# SECURING MANUFACTURING OPERATIONS WITH AIR-GAPPED **ZERO TRUST NETWORK ACCESS (ZTNA)**

appgate

Manufacturing businesses face increasingly complex cybersecurity challenges as they strive for operational efficiency. The rise of connected devices and automation technologies expands the attack surface, leaving critical systems vulnerable. Cybercriminals target these networks to disrupt production, steal intellectual property, and cause costly downtime. Traditional security measures like network segmentation and firewalls often prove insufficient against sophisticated cyberattacks. Without proper precautions, manufacturers risk jeopardizing operational continuity and safety by leaving vital systems exposed.

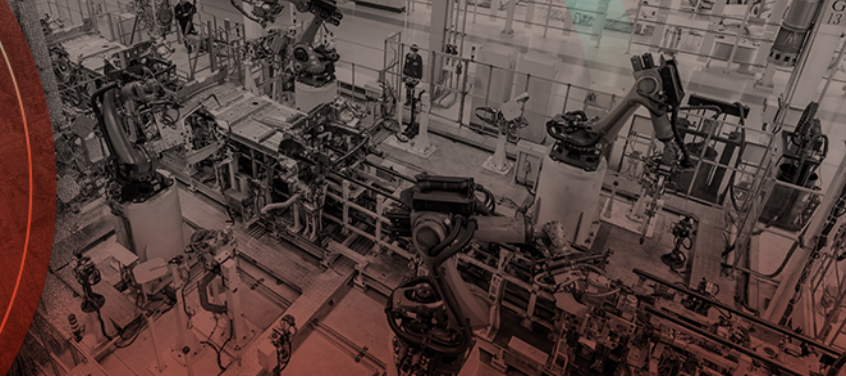
Air-gapping physically isolates critical systems from potentially untrusted networks, including the public internet and even corporate networks. This "air gap" significantly reduces the attack surface and mitigates the risk of network-borne cyberattacks. This approach is gaining traction among manufacturers seeking to eliminate vulnerabilities in their factory-floor IT and operational technology (OT) systems.

Air-gapped networks are a critical topic for manufacturing professionals. These isolated systems offer powerful protection for critical infrastructure in a constantly evolving threat landscape. By understanding the benefits, challenges, and best practices of air-gapping, manufacturers can make informed decisions about implementation. This includes identifying scenarios where air-gapping is most effective, weighing security trade-offs against operational flexibility, and exploring strategies to maintain core security benefits while addressing the limitations of isolation.

The increasing frequency and sophistication of cyberattacks in manufacturing underscores the importance of robust cybersecurity. Air-gapped networks represent a critical shift toward ensuring the integrity, confidentiality, and availability of critical systems. By implementing network separation, IT and Security teams can significantly enhance protections for sensitive operations, enabling digital transformation while preserving system integrity.

appgate

# NETWORK CHALLENGES IN MANUFACTURING



Digital transformation and advanced technologies increase the complexity of securing critical manufacturing systems. The industry's unique challenges and risks demand robust security measures. A pressing concern is the potential for catastrophic downtime. In 2024, the Global 2000 will lose a total of **$400 billion annually due to downtime, with an average of $200 million lost per company,** due to unexpected failures in digital environments. This highlights the critical need for effective security solutions that eliminate the risk of network-borne cyberattacks.

However, securing manufacturing networks is challenging. Without proper network isolation, centralized IT staff struggle to safely deploy software patches, firmware updates, or system upgrades, leading to time-consuming and error-prone manual processes. Additionally, managing the collection and analysis of production data from OT and industrial control systems (ICS) becomes crucial for reporting, diagnostics, and decision-making.

Even seemingly secure networks remain vulnerable. Imagine a scenario where an employee unknowingly uses an infected USB drive to transfer data within a manufacturing facility. This seemingly harmless action could introduce malware that spreads rapidly across internal systems, disrupting production lines, stealing sensitive intellectual property, or even causing physical damage to equipment. This highlights the importance of both secure data transfer protocols and proper network segmentation to limit the impact of such breaches. A lack of proper network segmentation hinders centralized IT staff from implementing automated monitoring, alerts, and remote diagnostics, potentially increasing downtime.

The Global 2000 will lose a total of **$400 billion annually due to downtime, with an average of $200 million lost per company** due to unexpected failures in digital environments

Manual data collection for auditing and regulatory compliance becomes necessary without proper network controls, increasing the potential for errors and inefficiencies. Inadequate network architecture can hinder the integration of modern IoT devices and cloud-based services, limiting Industry 4.0 initiatives. Additionally, backup and disaster recovery become more cumbersome in poorly designed networks, potentially prolonging recovery times.

