Smart connectivity for an even smarter factory

Executive summary

The manufacturing industry is profoundly transforming, driven by Industry 4.0 technologies such as IoT, robotics, AI and automation. Reliable and secure connectivity throughout the core value stream is critical to enabling these advancements, making private wireless and improved indoor coverage a compelling proposition.

It is clear the role that Verizon plays as an enabler in this transformation, and this document explores Verizon's point of view on the network architecture that provides the foundation for a continuing transformation journey. The architecture considers all modern connectivity options ranging from wired connectivity (e.g. fiber, ethernet, Internet and Private IP) and wireless connectivity (e.g. Private Wireless, Wi-Fi, Satellite). The architecture also explains how to secure the network and segment the traffic flow to provide business continuity, as well as enable modern and digital-forward manufacturing where Information Technology (IT) and Operational Technology (OT) functions intersect.

As relatively new technologies for enterprise, the document also explains the drivers and benefits of private wireless and neutral host networks for a manufacturing environment. There is a strong demand for automation, real-time decision-making, improved operational efficiency and ensuring robust cellular service across expansive outdoor and indoor facilities. With significant investments in 5G and experience building and operating fault-tolerant networks, service providers like Verizon are expected to have a unique role in helping shape the future of the manufacturing Industry.

Smart, future proof, highly resilient and cost efficient connectivity will empower the manufacturing industry by fostering innovation and enhancing operational efficiency. Additionally, it will ensure employees, visitors, partners and first responders have access to the public cellular network anywhere in the facility. While the initial setup may be challenging to understand, the long-term benefits outweigh the costs, positioning manufacturing for a bright future defined by precision and agility.

Ultimately, by investing in this foundational network architecture, manufacturers can enhance productivity, reduce costs and maintain a competitive edge in an increasingly digital world.

verizon business

The drivers for smarter connectivity

It will likely come as no surprise, but the amount of data created on the factory floor is increasing every year with a recent Deloitte survey[1] estimating manufacturers generate 1,812 petabytes (PB) of data annually. This shop floor data is helping manufacturers not only run their operations more efficiently, but also detect patterns in the data that can be used to address equipment or process problems before they impact production.

With digital automation, factory floors are quickly becoming less isolated data islands as third party vendors and partners need remote access to the factory floor to deliver, manage and maintain their onsite services. Manufacturers, for their part, have been investing in IT infrastructure to provide the coverage and connectivity needed, but new challenges are emerging that are adding increased pressure to find new ways to connect, and connect smarter.

The emergence of artificial intelligence (AI) will require more data sources than ever before, and scaling connectivity of these increasingly varied data sources with wired infrastructure is costly and inflexible. Traditional wireless connectivity such as Wi-Fi has served as a stop-gap solution but brings its own set of operational and scalability challenges, most notably the lack of reliability which can lead to negative operational impacts. There is a need for smarter wireless connectivity that has all the characteristics of a wired connection, and 5G in the form of a private 5G wireless network is the answer.

Manufacturers must adopt a "network optionality" approach, aligning each use case and process requiring connectivity to the most efficient network. This means not over-engineering or under-engineering the solution, but investing in networking that delivers each use case efficiently. For instance, a 5G private wireless and neutral host network can reduce the need for a traditional distributed antenna system (DAS) and two-way radio systems on site, removing two separate systems to install, manage and maintain. With increased efficiency from sharing portions of the Radio Access Network (RAN) between the two solutions, the neutral host network improves in-building public network coverage for traditional voice and data services, while the private wireless network overcomes coverage and reliability challenges of connecting IT/OT devices.

Smarter connectivity in the factory can be achieved and, as this paper will show, a 5G private wireless and neutral host network can be a key enabler. Furthermore, relying on a single source partner such as Verizon for all things wireless (Wi-Fi and cellular) and wired (fiber) can simplify administration and management of connected technology throughout the plant.

