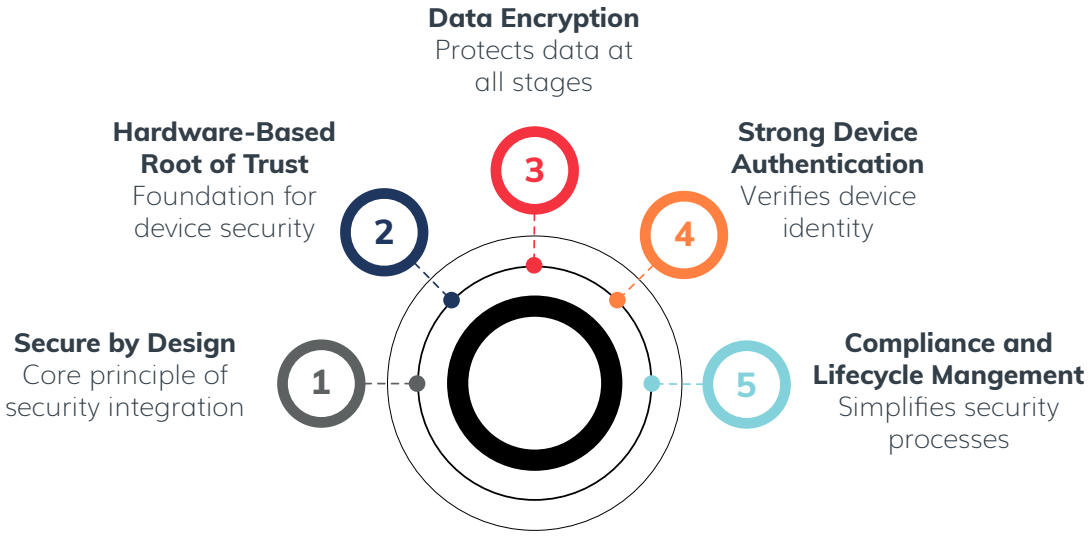
So what is the value proposition of adding security to an OEM's device?

"If you were just offering a communications device before, you could be looking at increased network security through the same lens as everyone else," said Michael Tate, chief operating officer and senior vice president of global sales and marketing for FreeWave. He adds, "The outcomes transform commodity-priced hardware into a differentiated solution."

"Today you are selling hardware and tomorrow you are selling a valuable solution with ARR, all while becoming more relevant to your customer and solving real security problems over just connectivity. If you have devices that give you security and also include communications, you're going to win faster."

> **"If you have devices that give you security and also include communications, you're going to win faster."**
>
> Michael Tate
> *COO and SVP of Global Sales and Marketing,* FreeWave

Secure by Design for OEM Solutions



The importance of cybersecurity extends to our readiness as a nation. Thousands of OEMs contribute to the U.S. defense industrial supply chain across 16 critical infrastructure sectors. According to the U.S. Department of Defense Cybersecurity Strategy, the first of its kind in the country's history, ensuring our safety means having "a cybersecurity framework built upon zero trust principles." As the network is continuously monitored, a zero trust security approach gives systems administrators time to focus on highest-risk items and stay ahead of threats. The Department of Defense has committed to fully deploy zero trust by the end of 2027.

How is security evolving for OEMs?

Secure by design is a principle that prioritizes security early in design rather than leaving it as an afterthought.

Industrial sectors like oil and gas, energy, municipal water and wastewater departments use thousands of devices across a network. These assets have multiple contracts and multiple vendors. A disgruntled employee or third-party vendor has the potential of seeing everything and doing serious damage with traditional security. A minute of downtime can cost millions. Take North America's largest steel producer, $30B Nucor, as an example. Its data breach in May 2025 due to "unauthorized third-party access" triggered shutdowns at multiple facilities.

As IT/OT integration grows, the Nucor data breach underscores how cyberattacks are growing in sophistication right along with the attack surface, which includes IIoT devices, communications, gateways, sensors, robotics, industrial routers, PLCs, and wireless access points.

Security is becoming everyone's concern, especially forward-thinking OEMs of industrial-grade networking hardware and edge devices like cellular routers, gateways, servers, and modems. Secure by design products give OEMs a competitive advantage in a crowded marketplace.

FreeWave Zentry™: Making a Network Invisible

The FreeWave Zentry solution is a zero-trust based security solution. It cloaks networks, making them "invisible" utilizing a simple concept: never trust, always verify. This means the system doesn't automatically trust anyone or anything trying to connect to it – even if they're coming from inside the network. Instead, every access request attempting to access resources is verified whether from a user, device, or application, no matter where they originate.

The Zentry solution is the first secure connectivity solution built on zero-trust principles for OEMs looking to integrate security in the development phase – and can be installed on most OEM remote devices that meet a minimum set of requirements. OEMs in small, niche markets to mass-produced industrial-grade products can embed Zentry in agricultural products, automation technology, and edge devices.

Devices include:

- Edge devices
- Connectivity devices such as cellular gateways and modems
- Compute devices like servers, desktops, and laptops

Zentry-enabled networks are "invisible" to the public, encrypted with no public IPs, open inbound ports, or static tunnels to scan or exploit. Identify-driven access appears only when needed and disappears when complete, leaving no standing exposure so authorized users, devices, or applications are granted the minimum necessary access rights. Those rights are continuously monitored and adjusted as necessary. Deterministic control removes noise, helping small security teams focus on real threats without wasting valuable time on false positives.