Balancing innovation with security requires manufacturers to carefully consider trade-offs between robust protection and operational flexibility. The key is developing comprehensive strategies that leverage internal resources and external expertise to create resilient, secure, and efficient operations in an interconnected world. Advanced network isolation techniques allow manufacturers to mitigate risks while maintaining agility.

# HOW AIR-GAPPING TRANSFORMS NETWORKING SECURITY FOR MANUFACTURING

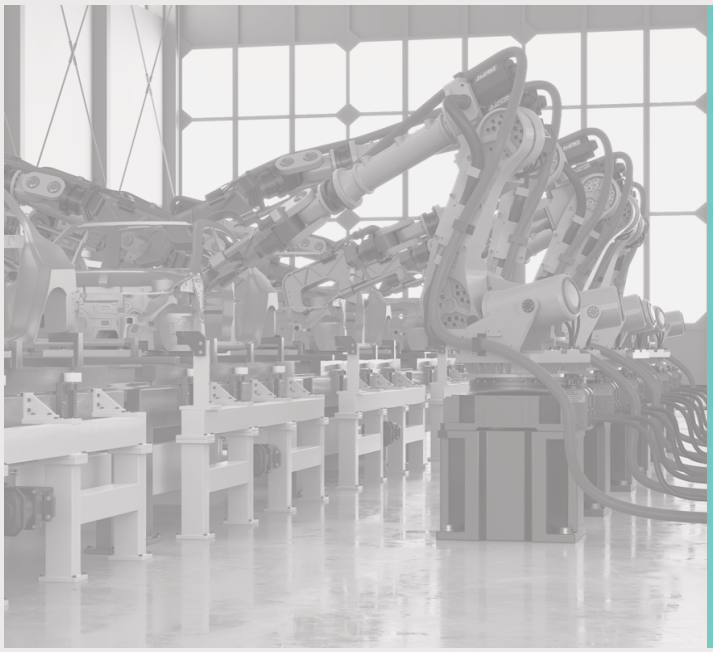
Air-gapped networks represent a paradigm shift in network security, providing physical isolation that eliminates the risk of network-borne cyberattacks. This is crucial for manufacturers protecting sensitive assets like OT and ICS. Air-gapped networks create a secure environment completely disconnected from untrusted networks.

## KEY BENEFITS OF AIR-GAPPED NETWORKS IN MANUFACTURING:

**Complete Isolation:** Air-gapped networks provide absolute separation from external networks, unlike traditional segmentation. This physical disconnect ensures critical systems remain inaccessible to unauthorized users and cyberthreats, significantly reducing the attack surface.

**Enhanced Data Protection:** Air-gapping offers unparalleled protection for sensitive manufacturing data. By physically isolating critical systems, manufacturers prevent unauthorized data exfiltration and protect proprietary information, trade secrets and intellectual property.

**Resilience Against Advanced Threats:** Air-gapped networks are inherently resistant to sophisticated cyberthreats that exploit network vulnerabilities or rely on internet connectivity. This resilience is invaluable in manufacturing, where system integrity is paramount.



Air-gapped networks address the critical need for stronger security in the face of increasingly sophisticated cyberthreats and stricter regulatory requirements. They empower IT teams to maintain complete control over critical systems and data, minimizing cyberattack risks while aligning with the stringent security demands of modern manufacturing.

# **UNIVERSAL ZTNA:** BRIDGING SECURITY FOR AIR-GAPPED AND CONNECTED NETWORKS

Universal ZTNA complements and enhances the security of air-gapped networks. It provides a unified framework for secure access across both isolated and connected systems, addressing the complex needs of modern manufacturing.

Universal ZTNA offers a consistent security model applicable to air-gapped, partially air-gapped and connected networks. This unified approach ensures consistent enforcement of access controls, authentication mechanisms, and security policies, regardless of user location or system access.

**UNIVERSAL ZTNA COMPLEMENTS** AND ENHANCES THE SECURITY OF AIR-GAPPED NETWORKS.

### Secure Access for All Users

A key advantage of universal ZTNA is its ability to provide secure access for all users, whether on-premises or remote, using any device, from any location. This flexibility is crucial in manufacturing, where employees, contractors and vendors require varying levels of access.

ON-PREMISES ACCESS:
For users within the manufacturing facility, universal ZTNA enforces strict access controls to air-gapped systems. This may include requiring users to be on a specific network segment, using a particular device, or passing additional authentication checks.

REMOTE ACCESS:
While true air-gapped systems remain physically isolated, universal ZTNA can provide secure remote access to adjacent systems or data repositories that interface with air-gapped networks. This allows for remote monitoring, reporting, or management functions without compromising the air-gapped environment.