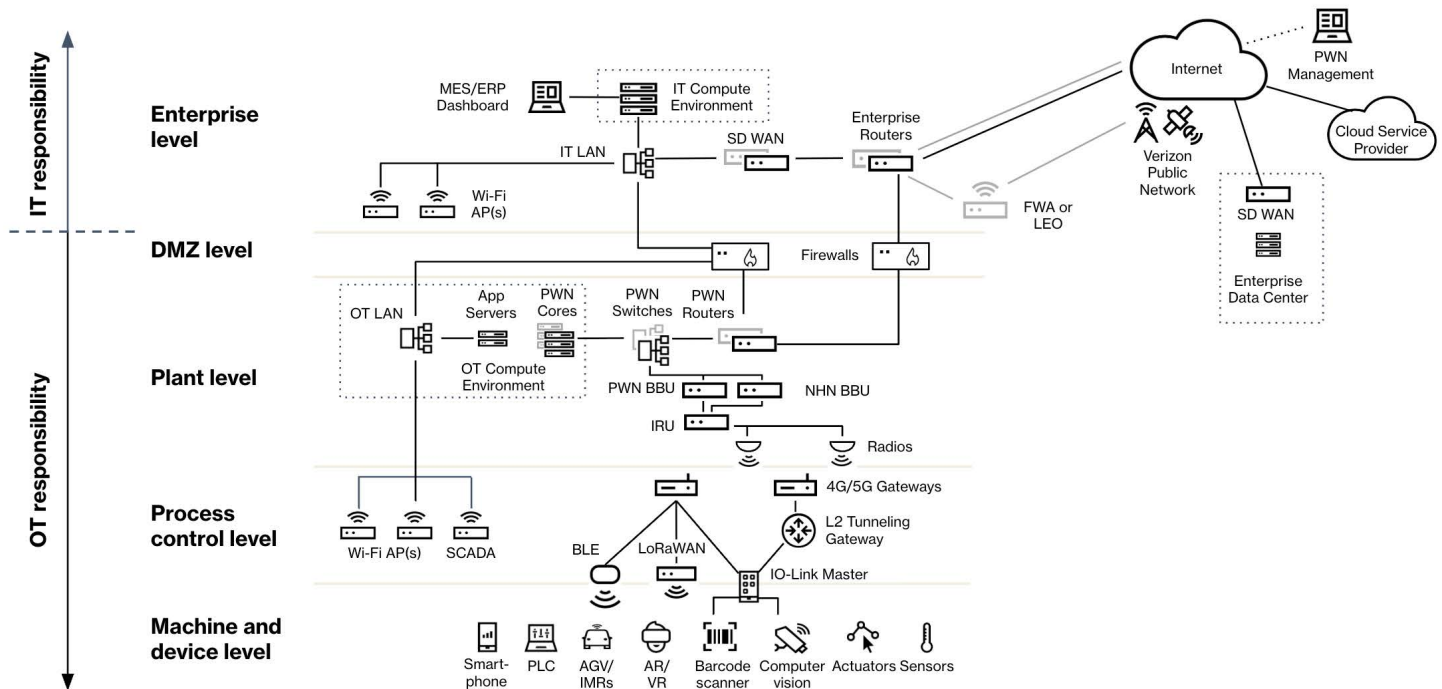# Manufacturing reference architecture

Before we explain the reference architecture, it is important to understand the key components of the private wireless and neutral host networks:

- **Core network:** The control system that manages devices, user authentication and data flow within the network.
- **Radio Access Network (RAN):** The wireless infrastructure (baseband units, indoor radio units, 5G radios) that provides connectivity to devices.
- **Edge computing integration:** Colocates local data processing with wireless connectivity for real-time applications.
- **User Equipment (UE):** Devices like IoT sensors, industrial robots, augmented reality (AR) tools and handheld devices connected to the network.

One of the benefits of the Verizon approach to private wireless and neutral host networks is that a portion of the RAN infrastructure can be shared across the two networks. This approach not only reduces the amount of equipment, power and cabling required, but can help simplify the operations and maintenance of the combined network.

High-level reference architecture

The figure below provides a reference architecture, grounded in the Purdue model and illustrates how the concepts discussed that provide network optionality can be implemented in a manufacturing facility.

