paloalto NETWORKS

Best practices to protect OT assets, networks and remote operations

Zero Trust Security to Protect All OT Environments

Digital transformation and connectivity in OT environments brings great promise.

Digital transformation is changing the face of industrial operations, presenting tremendous opportunities for organizations to revolutionize their businesses. Adoption of OT assets, 5G technology, and migration to the cloud are parts of the digital transformation many industrial organizations are pursuing to improve operational efficiency, reduce cost, and enhance worker safety.

This increased digitization means connectivity of machine to machine (M2M), machine to humans, and machine to outside the OT networks. This creates a connected ecosystem of cyber-physical systems (CPS). This trend is fueled by the following:

Smart Manufacturing

OT environments are going through Industry 4.0 initiatives fueled by digital technologies that connect employees, partners, suppliers, and machines. This integrated CPS ecosystem improves operational efficiencies, agility, and customer experience.

Old systems connecting to IT

Many existing OT systems developed without a focus on security are now connected to the IT network and the internet leading to security gaps. In addition, the growing complexity of OT systems and the patchwork of siloed security technologies have resulted in elaborate specialized network infrastructures that expand attack surfaces.

Accelerated remote connections due to the pandemic

The pandemic has accelerated connectivity as it required opening remote access to OT infrastructure via the internet for maintenance and operational purposes. It also forced some air-gapped OT environments to be opened to the cloud for remote analytics and asset maintenance.

OT Security Delivers Significant Benefits

- **Improve operational efficiency**
  Maximize operational uptime by reducing security breaches and automating processes.
- **Reduce costs**
  Minimize the costs associated with safety incidents, and maintenance through remote monitoring and asset management.
- **Enhance worker safety**
  Reduce the risk of equipment failures and accidents.

OT environment vulnerability and exposure to threats are at an all-time high and will continue to accelerate. CXOs face a precarious balancing act of maintaining availability, uptime, and safety while deploying and maintaining world-class security.

Despite OT benefits, the increased connectivity brings great risk to operations.

Organizations worldwide face an incredible challenge—security breaches that could stop operations. A breach negatively impacts revenue, brand, supply chain SLAs, and worker safety. Four trends are driving the increased risk of a security breach.

1. **Threat surface expansion**
   The threat surface is rising considerably as digital transformation initiatives lead to vulnerable legacy and new OT assets. These systems connect to the IT network (IT/OT convergence), 5G, cloud, and internet, as well as increased direct-to-app access for remote OT asset maintenance.

2. **Vulnerable targets for ransomware and IP theft**
   Ransomware and other cyber-attacks have escalated as the attackers target vulnerable OT assets.

3. **Increasing compliance pressure**
   Industry and regulatory compliance requirements continue to evolve to protect OT environments to address concerns about the potential impact of a security breach on operations, worker safety, revenue, and brand.

4. **Outdated and siloed security technologies**
   Current IT and OT security technologies are fragmented, piecemeal technologies that do not provide adequate protection and require specialized training, skills, and maintenance.

It is a perfect storm of digitization, threats, regulations, and outdated security. Unfortunately, a lack of modern-day comprehensive security for OT environments leaves them highly vulnerable to cyber-attacks.

CXOs are aware and concerned, but struggle to protect their OT environments.

Lacking a holistic solution to protect OT environments, CXOs are forced to choose among three less-than-ideal options.

1. **Address the challenges with too many, too few, or no security solutions**
   Some CXOs deploy multiple siloed security products in an effort to cover as many risks as possible, but face operational complexity, potential misconfigurations, and high total cost of ownership. Other CXOs are concerned that adding security technologies to their environment might impact operations, which has led to minimal security adoption. The third group of CXOs continues the physical separation between OT and the rest of the world, delaying digital transformation for as long as possible.

2. **Tolerate assumed security risk inside the OT network**
   Some CXOs choose to implement zero or very basic segmentation of the OT network. This allows lateral movement that can give an adversary complete access to the OT environment if the perimeter is breached.

3. **Allow remote access without consistent security inspection and control**
   Other CXOs allow remote access availability without appropriate security policies, inspections, and controls.

Gartner predicts that by 2025, 30% of critical infrastructure organizations will experience a security breach that will halt operations or mission-critical cyber-physical systems.[1]

According to the 2021 FBI Internet Crime Report, the US manufacturing sector saw 60+ attacks in 2021 since the Colonial pipeline hack in May 2021. That is about ten successful ransomware attacks every month.

Opportunities for attack in OT environments

LEGACY AND NEW OT ASSETS ARE CONNECTING TO IT AND CLOUD
400% expected increase in manufacturing OT assets.[2]

5G CONNECTS NEW TYPES OF ASSETS
15B 5G-connected industrial assets by 2026.[3]

REMOTE CONNECTIVITY IS ON THE RISE
70% of the ICS/SCADA assets have external connections.[4]

MANY OT ASSETS ARE VULNERABLE AND HARD TO PATCH
1K+ CVEs in industrial control systems, 80+ vulnerabilities in top 4 OT vendors.[5]

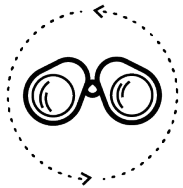
SaaS APPS ARE ANOTHER ATTACK VECTOR
33% of the ICS attacks used public-facing applications in 2021.[6]

REMOTE CONNECTIVITY IS A NEW ATTACK VECTOR
37% of the ICS attacks used external remote services in 2021.[7]

Zero Trust security approach needed to protect OT networks

Zero Trust is a cybersecurity strategy that eliminates implicit trust by continuously validating security posture. Rooted in the principle of “never trust, always verify,” Zero Trust protects OT environments in several ways. Taking a Zero Trust approach to OT security provides the most effective defense against cyber-attacks across OT assets and networks, remote operations, and 5G networks...

