Asegurando el perímetro Industrial

Un Enfoque de Confianza Cero para la Seguridad OT

Diego Salazar Gómez

Channel Systems Engineer

Ingeniero en seguridad de la información con más de cuatro años de experiencia en soporte, atención a clientes y liderazgo de equipos multidisciplinarios.

Actualmente dirige un grupo de especialistas, gestionando proyectos desde la visión estratégica hasta la ejecución técnica.

Se distingue por su proactividad, capacidad de trabajo en equipo y manejo de entornos complejos.

Enfocado en aportar valor estratégico y en el desarrollo continuo de su carrera profesional en seguridad informática.

paloalto NETWORKS

GBM

Jorge Clará

Cyber Security Pre-Sales Engineer

Ingeniero de sistemas informáticos, con especialización en seguridad Informática y auditoria de sistemas utilizando el análisis informático forense.

Posee más de 11 años de experiencia en tecnologías de networking y ciberseguridad, empleando de manera adecuada las buenas prácticas de la industria.

Jorge es un apasionado en aprender, ayudar y evolucionar en todos los retos que con lleva el mundo digital.

Agenda

- Introduction
- OT Security Solution Review
- Secure OT Networks & OT Assets
- Secure Remote Operations
- Secure 5G Assets & 5G Networks
- Final Q/A

OT Security Solution Review

Industrial organizations face unprecedented change

Accelerating Digital Transformation

OT networks are becoming more dynamic and hybrid

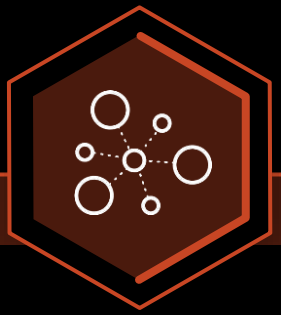
Dramatically increased threat surfaces

Intensifying Threat Landscape

Safety and operation downtime risks

Existing OT security not keeping pace

Advanced detections are required



Fragmented Defense Landscape

41%* of organizations work with 10 or more cybersecurity vendors

Complexity of point solutions is driving tool consolidation

Understanding OT attack surface trends helps define the right solutions

Top Attack Vectors

#1 Attacks from Unsanctioned Internet Connections for remote access and remote operations

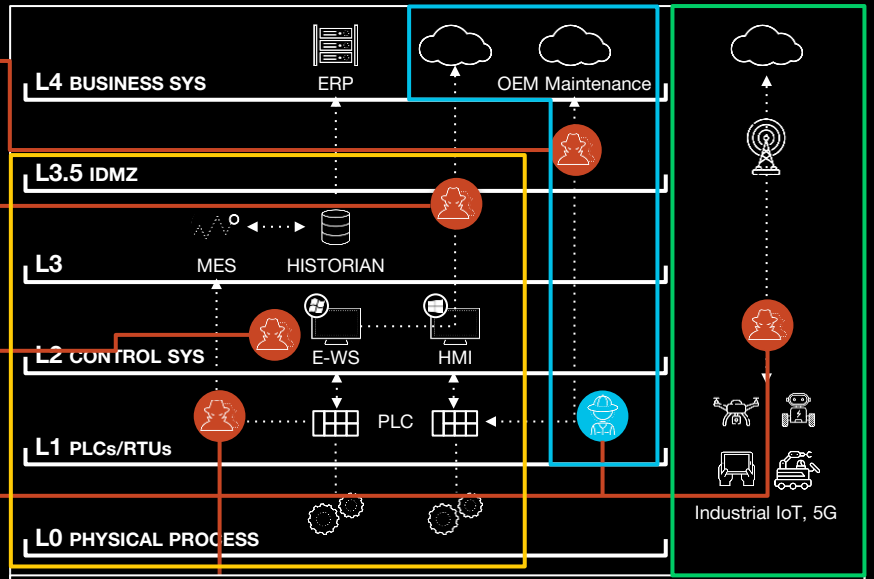
#2 Ransomware/Phishing that compromises IT and traverses to ICS networks

#3 Engg workstations & op assets compromised due to **unpatched legacy OS vulnerabilities**