The reference architecture was built with three main pillars of thought:

Secure: This is achieved by protecting devices from the Internet as well as segmentation of the wireless OT network and devices from the traditional OT network.

Reliable: Resilient connectivity and hardware provides the basis for high availability.

Cost effective: When possible, infrastructure was used to provide multiple services.

The WAN is provided using dual Internet connections and utilizing SD-WAN to provide advanced WAN features and leveraging a cost effective third link for disaster recovery.

The LAN and Wi-Fi is provided by segmenting out the IT and OT LAN/Wi-Fi but retaining management by a single control plane. This is to simplify management and provide greater correlation of events but still provides the ability to separate out the data flows between the two sides.

Private Wireless connectivity for OT devices provides reliable connectivity to mobile devices such as AGVs and AMRs as well as a lower cost alternative to industrial ethernet. The same wireless infrastructure is also used to provide a Neutral Host Network, providing public cellular connectivity to mobile carriers within the building while remaining completely segmented from the Private Wireless side.

Where necessary to protect infrastructure, security gateways are used to separate key points within the network. The wireless infrastructure, as it requires connectivity out to the Internet, has a security gateway. To separate out the wireless OT infrastructure from the OT LAN, a firewall is also used to provide an additional layer of protection.

Connection to Verizon public network

The primary recommendation for transport is for the site to use two diverse Verizon Internet connections for primary and secondary connectivity. Leveraging SD-WAN, dual Internet access provides a flexible "smart" WAN which is capable of routing around packet loss and latency issues while providing encryption for corporate data. Direct Internet connections also allow for efficient connectivity to the cloud and other Internet based locations including Neutral Host Carriers and Verizon Management systems. PIP (MPLS) is an alternative for those companies that require an additional layer of security and reliability.

As a low cost way to provide third leg connectivity, Fixed Wireless Access (FWA) has become a must have as it provides a separate way to connect a location that is not subject to local civil works and leverages completely separate infrastructure and technology. Where FWA is not available, Low Earth Orbit Satellite (LEO) connectivity can be used to provide the same diversity advantages of FWA.

Segmentation within the reference architecture

Segmenting IT and OT networks within a corporate LAN is crucial for enhancing security and ensuring operational reliability. IT networks typically support business functions like email, file sharing and enterprise applications, often connecting to the Internet and facing external threats.

OT networks, conversely, control and monitor physical processes through industrial control systems (ICS), prioritizing availability and safety, often using specialized protocols and legacy equipment less tolerant of disruption or standard IT security practices. Without segmentation (using techniques like firewalls and VLANs), malware or unauthorized access originating in the IT environment could easily spread to the OT network, potentially causing costly downtime, equipment damage or safety hazards.

This segmentation principle extends to wireless access. Corporate Wi-Fi, primarily serving IT users and devices, must be logically separated from any Wi-Fi networks used for OT purposes, such as connecting sensors or mobile human-machine interfaces (HMIs). Furthermore, private wireless networks can offer a secure and reliable wireless connectivity option, particularly for OT environments. By operating on dedicated infrastructure and leveraging cellular spectrum — either network spectrum designated by regulatory bodies (e.g. CBRS in the U.S.) or Verizon dedicated 5G spectrum — a private wireless network inherently provides strong segmentation from both public networks and the corporate IT LAN/Wi-Fi, minimizing interference and attack vectors for critical OT communications. Implementing robust segmentation across wired, Wi-Fi and private wireless network domains is essential for a resilient and secure modern enterprise.

Despite the need for separation, essential data often needs to flow between these zones, for example, sending production metrics from OT to IT business intelligence systems. Secure intersection without compromising OT security is achieved through strictly controlled conduits, typically a Demilitarized Zone (DMZ). This buffer network sits between IT and OT, regulated by firewalls enforcing granular rules that permit only specific, necessary traffic (defined protocols, ports, source/destination IPs) – usually data flowing from OT to IT as well as to the public cloud.

