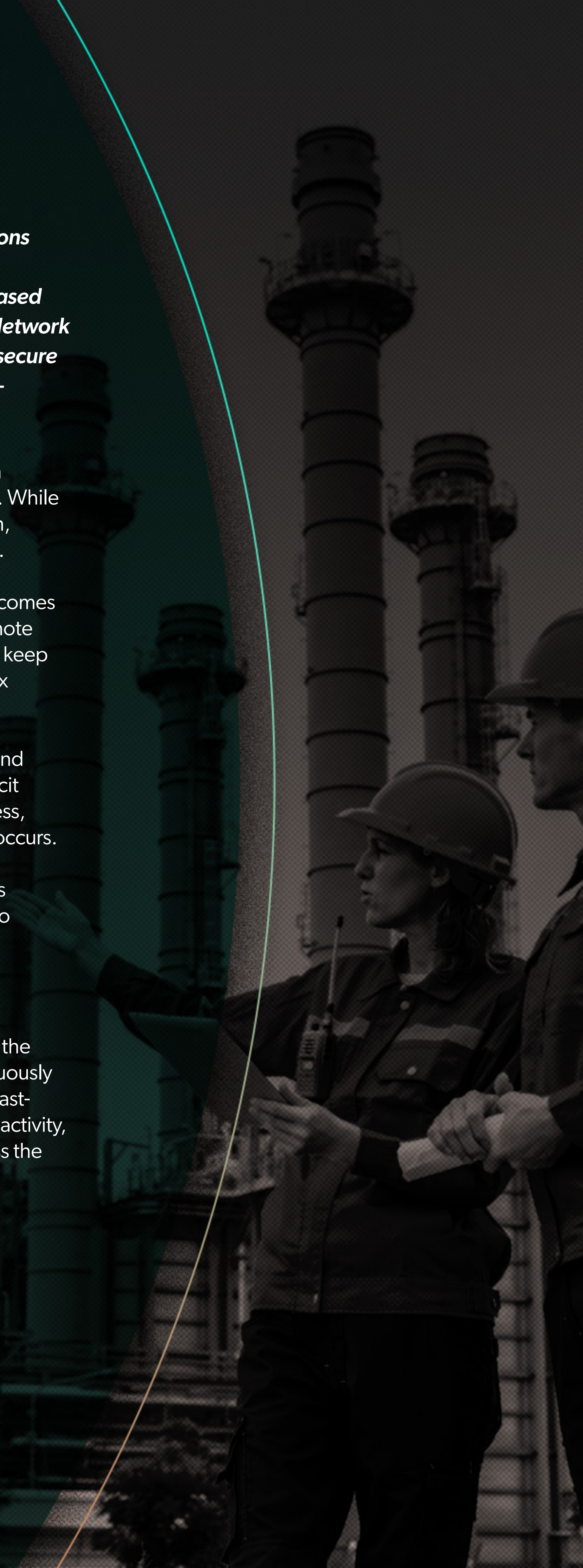
PROVIDING SECURE ACCESS TO MANUFACTURING WITH **ZERO TRUST NETWORK ACCESS (ZTNA)**

appgate



Manufacturing environments require secure access solutions as they navigate evolving cyberthreats and increased connectivity demands. Traditional VPNs and perimeter-based security measures fall short. By implementing Zero Trust Network Access (ZTNA), manufacturing organizations can enable secure and efficient access for all users, devices and workloads—regardless of location.

The manufacturing sector is undergoing a rapid transformation fueled by digital advancements and Industry 4.0 technologies. While this shift unlocks greater efficiency, productivity and innovation, it also exposes manufacturers to new cybersecurity challenges. As manufacturers integrate smart factories, remote work and interconnected devices, securing access to critical systems becomes paramount. Traditionally, manufacturers relied on VPNs for remote access. However, these legacy solutions are now struggling to keep pace with sophisticated cyberthreats and increasingly complex network environments.

VPNs were designed to create secure tunnels between users and networks, but they rely on an outdated security model of implicit trust. Once inside the network, users often gain excessive access, allowing attackers to move laterally across systems if a breach occurs. Furthermore, VPNs are difficult to scale, lack visibility into user activity, and struggle with the performance demands of today's distributed workforce and third-party vendors that are crucial to manufacturing operations.

To protect their valuable assets and data, manufacturers must transition to a more dynamic and secure access model. This is where ZTNA emerges as the ideal solution. ZTNA operates on the fundamental principle of "never trust, always verify." By continuously authenticating and authorizing users and devices, enforcing least-privilege access, and providing granular visibility into network activity, ZTNA ensures that only legitimate users and devices can access the specific resources necessary to perform their tasks.

appgate

SECURE ACCESS CHALLENGES IN MANUFACTURING

In the increasingly digitized manufacturing world, providing secure remote access to critical systems has become a significant challenge. **Employees, contractors, and third-party vendors need access to manufacturing networks from remote locations to maintain operational continuity and maximize efficiency**. However, this expanded connectivity increases exposure to a wider range of cyberthreats.