#4 Unauthorized access & risk from onsite 3rd party vendors and misuse of removable media

#5 (Trending up): ICS-specific attacks that compromise OT process integrity

OT Environment (Illustrative Purdue Model)



Integration with IT security is critical

72% of OT attacks come from IT

Palo Alto Networks State of OT report

Securing OT Requires

Secure **OT Network & Assets**

Secure **Remote Operations**

Secure **5G Assets & Networks**

Context Setting: Palo Alto Networks OT security solution

Comprehensive coverage, consistent zero trust security, simplified operations

1 Secure OT Networks & OT Assets

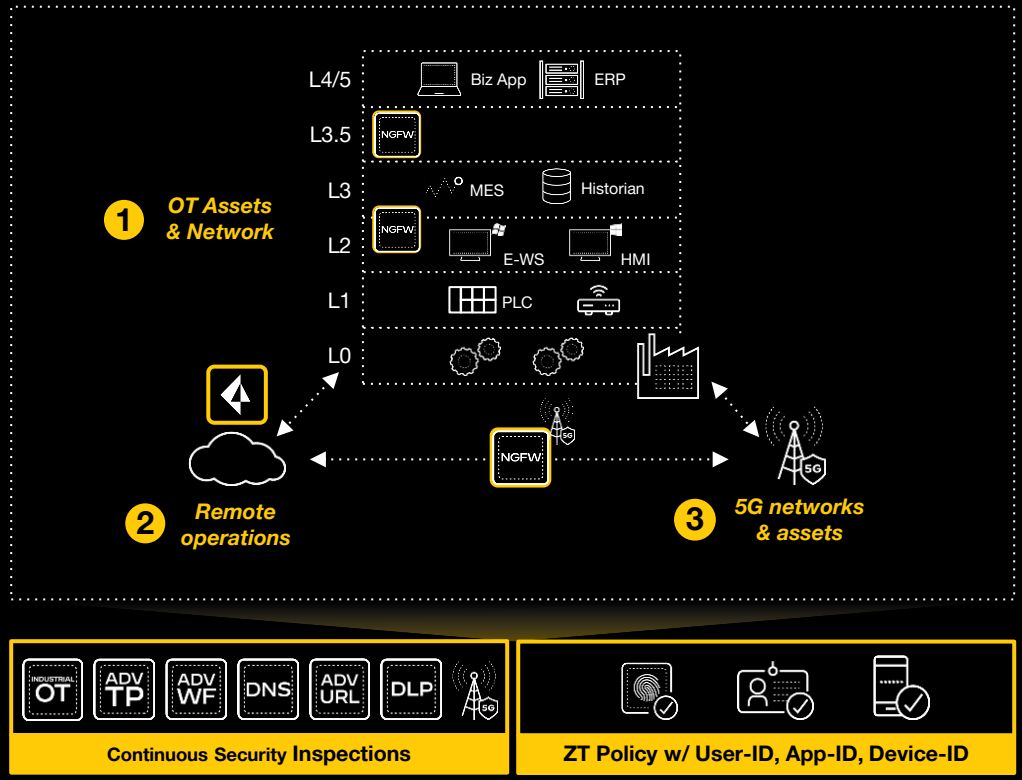
- Visibility into OT assets and risk factors
- IT/OT (iDMZ) and OT segmentation
- Continuous security inspections

2 Secure Remote Operations

- Secure OT remote access (with ZTNA)
- Centralized SCADA operations (with SD-WAN)

3 Secure 5G Assets & 5G Networks

- Mobile device (4G/LTE/5G) visibility
- Mobile identifier based security policy
- Advanced security inspections



Secure OT Networks & OT Assets

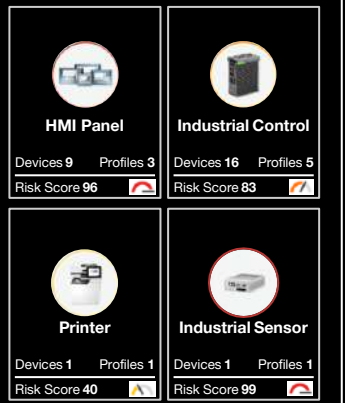
Industrial OT Security accelerates customer's security journey

