SECURING OPERATIONAL TECHNOLOGY NETWORKS IN MANUFACTURING WITH **DIRECT-ROUTED UNIVERSAL ZTNA**

appgate

The manufacturing sector is undergoing a significant transformation, driven by the integration of smart factories and Industry 4.0 technologies. While this technological leap promises unprecedented gains in efficiency, productivity, and uptime, it also exposes factories to a darker side of the digital age—an ever-growing and increasingly sophisticated wave of cyberthreats and other operational security risks.

Within the web of interconnected systems that power modern manufacturing, legacy operational technology (OT) and industrial control systems (ICS) remain particularly vulnerable to security failures. This vulnerability is further compounded by the rise of remote work and the diverse array of personal devices (BYOD) accessing critical systems. These systems—many of which were designed in an era with less emphasis on security—become prime targets for malicious actors. Industrial switches, cellular gateways and other OT devices, once considered the backbone of production, now represent potential entry points for cyberattacks. Ensuring the security of these devices, particularly in remote and BYOD scenarios is paramount to safeguarding the integrity of industrial operations.

The convergence of information technology (IT) and OT networks further amplifies this risk. What was once a clear demarcation between the digital realm of data and the physical world of production has blurred, creating new avenues for cyberthreats to infiltrate and disrupt operations.

In this new landscape, the traditional fortress-and-moat approach to cybersecurity—building a strong perimeter in the hopes of keeping threats out—is no longer sufficient. Instead, a paradigm shift is required, and the Zero Trust model, a security framework that operates on the principle of "never trust, always verify," emerges as a beacon of hope. Zero Trust Network Access (ZTNA), a core component of this model, secures vulnerable access points and hardens network perimeters. By continuously verifying and authenticating every user and device, enforcing least-privilege access, and providing granular visibility into network activity, ZTNA acts as a digital guardian, fortifying industrial systems against the rising tide of cyberthreats.

UNDERSTANDING THE CHALLENGES OF OT SECURITY IN MANUFACTURING

The manufacturing sector, historically a lucrative target for cybercriminals due to its low tolerance for downtime, faces a perfect storm of security challenges. According to Cybersecurity Ventures, **the global cost of cybercrime is expected to grow by 15 percent per year over the next five years**, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.

This alarming trend underscores the urgent need to address the unique security vulnerabilities plaguing the manufacturing industry, including:

LEGACY SYSTEMS AND PROTOCOLS

Many factories still rely on legacy equipment and protocols that were not designed with remote access or modern cybersecurity threats in mind. These outdated systems often lack robust security features, leaving them susceptible to exploitation by malicious actors.

LIMITED VISIBILITY AND CONTROL

The complex and interconnected nature of industrial environments often results in limited visibility and control over OT systems. This lack of insight makes it difficult to detect and respond to threats promptly, increasing the potential for damage. Real-time operational requirements further complicate matters, as security measures must not impede critical processes.

AIR-GAPPED NETWORK LIMITATIONS

The traditional belief that air-gapped networks offer sufficient protection for critical infrastructure and OT environments is no longer valid. The need to connect OT and IT networks for data analysis and remote management has introduced new pathways for threat actors to infiltrate industrial systems.

THIRD-PARTY ACCESS

Remote contractors and third-party vendors often require access to OT networks for maintenance, updates, or support. These external identities can have less secure devices, have weaker security controls, or lack awareness of internal security policies, making them prime targets for cyberattacks that could infiltrate the OT environment.

INSIDER THREATS AND HUMAN ERROR

While external threats remain a significant concern, insider threats and human error also pose substantial risks. Unintentional misconfigurations, accidental data exposure, and even malicious actions by disgruntled employees can have devastating consequences.

These challenges, combined with the ever-evolving threat landscape and the increasing financial incentives for cybercriminals, underscore the criticality of robust security measures tailored to the unique needs of the manufacturing sector.

> Outdated systems often lack robust security features, leaving them susceptible to exploitation by malicious actors.

HOW UNIVERSAL ZTNA TRANSFORMS OT SECURITY IN MANUFACTURING

ZTNA shifts the manufacturing industry's cybersecurity approach from reactive to proactive, **enabling organizations to anticipate and thwart threats before they cause harm.** ZTNA fortifies OT in manufacturing environments with a proactive defense strategy that encompasses these core principles:

CONTINUOUS AUTHENTICATION AND AUTHORIZATION

ZTNA solutions, like Appgate SDP, continuously verify the identity and security posture of users and devices before granting access to resources. This ensures that only authorized individuals (both internal employees and third-party users) and devices can access core systems, even if they are within the network perimeter.

LEAST PRIVILEGE ACCESS

By adhering to the principle of least privilege, ZTNA solutions only grant users the minimum level of access necessary to perform their specific tasks. This significantly reduces the attack surface and limits the potential damage that can be caused by compromised credentials or devices.

REAL-TIME THREAT DETECTION AND RESPONSE

ZTNA solutions provide comprehensive visibility into user and device activity, enabling security teams to detect and respond to threats in real-time. This enhanced visibility allows for swift isolation of compromised devices or users, minimizing the impact of a security incident.

In essence, **ZTNA transforms OT security in manufacturing by eliminating implicit trust**, enforcing granular access controls, implementing stringent device posture checks and providing real-time visibility into network activity. This comprehensive approach significantly strengthens the security posture of manufacturing environments, protecting critical infrastructure and sensitive data from the ever-evolving threat landscape.

