The Power of &

A CISO's guide to navigating OT & IT convergence in the manufacturing industry.

paloalto® NETWORKS | STRATA™

As emerging technologies allow you to connect your organization's operational technology (OT) assets to enterprise IT systems and the cloud, it's opening up unprecedented opportunities to digitally transform operations.

The benefits of OT-IT convergence are well known: connected value chains; increased efficiency, productivity, and resilience; automated links between your plants and your customers; and much more.

Manufacturing 4.0 initiatives can increase labor productivity by 30 percent and reduce machine downtime by 50 percent—all while controlling costs and improving safety.[1]

With so much to gain, it's no wonder boardrooms across the industry are set on reaping the benefits of OT-IT convergence as quickly as possible.

Doing so securely, however, is the tricky part because you need to manage the unique cybersecurity challenges of OT connectivity. This includes the implicit risk of connecting inherently vulnerable systems in a highly sophisticated threat landscape amid the complexity of varied and sometimes conflicting boardroom priorities.

1. Capturing the true value of Industry 4.0, McKinsey & Company.

paloalto NETWORKS | STRATA

How can you ensure that your OT assets are secure and support the initiatives that will power your organization into the future?

paloalto NETWORKS | STRATA

400% expected increase in manufacturing OT assets

15B 5G-connected industrial assets by 2026

70% of ICS/SCADA assets have external connections

1K CVEs in industrial control systems

80+ vulnerabilities in top four OT vendors

33% of ICS attacks in 2021 used public-facing applications

37% of ICS attacks in 2021 used external remote services

Progress has outpaced security.

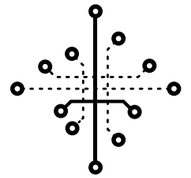
If your organization has begun to converge OT and IT environments without an integrated, end-to-end security solution in place, you're not alone.

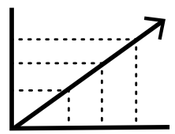
Manufacturing organizations are connecting OT assets at a breathtaking pace. By 2026, industrial organizations are expected to employ more than 15 billion new and legacy assets connected to 5G, the internet, and the cloud. And by 2030, manufacturers are likely to increase their use of OT assets by 400 percent.[2]

As OT systems are integrated into IT environments, manufacturing organizations can use powerful computing platforms and cloud-delivered enhanced services to achieve a wide range of benefits.

Maintaining OT systems remotely allows IT expert technicians to diagnose and fix problems at any time from anywhere, reducing downtime.

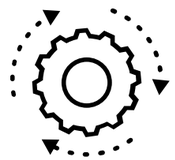
Organizations can use AI and machine learning models to create greater symbiosis in human-machine interaction.





Capturing data from OT assets in real time drives innovation in process engineering.

End-to-end digitization streamlines design, engineering, and production, reduces time to market, and makes organizations more responsive to customer needs.



2. MarketsandMarkets 5G Industrial IoT Market Report, 2021.

So far, the solutions that have been available to secure OT-IT convergence have been unable to deliver end-to-end visibility & the control to prevent threat actors from gaining access—or avert a widespread attack.

OT-CENTRIC SOLUTIONS

Strong visibility without device-level management or control

IT-CENTRIC SOLUTIONS

Management and segmentation capabilities without adequate visibility

paloalto NETWORKS | STRATA

OT-IT convergence brings two worlds together.

Historically, OT systems have been protected from cyber threats by air gaps. Without connections to the data center, the cloud, or the internet, most weren't built with connectivity in mind. As a result, they lack the built-in security features of systems designed for the IT landscape.

Connecting them removes the protection of having an air-gapped OT environment, potentially exposing uniquely vulnerable systems to sophisticated threat actors and putting the whole organization at risk.

Air-gapped environments also create a management challenge. OT and IT have been evolving rapidly for decades, with different overarching goals. Converging the technologies requires bringing together leaders with different, and potentially conflicting, priorities.

Stakeholders in OT-IT convergence

C-Suite

Focused on achieving board-level commitments to profitability, sustainability, and growth.

OT leaders

Focused on optimizing human-machine interaction and improving OT system efficiency.

IT leaders

Focused on achieving Manufacturing 4.0 goals through enterprise-wide modernization and streamlined operations.