1 2 3 4 5

DISCOVERY

Auto discover, classify and assess risks of the IoT devices

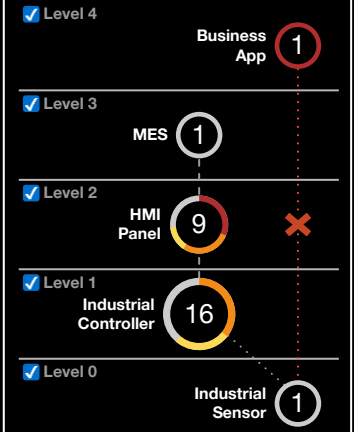
Device Categories (sample)



DEVICE COMMS

Understand device communication pattern and normal behavior

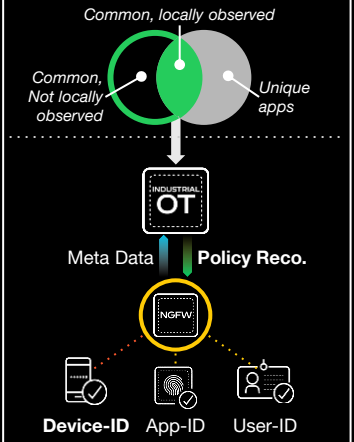
Device Communication Patterns



SEGMENTATION

Segmentation and prescriptive least access control policies

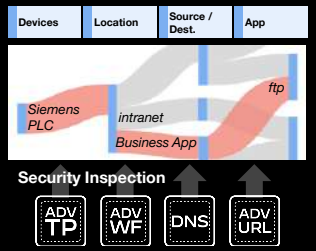
Device Behavior Analysis



MONITORING

Continuous monitoring – trust verification and security inspection

Continuous Monitoring

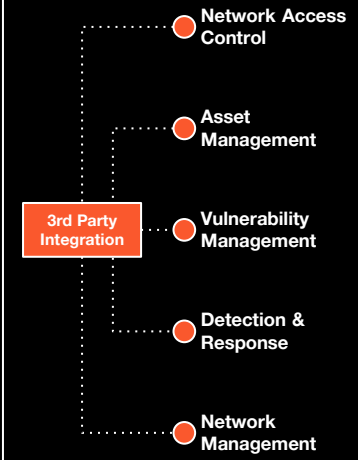


OT Process Integrity (sample criteria)

1. **SELECT: DEVICES** THAT COMMUNICATE WITH **DEVICES** BY **TRAFFIC VOLUME** OR **APP USAGE**
2. **ADD ACTION: GENERATE ALERT** AS **PRIORITY** AND SEND TO **3RD PARTY** AND/OR **ASSIGN TO USER**