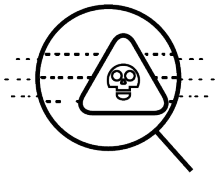
Complete Visibility



Least-privilege Access Control

Continuous Trust Verification

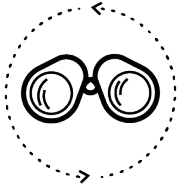
Continuous Security Inspection



*Expected number of devices in 2030 and % increase from 2020 to 2030.

Comprehensive visibility of OT assets, apps, and users across OT networks, remote operations, and 5G networks

Complete Visibility



Zero Trust is founded on accurate visibility of assets, apps, and users. To effectively protect networks, it is vital to have visibility into all connected assets and devices, including sanctioned and unsanctioned, and newly deployed. This also includes network behavior, all applications, and all internet connections.

Visibility into OT assets allows understanding of which assets are most critical to the operation of the business, and helps determine the OT asset risk by monitoring internal and external communications (e.g., remote operations communication) and alerts in case of deviation from normal process behavior. To ensure no disruptions, the asset identification and risk assessment process should be passive and non-intrusive to OT operations.

Least privilege access: secure the OT perimeter, assets, and enforce segmentation policies

Least-privilege Access Control

Zero Trust security starts with least privilege access and securing the OT perimeters with an effective segmentation of the OT networks from corporate IT and Internet. This helps to protect on-site and remote operations, and 5G assets by reducing the attack surface and preventing unauthorized access and lateral movements of threats.

Secure OT assets with further zoning and segmentation based on OT assets, protocols, and risk context. Contextual and granular segmentation policies should be created to effectively separate the different parts of the network and enforce least-privilege access while adhering to best practice standards for segmentation.

Continuous trust verification: continually assess OT asset communications and processes

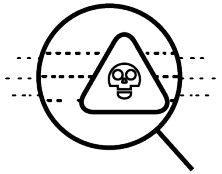
Continuous Trust Verification

Continuous trust verification identifies unwanted asset communications and segmentation policy breaches in OT assets and networks. It should also assess changes in asset posture, user behavior, and app behavior.

Any suspicious behavior should be detected immediately to revoke access in real time. Continuous trust verification accelerates incident response by correlating, isolating and quarantining infected OT assets from the network.

Continuous security inspection: prevent threats to critical systems

Continuous Security Inspection



Continuous security inspection is the final and crucial step in closing the Zero Trust security loop for network-connected assets. Even if an asset has been profiled and placed in the correct segment, it could still be compromised during its connection to the network. Continually monitoring all logs through Layer 7, maintains and protects the network.

Deep and ongoing inspection of all traffic, even for allowed connections, prevents all threats, including zero-day threats. To prevent threats to critical systems and policies, technology must be in place to defend against known and unknown threats and ICS-specific threats.

The most comprehensive Zero Trust security for OT assets and networks, remote operations, and 5G networks

The benefits of digital transformation and connectivity in OT environments is undeniable, but so are the risks. Palo Alto Networks provides the most comprehensive Zero Trust with the widest coverage of Zero Trust principles across OT networks, remote operations, and 5G networks.

Reduce operations complexity by 95% with a unified security platform.[8] Extract the maximum benefit from all assets with the least risk of exposure to cyber threats. Be future-ready for 5G by adopting digital transformation with confidence as Palo Alto Networks secures your 5G connected assets and networks.

Powered by the industry's first AI/ML-powered visibility engine, Palo Alto Networks Zero Trust OT Security solution delivers the most comprehensive OT visibility and consistent Zero Trust security, leveraging both on-prem security control and cloud-delivered security services.

Think Zero Trust OT Security.
Think Palo Alto Networks.

At Palo Alto Networks our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We are at the forefront of protecting tens of thousands of organizations across clouds, networks, and devices and help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration.

Curious to learn more about Zero Trust OT Security?

CHECK OUT THESE RESOURCES →

Founded in 2005
Palo Alto Networks is based in Santa Clara, California, and serves customers globally with offices worldwide.

1 .Gartner, Inc., Press Release, 2021
2. Gartner, Inc., Gartner IoT Forecast, 2022
3. MarketsandMarkets™, 5G Industrial IoT Report, 2021
4. ISF Research, ICS Insights: Organic Convergence, 2021
5. CISA, ICS Cybersecurity Alerts & Advisories (analysis), 2023
6, 7. SANS, 2021 Survey: OT/ICS Cybersecurity, 2021
8. ESG, Analyzing the Economic Benefits of Palo Alto Networks Industrial OT Security, 2023

www.paloaltonetworks.com

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087