In addition, technologies like unidirectional gateways can enforce one-way data flow physically. This allows IT to receive necessary operational data without having any direct path back to control or potentially compromise the secure OT environment. Wireless access must mirror this segmentation; corporate IT Wi-Fi remains separate from any OT wireless needs, while private wireless networks offer an inherently segmented, secure wireless overlay, particularly suited for OT's reliability and security demands.

Private Wireless Networks

As manufacturers embrace digitalization, the demand for high-performance, secure and customizable connectivity solutions has never been greater. Private wireless networks—built on cellular technologies such as LTE or 5G—offer the ability to address these needs while providing operational reliability and data sovereignty.

Unlike public networks, private wireless networks provide tailored coverage, capacity and control, making them ideal for modern manufacturing challenges. It uses cellular technology to enable seamless communication between devices, machines and systems within a manufacturing facility.

Why Private Wireless Networks?

A Verizon Private Wireless Network provides minimal interference and consistent performance, which is crucial for time-sensitive manufacturing applications such as robotic coordination and real-time quality control. Data transmitted over a private wireless network remains within the factory's boundaries, reducing the risk of cyber threats and helping the factory in meeting its compliance with stringent industry regulations.

Manufacturers can design private wireless networks to meet their specific needs, such as prioritizing bandwidth for critical operations or expanding coverage in challenging environments like large factory floors. These networks can easily scale to accommodate new devices and use cases as manufacturing facilities grow and evolve.

A Verizon Private Wireless Network provides connectivity for mobile devices with centralized control, real-time insights, analytics and visibility into the entire network through a rich, customer-facing web portal.

Overall this architecture provides seamless integration between operational and enterprise technologies while prioritizing security, reliability and scalability to meet the demands of modern manufacturing environments.

Key characteristics of a private wireless network:

Enhanced security: Supports data privacy as information remains within the facility. Offers better control over access and network policies compared to public networks or Wi-Fi.

Future ready – Long refresh cycle: Future-proof hardware that is expected to support business needs for 10+ years. The longer refresh cycle reduces future investment significantly compared to other IT infrastructure or Wi-Fi. Software updates provide continuous enhancements and any required operational fixes.

High performance: Provides ultra low latency communication and can handle massive device connectivity with high throughput and minimal interference.

Dedicated infrastructure: Owned or leased exclusively by the manufacturing company, operates on licensed or unlicensed spectrum.

Customizable network features: Configurable to meet specific operational and production needs.

Network requirements analysis

Designing and implementing private wireless networks for the manufacturing industry requires careful consideration of various technical, operational and strategic factors to provide reliable performance, scalability and security. The design is fully customized based on the needs of the enterprise:

- **Connectivity needs**: Number and types of devices (e.g., tablets, IoT sensors, robotics, cameras, AR/VR systems). Required bandwidth and throughput per device/application
- **Performance criteria:** Low latency for real-time applications. High availability and reliability for critical operations
- **Coverage area:** Size and layout of the facility (indoor, outdoor, multi-site)
- **Wireless standards:** Choose between LTE, 5G based on performance needs
- **Spectrum:** Licensed, unlicensed or shared spectrum
- **Integration with existing networks:** Ensure seamless interoperability with legacy systems, including Wi-Fi
- **Data protection:** Encryption for data in transit and at rest
- **Access control:** Role-based access, multi-factor authentication (MFA), SIM-based verification and secure device onboarding
- **Network segmentation:** Isolate critical systems (e.g., production line controls) from less sensitive systems

Neutral Host Networks

In today's hyper-connected world, access to public cellular networks in manufacturing facilities is becoming as critical as electricity, running water and air conditioning. These networks not only help connect employees with family and friends, but are essential to vendors, partners and even customers who are visiting the facility – not to mention first responders in the case of an emergency.

A neutral host network allows a manufacturer to cost-effectively extend the network of multiple public mobile network operators into their facility, enabling better coverage and connectivity for all subscribers regardless of carrier. From a user perspective, there is no difference in terms of service whether connected indoors on the neutral host network or outdoors on the public cellular network.

Why Neutral Host Networks?