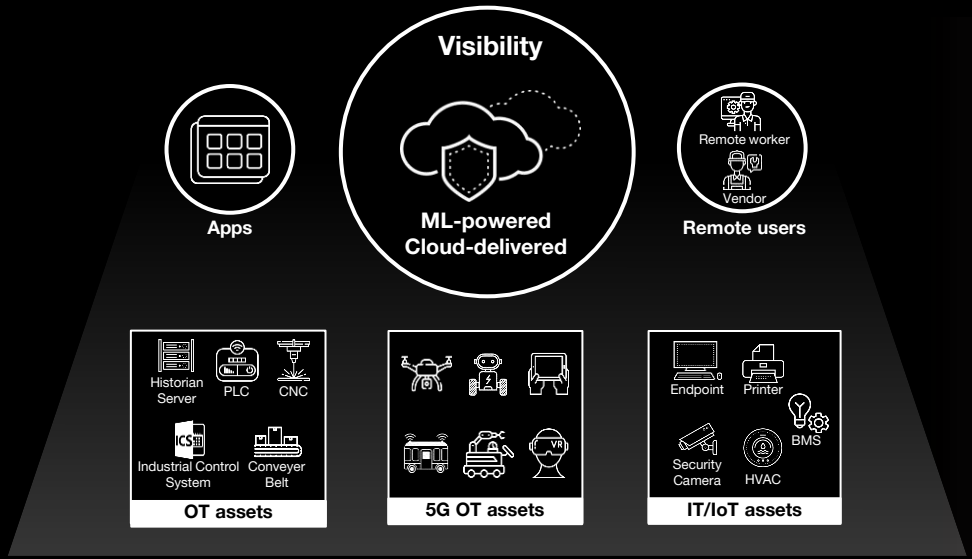
AUTOMATION

Simplify operations and automate workflow



The solution is anchored on comprehensive OT specific knowledge

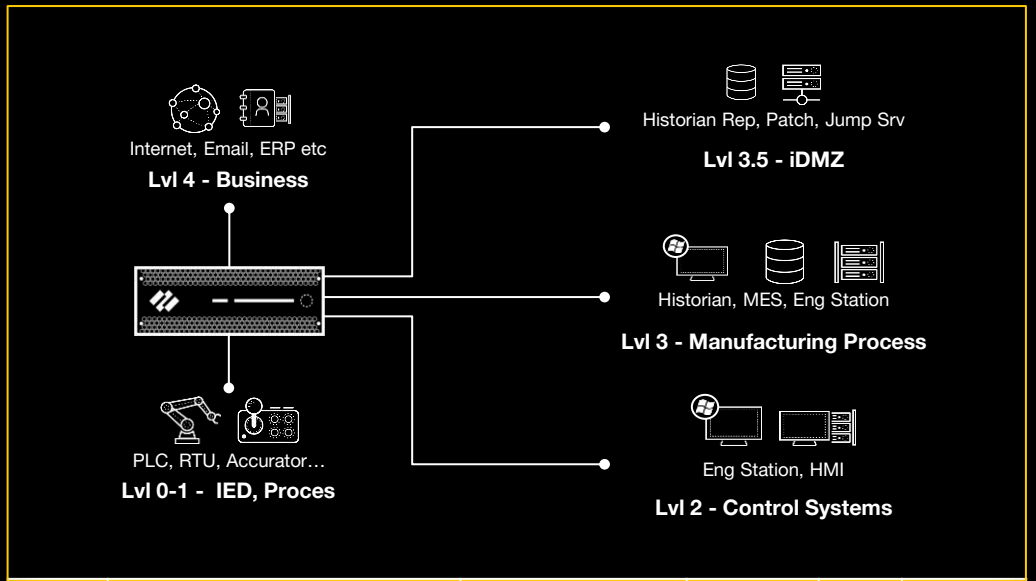
Industry's 1st AI/ML visibility engine for assets, apps & users across OT networks, 5G networks & remote operations



- **ML-powered scalable discovery**
- **OT/IoT/IT/5G assets, assets, and protocols context**
- **Apps at layer 7 and users identity**

700+	Unique OT Assets Profiles
1000+	OT/ICS App-IDs
600+	OT/ICS Threat Signatures

Contextual segmentation and least privilege access policy



	Source			Destination				
Rule	Zone	Address	User	Zone	Address	Application	Action	Security Profile
PLC READ	OT L3	Siemens HMI	ICS_VENDOR_A	ICS	Siemens PLC	S7_Read	Allow	Threat Prevention (Modbus Exploits)

Device-ID
Complete inventory of IT & OT assets powered by IoT Security
ML-powered device classification and behavior monitoring

App-ID
Comprehensive ICS/SCADA protocol coverage with deep insight
All major ICS & SCADA protocols across industries.
Protocol insight to monitor & protect process integrity

User-ID
Role-based access control for hybrid OT environments
OT personnel, onsite 3rd party vendors etc