Plant managers

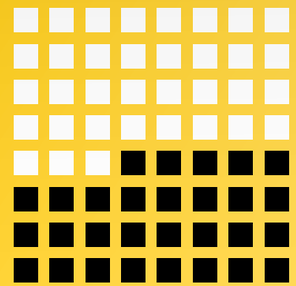
Focused on keeping plants operational and productive and maintaining worker and environmental safety.

Secure OT-IT convergence requires a solution that not only solves the technical challenges of cybersecurity, but also delivers on the key priorities of each of your stakeholders. How do you ensure safe, secure plant operations today and open the door to the future?

How do you secure your OT assets and streamline operations?

paloalto NETWORKS | STRATA

Attacks on OT assets can have greater and more negative effects than attacks on IT systems because their impacts aren't limited to digital environments.



35%

of the 64 OT cyberattacks reported in 2021 had physical consequences[3]

$140M

estimated damage from 2021 attacks per incident[3]

paloalto NETWORKS | STRATA

3. "How to enhance the cybersecurity of operational technology environments" McKinsey & Company, 2022.

Three focus areas for secure OT-IT convergence.

At Palo Alto Networks, we understand the urgent business need to connect your OT systems to your IT infrastructure, the unique security risks associated with OT-IT convergence, and the significant harms an OT cyberattack can cause.

Focusing on three use cases can help you make your OT environment as secure as your IT systems—and ensure that all your stakeholders get what they want.

1 Ensure comprehensive visibility

2 Deliver Zero Trust Security for all OT environments

3 Simplify operations

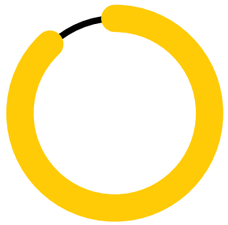
paloalto NETWORKS | STRATA

FOCUS 1

Comprehensive visibility.

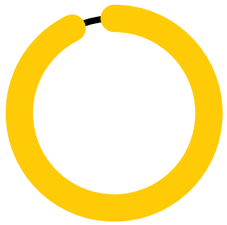
You can't protect what you can't see, but having OT systems connected to your IT infrastructure doesn't in itself make them visible to your security stack. Securing OT assets begins with an automated solution that ensures you're getting the full context of every asset—its purpose, what security policies apply, and what data it is accessing—all the time. Does your security solution provide automated visibility throughout your OT environment?

Zero Trust OT Security delivers comprehensive visibility and control.



90%

of assets are discovered within the first 48 hours[4]



95%

more simplified than other OT security services[5]

Automated visibility for all OT assets

- Automate discovery and profiling of new and existing assets using AI, machine learning, and crowdsourced telemetry.
- Gain context-rich insight into your OT environment with Device-ID, App-ID, User-ID, and 5G Equipment ID.
- Detect even unknown and zero-day threats with proactive threat prevention, bringing the industry's leading IPS, malware analysis, and web and DNS prevention technologies to your OT systems.

Critical business benefits

- Provide secure access for on-site and remote users with the leading cloud-based secure access service edge (SASE) solution.
- Simplify compliance with industry guidelines and government regulations with an up-to-date, accurate inventory of your OT landscape.
- Save countless hours by eliminating the manual process of gathering asset data, and respond to threats in minutes, instead of days or weeks.

CUSTOMER SPOTLIGHT

BRISA

Tire manufacturer Brisa uses Palo Alto Networks Zero Trust OT Security for visibility and to protect the more than 2,500 OT and IoT assets powering its smart manufacturing operations. Using the solution has reduced OT security costs by at least 30 percent, increased the security team's productivity by 20 percent, and resulted in a stronger overall security posture.

paloalto NETWORKS | STRATA

4. Palo Alto Networks internal testing, Enterprise IOT Service, 2020.
5. The Enterprise Strategy Group Economic Validation report on Industrial OT Security, commissioned by Palo Alto Networks, 2023.

FOCUS

2

Zero Trust security for all OT environments.

At a time when sophisticated threat actors are leveraging AI to increase the speed and effectiveness of their attacks, Zero Trust security is essential, especially in cyber-physical manufacturing environments where a security breach can compromise worker safety or cause an environmental catastrophe.

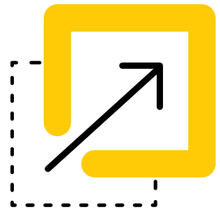
Do you struggle to apply a Zero Trust security approach to your connected OT systems?

paloalto NETWORKS | STRATA

Zero Trust OT Security is built to bring Zero Trust to the shop floor.