DIRECT-ROUTED ZTNA: A TAILORED NETWORK SECURITY SOLUTION

Unlike most ZTNA solutions that route traffic through a cloud broker, direct-routed ZTNA, such as Appgate SDP, offers distinct advantages for OT in manufacturing environments.

Direct-routed ZTNA avoids the limitations of cloud-routed solutions when dealing with complex network architectures, including the intricate topologies and hybrid infrastructures common in manufacturing. It allows for full control over data movement across the network, accommodating the complex connections and legacy systems often found in OT environments.

By eliminating the need to route traffic through a cloud broker, direct-routed ZTNA also significantly reduces latency and performance impact, improving overall performance. This is crucial in OT environments where real-time responsiveness and high throughput are essential for vital processes.

Direct-routed ZTNA can seamlessly integrate with existing security tools and infrastructure, allowing organizations to leverage their current investments while enhancing security with Zero Trust principles. This flexibility, including integrating with existing security tools, is vital in OT environments where replacing legacy systems can be costly and disruptive.

DIRECT-ROUTED ZTNA offers simplified deployment and management options, reducing administrative overhead and complexity.

Compared to cloud-routed solutions, direct-routed ZTNA offers simplified deployment and management options, reducing administrative overhead and complexity. It allows for flexible deployment across the hybrid infrastructure, including on-premises, cloud and edge environments. This ease of deployment and management is particularly beneficial in OT environments where resources may be constrained.

APPGATE SDP: PROTECTING INDUSTRIAL SYSTEMS WITH ZTNA

Appgate SDP, a universal ZTNA solution, is well-suited to address the manufacturing industry's unique challenges, offering several features that make it a valuable asset in securing OT environments.

Appgate offers a range of benefits for OT environments, including:

ENHANCED SECURITY

By eliminating implicit trust and enforcing granular, context-aware, least privilege access controls, Appgate SDP significantly reduces the attack surface, making it harder for threat actors to move laterally within the network.

IMPROVED VISIBILITY AND CONTROL

Appgate SDP provides deep visibility into all network traffic and user activity, enabling security teams to quickly detect and respond to potential threats.

REGULATORY COMPLIANCE

Many OT systems are subject to strict regulatory requirements. Universal ZTNA helps manufacturers meet these compliance mandates by providing robust access controls and audit trails.

SECURE REMOTE ACCESS

Appgate SDP facilitates secure remote access for employees, contractors, and partners without exposing the entire network, which is especially important in today's hybrid work environment.

SECURITY FOR AIR-GAPPED AND CONVERGED NETWORKS

Appgate SDP delivers effective security for these converged environments with its Zero Trust model, granular access controls, and Single Packet Authorization. This ensures only authorized users and devices can access specific resources, minimizing the attack surface and mitigating internal and external threats.

By adopting Appgate SDP and embracing the Zero Trust security model, manufacturers can better protect their infrastructure, mitigate the risk of cyberattacks and ensure the continued operation of their production processes.

CASE STUDY: GLOBAL MANUFACTURING COMPANY GOES CLOUD-FIRST WITH ZERO TRUST

Challenge

After spinning off from a larger manufacturing conglomerate, this 2,000-person company initiated a cloud-first strategy to modernize its operations and strengthen security with Zero Trust. The need for secure, scalable access became even more critical when a 300% increase in remote workers highlighted the limitations of their legacy VPN.

Solution

The company chose Appgate SDP, a Zero Trust Network Access (ZTNA) solution, to secure its infrastructure and support its global, cloud-first ambitions. Appgate SDP's identity-centric approach enabled the company to control access across borders, securely connect remote and third-party users, and reduce the complexities of their multi-national IT environment.

Results

By implementing ZTNA, the company achieved:

Enhanced Security and Accessibility: Enabled secure remote work for 80% of employees, up from 12.5%, with expectations that half of the workforce will continue remotely.

Accelerated Provisioningt: Reduced provisioning time by 87.5%, from days to mere hours.

Improved Cloud Transformation: Strengthened digital transformation initiatives by 60%, supporting secure, global operations and simplified connectivity.

Through Appgate SDP, the company successfully enabled a secure, cloud-first model, equipping it to innovate and scale confidently in a complex, global environment.

EMBRACING ZERO TRUST AS A PROACTIVE SECURITY STRATEGY

The manufacturing industry faces a relentless wave of cyberattacks, making robust security controls an absolute necessity for both protecting critical industrial systems and ensuring business continuity. Universal ZTNA offers the most compelling solution, safeguarding systems and sensitive data by abolishing implicit trust and enforcing least privilege access. This strategic approach substantially reduces the risk of cyberattacks, empowering factories to confidently pursue digital transformation objectives in a secure environment.

Successful ZTNA implementation in a factory environment requires meticulous planning and thoughtful consideration. Organizations must identify their most indispensable assets and data to design a ZTNA architecture that provides appropriate protection. Selecting a ZTNA solution that seamlessly integrates with existing infrastructure and workflows is imperative for a successful transition. By embracing advanced security controls like multi-factor authentication (MFA), identity provider (IDP) integrations, and continuous authentication, manufacturers can further strengthen their security posture and ensure operational agility.

In the face of evolving threats, Zero Trust is not merely a trend but a fundamental shift in how we approach cybersecurity in the manufacturing sector. By embracing Zero Trust and leveraging robust ZTNA solutions, manufacturers can navigate the complexities of the digital age, fortify their operations against cyber risks, and unlock the full potential of Industry 4.0.

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