Unlike previous approaches to improving in-building connectivity (such as DAS or Distributed Antenna Systems), a Verizon Neutral Host Network is a single, shareable wireless infrastructure that uses licensed spectrum and provides a cost-effective platform to support a manufacturer's evolving digital strategy.

Today's factories do not operate in isolation from the rest of the world and there are several good reasons why improved public cellular connectivity inside the factory is increasingly important. Manufacturers rely on an ecosystem of ISVs, OEMs, partners and other third parties that may need public cellular connectivity from the factory floor. Additionally, as some manufacturers adopt BYOD strategies for their employees, ensuring connectivity for multiple mobile operators becomes increasingly important.

A Verizon Neutral Host Network can leverage portions of the same infrastructure used to deliver a Verizon Private Wireless Network, while ensuring separation between private and public cellular traffic. This approach provides manufacturers a more robust communications platform to address a range of business needs.

Key characteristics of a neutral host network:

Scalable in-building connectivity: Offers tailored and scalable connectivity solutions. It's not a one-size-fits-all approach; rather, it caters to the unique requirements of individual locations.

Multi-carrier system: Facilitates seamless connectivity for public subscribers from various mobile carriers to connect to a common radio access network.

Cost-effective alternative: Simplified wireless connectivity management and robust coverage for users, all from a single shared network.

Sustainable solution: Reduced network footprint and energy consumption while meeting high-demand connectivity requirements.

Enterprise integration and management

To enable modern, digital-forward operations, connectivity systems must integrate with OT and IT operational management systems, especially for ticket, change, performance and order management. There are a plethora of vendor and architecture choices in this space. Our approach is to give a variety of integration options to meet specific customer needs: (1) provide a native integration option with an industry leading platform, (2) provide a rich API layer that can integrate to any system. Verizon chose ServiceNow for native integration, but many customers also directly connect to our Digital Enablement Platform via APIs. The benefits to the enterprise include maintaining a single pane of glass for operational teams, reduction of manual work, and speed of change and ticket management.

Moreover, the connectivity layer should provide intelligent insights to Manufacturing Execution Systems (MES) and Enterprise Resource Planning (ERP). This will improve decision making for operational efficiency and life cycle management. Verizon's AI Ops platform and On-Site Network Dashboard (OSND) are examples of innovation in this space. AI Ops provides predictive analytics and anomaly detection. OSND is an industry leading platform that provides performance insights for the private wireless network.

The reference architecture is also applicable to all policy decisions and systems selected by the enterprise for policy management. This encompasses, but is not limited to, the implementation of consistent physical and logical access policies, router and firewall policies, device management, and identity management policies and platforms.

Comparing Private 5G and Wi-Fi

As a major provider of Wi-Fi networks, Verizon continues to see meaningful value with Wi-Fi, especially for carpeted (office) environments in a plant, as well as in its ability to support a wide range of devices that may already be deployed in a factory such as tablets, laptops and certain sensors. In the manufacturing industry, the choice between Wi-Fi and a 5G private network hinges on the specific application requirements, cost considerations and the desired level of performance and security. Enterprises, however, don't have to choose between private 5G and Wi-Fi. The optimal approach often involves strategically combining them to build a wireless network infrastructure that's both flexible and robust, perfectly suited to their unique needs and the applications they support.

While secure, private 5G and Wi-Fi cater to different needs. The simplicity and broad adoption of Wi-Fi make it the go-to wireless solution for general enterprise applications, excelling in typical usage scenarios. However, its performance can be challenged by increasing device density and type, expanded coverage requirements or applications with high bandwidth and low latency demands.

Given the growing diversity of enterprise wireless applications, relying solely on Wi-Fi is becoming inadequate. A balanced approach uses Wi-Fi for basic connectivity and deploys private 5G for more intensive applications. Rather than being separate options, private 5G and Wi-Fi can actually enhance each other. This synergy allows enterprises to build a resilient and versatile wireless infrastructure that meets the demands of various applications and organizational requirements.