Antiquated VPNs operate on a perimeter-based security model that assumes implicit trust once a user is authenticated, granting broad access to the entire IT estate. This allows malicious actors to move laterally within the network if initial defenses are compromised. Additionally, VPNs lack the visibility and granular control needed to manage diverse remote users, from full-time employees to third-party contractors and vendors who require specific, limited access.

The challenge extends beyond VPN limitations. The demand for remote access coincides with a dramatic rise in cyberattacks targeting the manufacturing sector. According to IBM's X-Force Threat Intelligence Index 2024, manufacturing has been the most targeted sector for three consecutive years, representing 25.7% of all attacks. This surge is driven by the sector's increasing connectivity and data transparency, which creates more access points and vulnerabilities for attackers to exploit.

Manufacturing has been the most targeted sector for three consecutive years, **representing 25.7% of all attacks.**

In an industry where downtime can be devastating, manufacturers must balance the need for fast, reliable access with robust security against both external and internal threats. This includes managing risks posed by employees accessing systems from unsecured devices or networks, as well as contractors and vendors who require temporary or limited access. With diverse users accessing manufacturing networks remotely, robust security measures that go beyond traditional VPNs are vital to protecting critical operations.

INTRODUCING UNIVERSAL ZTNA:
A MODERN SOLUTION FOR MANUFACTURING

Universal Zero Trust Network Access (ZTNA) replaces the outdated "all-or-nothing" approach of VPNs with dynamic, context-aware access control. This allows manufacturers to securely support remote work, third-party vendors, and contractors while maintaining control over sensitive assets. Universal ZTNA provides a unified approach to secure access for every user—employees and third-party vendors—from any device, in any location.

KEY BENEFITS OF ZTNA IN MANUFACTURING:

Reduced Attack Surface: Unlike traditional VPNs, which rely on exposed open ports vulnerable to cyberattacks, Single Packet Authorization (SPA) technology keeps manufacturing systems and resources invisible until a trusted identity is authenticated. This minimizes the attack surface and hides critical assets like production systems and operational technology from unauthorized users.

Identity-Centric Authentication: VPNs typically rely on IP addresses for access. Modern ZTNA solutions integrate multiple identity sources and contextual data such as time of access, device security posture and location. This ensures that only authorized users—whether employees on the factory floor or third-party contractors—can access sensitive manufacturing systems and networks.

"Segment of One" Access Control: Advanced ZTNA solutions enforce strict least-privilege access, allowing users and machines to interact only with the necessary systems. SPA and "segment of one" capabilities significantly reduce the risk of lateral movement within the manufacturing network.

Seamless Integration with Manufacturing Operations: ZTNA solutions seamlessly integrate with existing manufacturing IT and OT systems through programmable APIs, enhancing network visibility and automation. This flexible, software-defined approach scales effortlessly within dynamic manufacturing environments, enabling factories to adapt as they grow and onboard new third-party vendors or contractors.

By adopting universal ZTNA, manufacturers address the critical need for secure, scalable remote access that traditional VPNs struggle to provide. As organizations embrace remote work and rely on a broader ecosystem of partners and contractors, universal ZTNA empowers IT teams with full control over access. This approach reduces the attack surface and aligns with the operational agility required in today's manufacturing environments. By leveraging ZTNA's context-aware policies, manufacturers can dynamically adapt to evolving security requirements and manage remote access without compromising performance or productivity.

DIRECT-ROUTED ZTNA: OPTIMIZING NETWORK PERFORMANCE FOR MANUFACTURING

Real-time communication and low-latency network access are essential for maintaining efficiency in manufacturing. **Direct-routed ZTNA offers a solution by eliminating the need to route traffic through a cloud broker.** Instead, traffic is routed locally, reducing latency and improving the speed and reliability of remote access for employees and third-party contractors interacting with critical production systems.

Direct-routed ZTNA gives manufacturers greater control over network traffic. By keeping traffic within the local network infrastructure, organizations optimize performance while maintaining stringent security protocols. This is crucial in hybrid environments, where on-premises and cloud-based systems must work together seamlessly without compromising speed or introducing bottlenecks.

Another advantage of direct-routed ZTNA is its easy integration with existing manufacturing systems. Manufacturers can adopt a Zero Trust model without overhauling their network architecture, minimizing disruptions and lowering costs. This approach ensures secure, high-performance access for remote users, enabling manufacturers to maintain productivity while addressing the evolving security challenges of today's connected operations.

DIRECT-ROUTED ZTNA gives manufacturers greater control over network traffic.

APPGATE SDP: UNIVERSAL ZTNA FOR MANUFACTURING

Appgate SDP Universal ZTNA is an advanced alternative to traditional VPNs, aligning with Zero Trust cybersecurity programs tailored for manufacturing. The solution delivers adaptive, identity-based access control, ensuring users access only authorized resources, both remotely and on the local network. With its direct-routed architecture, Appgate SDP eliminates unnecessary traffic rerouting to a vendor-hosted cloud, offering seamless, latency-optimized access to critical systems without compromising security and performance.