Imagine: instead of having a single wall around your castle (traditional perimeter-based security), everyone's

IDs are checked at every door, every time they want to enter a room. If a threat breaches a room, the risk is limited to that room, not the entire castle (this is called microsegmentation). Even further, with the Zentry solution enabled, the risk is further segmented and walled off from people ever seeing the rest of the network.

This approach minimizes risk because it assumes there's always a potential threat, externally or internally.

Transforming the Customer Experience for OEMs

Tate says the value add, ease of use, and security benefits of a device with the FreeWave Zentry solution is a trifecta for OEMs. Adding Zentry security increases revenue, growth, and customer satisfaction.

Since the Zentry solution can be applied directly onto a network server, it saves an OEM's end customer valuable time and money by eliminating touch points they otherwise would have to address: a host, multiple SIM cards, a central console, an independent carrier, edge devices, static IPs. The Zentry solution initiates outbound connections only so there are no open inbound ports and no vulnerabilities to port scanning because all avenues for outside access are closed.

"We're working with an OEM edge device manufacturer whose products are in more than 150 countries," said Tate. "We're setting them up to securely transport data using the Zentry solution and the Zentry console. This makes their cellular gateway products more valuable and moves them from a commodity product fighting for the price point to a network security solution that prioritizes end customer needs."

"We're setting them up to securely transport data using the Zentry solution and the Zentry console. This makes their cellular gateway products more valuable and moves them from a commodity product fighting for the price point to a network security solution that prioritizes end customer needs."

Michael Tate
COO and SVP of Global Sales and Marketing, FreeWave

Tate says that embedding the Zentry solution in a product allows the OEM to go horizontal in the value chain. Every slot an OEM fills for a customer saves them stress and work. Embedded cybersecurity gives OEMs a stronger value proposition as an innovator and brand leader. The Zentry security solution can be integrated into a variety of OEM products and environments, including:

- Linux® boxes
- Cellular gateways
- Docker™ and containers
- Mobile phones
- Laptops
- iPad®
- macOS®
- Mobile or Android®
- iOS®

FREEWAVE

When an OEM product includes integrated cybersecurity, end customers save significant time and effort negotiating with carriers, managing SIM cards, configuring complex network settings like VPNs and static IPs, and coordinating with multiple vendors for security solutions. This streamlines billing, reduces administrative overhead, and eliminates the need for specialized IT resources to maintain separate security infrastructure.

The result?

A simpler, more secure, and cost-effective experience for an OEM's end customer. In a fast-changing world, one question to ask for OEMs is: Do you want to be what you've always been or add more value as a point of differentiation?

Recurring Revenue Stream for OEMs

The Zentry console is intuitive and can be configured in minutes. From the console, an OEM has a panoramic view of users, the network, and applications. Here, OEMs have an opportunity to extend their expertise. As a managed service or SaaS product, layering the Zentry security solution onto a device takes security monitoring off the shoulders of end customers.

For example, an OEM could bundle the Zentry solution as part of a premium service package, charging customers a recurring monthly fee for enhanced security, simplified network management, and reduced need for traditional VPNs and static IP configurations. **The Zentry console becomes a software management tool providing a new revenue stream for OEMs.**

Zentry is built for the edge and works seamlessly in OT, IoT, and disconnected environments where most zero trust tools cannot operate. OEMs can expect simple integration as Zentry works alongside existing security operations centers (SOCs), security information and event management (SIEM) tools, and firewall tools without complex reconfiguration.

FREEWAVE

Adding "Zen" to Product Value

In the Japanese arts, Zen means peace and calm, deeply rooted in intuition. The Zentry solution gives this same peace of mind for OEMs and their end customers.

In the AI era, critical data is increasing. IIoT devices at the edge are multiplying. IT and OT continue to converge. Amidst this rapid change, FreeWave is making the Razor's Edge™ simple, secure, and connected.

Our long view is on the edge, where unmanned, remote assets are spread out, oftentimes powered by batteries and solar. Along the network, a heartbeat goes back and forth, verifying important data coursing through critical infrastructure, from pump or valve or other device to people. Oftentimes unsecured, these highly volatile assets require ironclad security for uninterrupted business operation.

When you choose FreeWave, you choose resilience over risk for your OEM customers. Learn more about the FreeWave Zentry solution and start integrating security into your OEM solution, delivering greater value and differentiation in the marketplace.

FreeWave Technologies, Inc. continues to transform industrial communication with more than 30 years of proven, proprietary radio technology deployed in the world's most demanding environments. We're delivering open-standards wireless networks, AI-powered edge applications, an integrated cloud platform, and edge solutions secured by FreeWave's Zentry zero trust architecture. FreeWave secures the entire data lifecycle, from collection to monetization. Backed by a strong IP portfolio and global partnerships, we're built for the future of industrial intelligence.

FREEWAVE CORPORATE HEADQUARTERS

5395 Pearl Parkway
Boulder, CO 80301

Toll Free +1 866.923.6168
Local +1 303.381.9200

Email: insidesales@freewave.com
Visit: freewave.com

FREEWAVE