Some key differences between the two technologies:

- **Network handoff / mobility:** 5G technology represents a significant leap forward in mobile communication, and enhanced mobility is one of its key promises and advancements over Wi-Fi. Network controlled handoff in cellular ensures no data is lost or interruption is caused during the transition, whereas the client-driven handoffs in Wi-Fi heavily depend on the device to make connectivity decisions. Client driven handoffs can impact performance, reduce throughput and increase latency. Private 5G inherently offers a more robust, seamless and network-controlled handoff mechanism due to its cellular architecture and use of spectrum, making it a better choice for applications requiring truly uninterrupted connectivity and highly predictable performance.

- **Ubiquitous coverage:** Manufacturing facilities often involve heavy machinery, hazardous materials, high-voltage electricity and fast-paced operations. Immediate response is critical. Cellular is better able to reliably propagate signals in areas with physical obstacles. Workers can be assured of having a connection regardless of where they are in the factory (e.g. e-911 access).

- **Deterministic network:** Manufacturers require the predictability and availability for every function and process on the factory floor especially in the core value stream. Private 5G is an engineered solution that provides required QoS. Wi-Fi is a shared network offering best effort connectivity.

- **Exterior spaces:** Cellular technology inherently provides much broader uninterrupted coverage compared to Wi-Fi, which typically has a limited range around an access point. Private 5G networks are designed to blanket large outdoor areas, where deploying extensive Wi-Fi infrastructure would be impractical or costly.

- **Interference Management:** Private 5G leverages sophisticated cellular technologies to combat interference. Private 5G networks employ robust scheduling algorithms that allocate dedicated wireless access to clients for specific periods. This provides devices with the bandwidth and resources they need without contending with others, unlike the "listen before talk" mechanism in Wi-Fi, which can lead to collisions and retransmissions in congested environments.

- **Device security:** SIM authentication, encryption of data and network-originated access control are some of the key factors in the superiority of 5G security as compared to Wi-Fi.

While Wi-Fi remains a crucial technology for localized wireless access, especially indoors, 5G offers significant advantages for providing robust, wide-area, high-capacity and low-latency connectivity in outdoor environments, enabling a new range of mobile and IoT applications.

	Wi-Fi	Private 5G
General office connectivity	√	
Less critical machine monitoring	√	
Handheld / mobile devices	√	√
Guest networks	√	
Mission-critical applications		√
High bandwidth requirements	√	√
Large-scale IoT deployments		√
Harsh industrial environments		√
Enhanced security		√
Seamless mobility		√

While Wi-Fi 7 does have some major enhancements specially on the bandwidth/throughput and latency, it does not fundamentally change the need for more APs in challenging RF environments. The need for higher density of APs (due to shorter range of Wi-Fi) drives the cost up significantly. Higher cost of installation labor, Ethernet cabling, power over Ethernet switches and maintenance makes it a challenging connectivity solution for a manufacturing environment with demanding industrial applications.

In many cases, a hybrid approach might be the most effective solution, using Wi-Fi for less critical applications and office connectivity while deploying a private 5G network for demanding, mission-critical use cases on the factory floor. Ultimately, the decision depends on a thorough assessment of manufacturing needs, the specific applications to be deployed, budget and long-term digital transformation strategy.

Addressing security challenges with Zero Trust

Manufacturing companies often face security risks due to outdated factory floor equipment with long lifespans, sometimes exceeding 20 years. These essential machines may have overlooked security vulnerabilities and weaknesses due to maintenance and patching challenges or their custom-built nature.

We are increasingly seeing manufacturers implement Zero Trust Network Access (ZTNA) platforms. ZTNA overcomes the security limitations of legacy manufacturing systems by supporting all ports, protocols and server-initiated flows. This approach ensures that only authorized users can access these systems, protecting them from potential exploitation even if they lack built-in security features.

With the convergence of IT and OT it is critical to understand the difference between IT and OT ZTNA when considering a Secure Service Edge (SSE) solution.

- **IT is user-centric:** It secures access for users to applications and data. The main goal is to verify a user's identity and device posture before granting least-privilege access, effectively replacing traditional VPNs. Its priority is data confidentiality and integrity.

- **OT is device-centric:** It secures the communication and operation of industrial devices and sensors. The main goal is to protect critical infrastructure and ensure production safety and availability. Its priority is the reliability and safety of industrial processes.