Apply Zero Trust to every environment

- Zero Trust security for OT networks and assets, remote operations, and 5G networks and devices.
- World-class access control to ensure the right people have the right access to the right assets—all the time.
- Asset-level segmentation to eliminate implicit trust and ensure continuous validation.



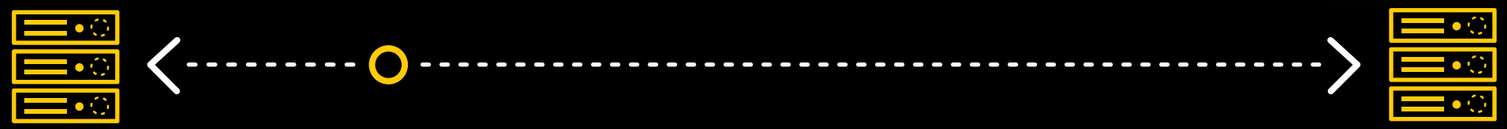
20x faster
policy creation[6]

Critical business benefits

- Continually assess security posture and stop advanced threats in seconds.
- Automate quarantine of compromised assets to prevent lateral movement and minimize impacts on production.
- Achieve the least-privileged access, enforcement, and segmentation capabilities of your IT environment across the OT landscape.

100%
of OT traffic is validated[6]

6. Forrester Total Economic Impact™ (TEI) study, 2021.



Only

13.5%

of enterprises are currently focused on or already monitoring lateral traffic[7]

East-west traffic inside an OT environment, which is secured by a Zero Trust approach, represents the greatest OT security threat.

Security products designed for other markets are primarily focused on north-south traffic, such as communication between the data center and the cloud, leaving a critical gap that can only be closed with Zero Trust security built specifically for the unique architecture of OT environments.

7. VDC Research, Never Trust, Always Verify, 2023

FOCUS 3

Simplified operations.

In the past, each new security challenge has been met with a unique, best-of-breed solution. If your organization is like most manufacturers, you're using dozens of point solutions, each requiring specialized training and with its own user interface. A unified platform provided by a single vendor allows you to simplify deployment and operations.

Zero Trust OT Security converges OT and IT security in a single platform.

95%
reduction in complexity compared to alternatives[8]

Achieve ROI of up to
351%[8]

Improve your security posture with streamlined operations

- Use a single, integrated platform to proactively detect, manage, and secure all users, assets, and networks.
- Adapt to new challenges with the ability to set and change policies up to 20 times faster.
- Harmonize OT security with security orchestration, automation, and response (SOAR) for a playbook-based incident response.

Critical business benefits

- Improve operational costs and reduce the risk of downtime, non-compliance, and a potential breach.
- Deploy 15 times faster with automated implementation, reducing the impact on plant operations.
- Help the business grow while driving down OT and IT costs through security consolidation.

CUSTOMER SPOTLIGHT

Eczacıbaşı

Turkish industrial group Eczacibasi is reducing its overall security costs by consolidating enterprise and OT security with Palo Alto Networks. Using Zero Trust OT Security, the group's 46 companies operating in 12 countries benefit from centralized OT security management. The solution integrates seamlessly with Prisma® Access and delivers comprehensive visibility and control over every OT application and function using OT protocols without impacting network performance.

paloalto NETWORKS | STRATA

8. Enterprise Strategy Group, Analyzing the Economic Benefits of Palo Alto Networks Industrial OT Security, commissioned by Palo Alto Networks, 2023.

paloalto NETWORKS | STRATA

Unleash the Power of &

At Palo Alto Networks, our mission is to empower manufacturing leaders like you to see around every corner, automate security workflows, and bring IT-grade Zero Trust to every OT environment.

With fully integrated OT and IT security, you can rest assured that your plants will keep working safely, your stakeholders will stay happy, and you can reach boldly for your business goals.

That's the power of &

knowing you can keep your entire infrastructure safe

&

- Ensure your plant operations run smoothly
- Free your teams from low-level, manual work
- Drive future success with a platform to support any Manufacturing 4.0 initiative
- Achieve your full transformation

The future of manufacturing has arrived.

Embrace it confidently with Zero Trust OT Security from Palo Alto Networks.

WWW.PALOALTONETWORKS.COM/INDUSTRY/MANUFACTURING