Universal ZTNA enables manufacturers to create a comprehensive security framework that respects air gaps while providing secure, controlled access to critical systems. This enhances protection while improving operational efficiency by enabling secure access for authorized users across various scenarios.

# **APPGATE SDP:** SECURE AIR-GAPPED NETWORKS FOR MANUFACTURING

Appgate SDP, a universal ZTNA solution, is well-suited for implementing and managing air-gapped networks in manufacturing. It provides robust security for critical systems and data, enabling the creation and maintenance of physically isolated network segments to ensure sensitive OT and ICS remain disconnected from vulnerable networks. Appgate SDP's direct-routed architecture supports air-gapped environments, delivering the security of physical isolation with the performance and control of local network connections.

**Appgate SDP benefits for air-gapped networks in manufacturing include:**

### PHYSICAL ISOLATION ENFORCEMENT:

Appgate SDP enables true air-gapped environments for critical systems, ensuring secure, on-premises connectivity for factory floor equipment and sensitive production systems isolated from external networks, significantly reducing the risk of cyber intrusions and unauthorized access.

### SECURE DATA TRANSFER PROTOCOLS

Appgate SDP supports secure, one-way data transfer mechanisms when necessary, allowing for critical production data extraction or system updates without compromising the air-gapped environment.

### GRANULAR ACCESS CONTROL:

Appgate SDP enables fine-grained access controls within air-gapped environments, ensuring only authorized personnel can interact with specific systems or data, further enhancing security and reducing insider threats.

### COMPREHENSIVE AUDIT AND COMPLIANCE SUPPORT:

Appgate SDP provides detailed logging and reporting capabilities, simplifying compliance with industry regulations and internal security policies. This is crucial for demonstrating the effectiveness of air-gapped security measures during audits.

Appgate SDP enables manufacturers to create and manage air-gapped networks, protecting critical assets from cyberthreats while maintaining operational flexibility. This approach provides a solid foundation for securing sensitive systems and data, ensuring business continuity, and avoiding costly downtime.

CASE STUDY:

## Innovative Manufacturing Company Embraces Zero Trust with Appgate SDP

### Challenge

An ISO 9001:2008 certified contract manufacturing company faced limitations with their existing VPN solution. They needed to provide secure access to remote users, prevent unauthorized access, and implement dynamic access policies based on user and device context. Additional requirements included secure access to remote endpoints, step-up MFA for software patches, and management of security for Integrated Lights-Out (iLO) devices and network appliances. The company also sought to future-proof their security framework.

### Solution

The company deployed Appgate SDP to address these challenges. By implementing a Zero Trust architecture with direct routed access, the solution provided granular access controls and dynamic authentication mechanisms. Appgate SDP's open APIs facilitated seamless integration across business, IT, and security solutions, enhancing network visibility and automation capabilities. The software-defined nature of the solution ensured effortless scaling with dynamic infrastructure.

### Results

With Appgate SDP, the manufacturing company achieved:

**Zero Trust transformation**: Successful transition from legacy VPN to a Zero Trust architecture

**Least privilege access:** Improved network security with dynamic, least-privileged access policies

**Enhanced performance:** Faster, more reliable access with low-latency, high-throughput network performance

**Flexibility and scalability:** Increased scalability and adaptability across business, IT, and security systems

With Appgate SDP, the innovative manufacturing company strengthened its security posture, improved operational flexibility, and established a secure foundation for future growth and expansion.

## EMBRACING AIR-GAPPED NETWORKS FOR A SECURE MANUFACTURING FUTURE

As the manufacturing sector navigates the digital transformation of Industry 4.0, robust security solutions are essential for operational resilience and safeguarding sensitive systems. Air-gapped networks provide a comprehensive approach to isolating critical OT and ICS from cyberthreats. This absolute isolation ensures sensitive systems remain completely disconnected from external networks, significantly reducing the risk of unauthorized access and cyberattacks.

Air-gapped networks are more than just network segmentation; they represent a fundamental security breakthrough for the increasingly complex needs of manufacturing. Traditional network architectures, even with firewalls and VPNs, can still be vulnerable. This is particularly concerning given the rise in sophisticated cyberattacks targeting the manufacturing sector. Air-gapped principles enable manufacturers to better defend against these threats and prevent operational disruptions.

Successfully implementing air-gapped networks requires careful planning and integration into the existing manufacturing ecosystem. Air-gapped solutions allow manufacturers to isolate their most sensitive industrial networks without completely sacrificing operational efficiency. Air-gapped networks are not a temporary fix, but rather a necessary evolution in cybersecurity for high-risk environments. By embracing air-gapped networks and physical isolation, manufacturers can confidently secure critical operations, protect valuable assets and intellectual property, and ensure long-term business continuity in the face of growing cyber risks.

---

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