An SSE platform unifies these two approaches by providing a single framework to apply Zero Trust principles across the entire organization. However, it applies different policies and enforcement mechanisms for each domain:

In short, while both use the "never trust, always verify" principle, IT ZTNA asks, "Is this the right user accessing this application?" whereas OT ZTNA asks, "Is this a legitimate device making an authorized command?" An effective SSE solution understands this distinction to provide comprehensive security for both the corporate network and the factory floor.

By adopting these solutions, manufacturers can realize several benefits:

- **Reduce the attack surface:** Limit access to only verified users and resources, thereby minimizing the potential impact of security incidents.

- **Enable digital transformation:** Securely connect diverse systems, applications and users without compromising security or privacy.

- **Enhance compliance:** Meet industry regulations and data protection requirements through detailed access controls and robust security measures.

- **Improve operational efficiency:** Streamline workflows, simplify access management and gain valuable security insights to optimize operations.

ZTNA is a fundamental element of an SSE platform, which encompasses a range of security functionalities beyond access control, such as Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP) and Firewall as a Service (FWaaS). Secure Access Service Edge (SASE) integrates networking and security services, with ZTNA serving as a key component.

In today's evolving manufacturing environment, secure access and data protection are crucial. A robust ZTNA platform, along with the broader implementation of an SSE solution, equips manufacturers with the necessary tools and framework to establish a resilient and adaptable cybersecurity posture.

Private wireless and SSE are distinct but integrable for a comprehensive IT/security strategy. Private wireless enhances foundational security, particularly with SSE. For example, a private 5G network connecting factory devices can leverage SSE for secure cloud data transmission. The choice depends on an organization's specific needs for connectivity, enhanced security, or secure cloud access.

The unique challenge of IoT vulnerability management

The manufacturing segment is inherently reliant on IoT devices for streamlined productivity and countless other benefits. All too often these devices go unchecked for security vulnerabilities or have weak or limited built-in protections to start. A single vulnerable IoT device could offer hackers a virtual open door to the network and everything that's attached to it. Vulnerability management in IoT and OT environments may not be as simple as applying traditional IT security practices due to the unique constraints and critical functions of these devices.

A tailored approach is necessary, focusing on a risk-based methodology, the implementation of strict access controls and the deployment of specialized monitoring tools. While achieving the same level of security as traditional IT systems may not always be feasible, these strategies can significantly reduce risk and contribute to a more resilient security posture.

Effectively managing vulnerabilities in IoT and OT is becoming increasingly crucial. By acknowledging the distinct challenges and implementing targeted solutions, organizations can better protect these vital assets from evolving cyber threats. As the landscape of security continues to change, strategies must adapt accordingly.

Conclusion

The days of limited text based data exchange on a plant floor are ending. Businesses are increasingly demanding real time data to be delivered from the plant floor to other enterprise groups, functions and processes. In addition, the surge of services around AI, video analytics/machine vision, digital twins and numerous other use cases points to the need for a fundamental rethinking of the network services required to support Industry 4.0 and factories of the future.

Verizon Business has the proven expertise and experience to deliver digital transformation combined with the appropriate network strategy. Our experts will work to create an effective network strategy and execute against it to ensure the organization has a solid network foundation to accommodate existing and future needs. This would include the ability to leverage private cellular technologies such as 4G/5G, Edge and Neutral Host Networks to operate more efficiently and innovate more effectively.

Additional resources

Verizon has the ability to enable multiple solutions through our partners as well as the ability for developers to integrate our services into their products through our APIs. The following link details our capabilities, use cases and case studies for manufacturing focused customers:

1. Manufacturing Webpage
2. Private MEC Webpage
3. 5G Edge Developer Portal
4. Private Wireless Networks for Manufacturing Solution Brief
5. Holistic approach towards securing Operational Technologies (OT)
6. Establishing a zero trust model in IoT environments

1. deloitte.com/cn/en/pages/consumer-industrial-products/articles/ai-manufacturing-application-survey.html

verizon business