Appgate SDP offers numerous advantages for manufacturing environments:

ISOLATED SEGMENT ACCESS CONTROL:

Manufacturing systems, such as factory floor equipment, often require on-site access. Appgate SDP enforces strict policies to ensure users are not only authenticated based on identity and role but are also physically on the network ("on-net") to meet audit and compliance requirements. This limits exposed attack surfaces and enforces the principle of least privilege.

EFFICIENT REMOTE ACCESS:

Appgate SDP provides secure remote access for employees, contractors, and partners without exposing the entire network. This ensures secure and efficient remote connections, reducing reliance on outdated VPN technology.

IMPROVED VISIBILITY AND CONTROL:

Appgate SDP offers comprehensive visibility into network traffic and user activities, allowing security teams to quickly identify and address potential threats. This is crucial for maintaining tight security across complex manufacturing environments.

ENHANCED SECURITY:

By eliminating implicit trust and applying granular, context-aware access controls, Appgate SDP minimizes the attack surface and prevents unauthorized lateral movement. Only verified and authorized users can access critical systems, whether remote or on-net, providing "universal ZTNA."

By adopting Appgate SDP, manufacturers can replace legacy VPN solutions, securing both remote and on-net access while enhancing operational efficiency, all without requiring internet connectivity for critical network segments.

CASE STUDY: LEADING MANUFACTURER Revolutionizes Remote Access with Appgate SDP

Challenge

A global leading equipment manufacturer faced limitations with their legacy VPN solution. Their rapid global expansion and remote workforce demands highlighted bandwidth constraints, security risks, and an inability to provide granular access control. The COVID-19 pandemic further magnified these challenges with the need to onboard thousands remote users quickly. Their VPN couldn't scale to meet the demands of secure, flexible remote access for employees and third-party vendors, nor could it support the seamless integration of new IT systems during mergers and acquisitions (M&A).

Solution

The manufacturer deployed Appgate SDP to address these challenges. By enforcing role-based access controls and leveraging split tunneling to optimize network traffic, Appgate SDP allowed them to enhance security and performance simultaneously. The solution's rapid deployment capability enabled the company to onboard thousands of remote users in just seven days. Furthermore, Appgate SDP provided a scalable platform that easily integrated new users and systems during M&A activities.

Results

With ZTNA, the manufacturer achieved:

Rapid user onboarding: Thousands of remote users were onboarded within seven days during the pandemic.

Enhanced security: Granular access controls ensured that users could only access necessary systems and applications, reducing the risk of exposure.

Seamless M&A integration: The flexible architecture streamlined the onboarding of users from acquired companies, ensuring uninterrupted operations.

Improved vendor management: Targeted access controls enabled secure, limited access for vendors and partners.

By replacing their VPN with Appgate SDP, the manufacturer enhanced its security posture, improved operational flexibility, and established a secure foundation for future growth and global expansion.

EMBRACING ZTNA FOR A SECURE MANUFACTURING FUTURE

As the manufacturing sector navigates the digital transformation of Industry 4.0, adopting advanced security solutions is crucial for operational resilience and safeguarding sensitive systems. Replacing legacy VPNs with universal ZTNA provides a modern, scalable approach to secure remote access for employees, third-party vendors, and contractors. With ZTNA, manufacturers enforce strict access controls, ensuring that only verified users can access specific resources, significantly reducing the risk of unauthorized access.

ZTNA is more than just a VPN replacement; it's a strategic security evolution designed to meet the increasingly complex needs of manufacturing networks. Traditional VPNs grant excessive access, creating vulnerabilities that leave organizations exposed to threats. This is compounded by the continuous discovery of Common Vulnerabilities and Exposures (CVEs) in VPN technologies, highlighting critical security flaws that attackers can exploit. These risks increase the likelihood of unauthorized access and make securing the network more challenging. By adopting Zero Trust principles, manufacturers can better defend against cyberthreats and prevent operational disruptions.

Successfully adopting ZTNA requires careful planning and an understanding of its integration into the existing manufacturing ecosystem. By leveraging a ZTNA solution that seamlessly integrates with current infrastructure and allows for flexible deployment across hybrid environments, manufacturers can secure their industrial networks without overhauling legacy systems. ZTNA is not a temporary fix, but a necessary evolution in cybersecurity. By embracing ZTNA and the Zero Trust model, manufacturers can confidently secure their operations, protect valuable assets,

Appgate secures and protects an organization's most valuable assets and applications. Appgate is the market leader in Zero Trust Network Access (ZTNA) and online fraud protection. Appgate products include Appgate SDP for Universal ZTNA and 360 Fraud Protection. Appgate services include threat advisory analysis and ZTNA implementation. Appgate safeguards enterprises and government agencies worldwide. Learn more at appgate.com.

appgate