Mitigate critical vulnerabilities without disruption

with industry's only risk-based guided virtual patching solution

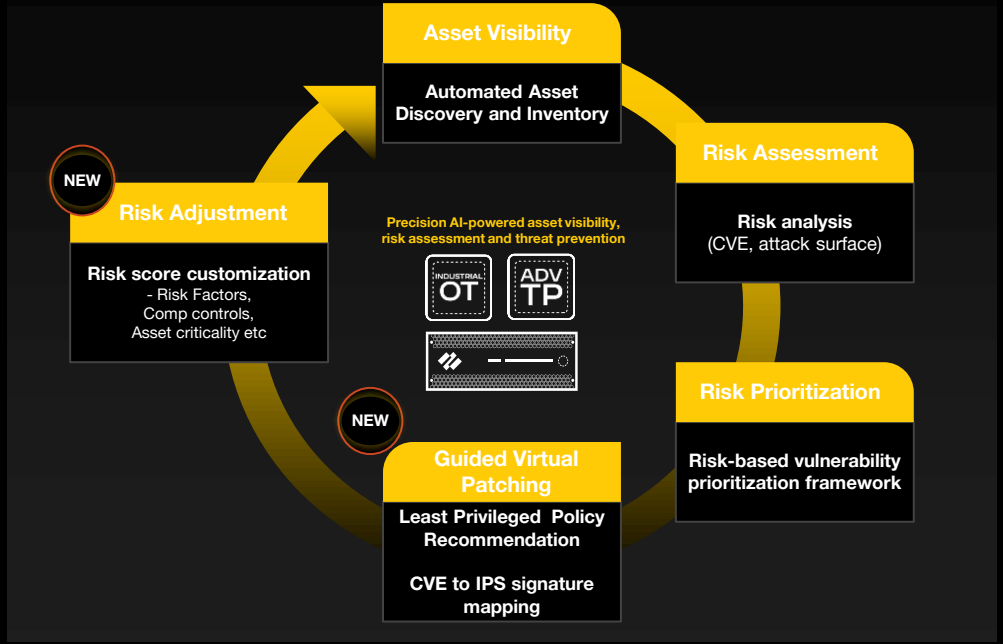
Challenges

Too Many Vulnerabilities

OT Assets are hard to patch
due to limited downtime

Complex mitigation controls across multiple tools

End-to-End OT risk management workflow in an unified platform



Benefits

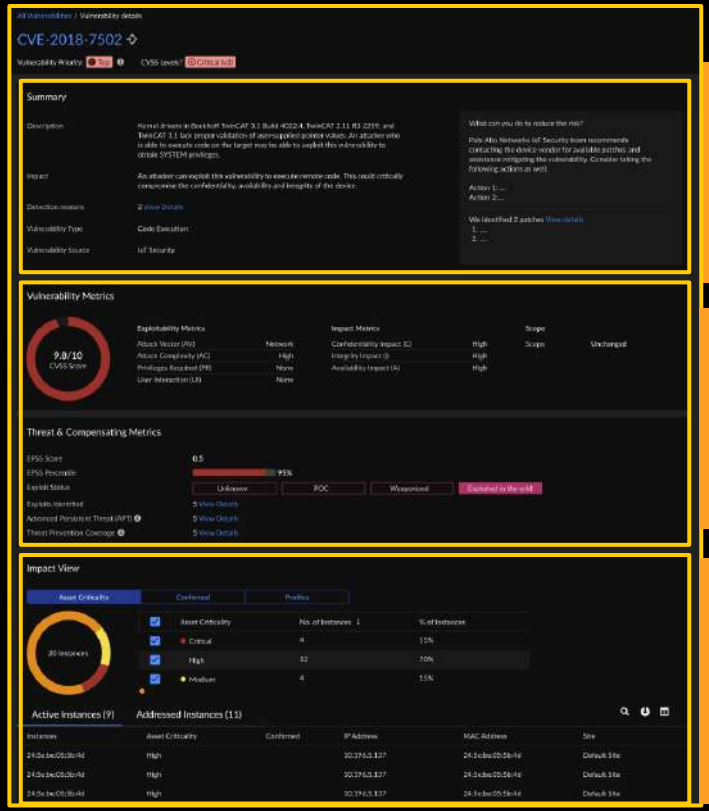
Reduce vulnerability noise, focus what matters most

Mitigate critical risk for hard to patch OT assets

Streamlined risk management workflow in an unified platform

paloalto NETWORKS | STRATA

Vulnerability Assessment and Risk Prioritization



Summary

For vulnerability context and recommendations
- Vulnerability Description
- Detection reason / matching criteria
- Potential Impact
- Recommendations and patch information

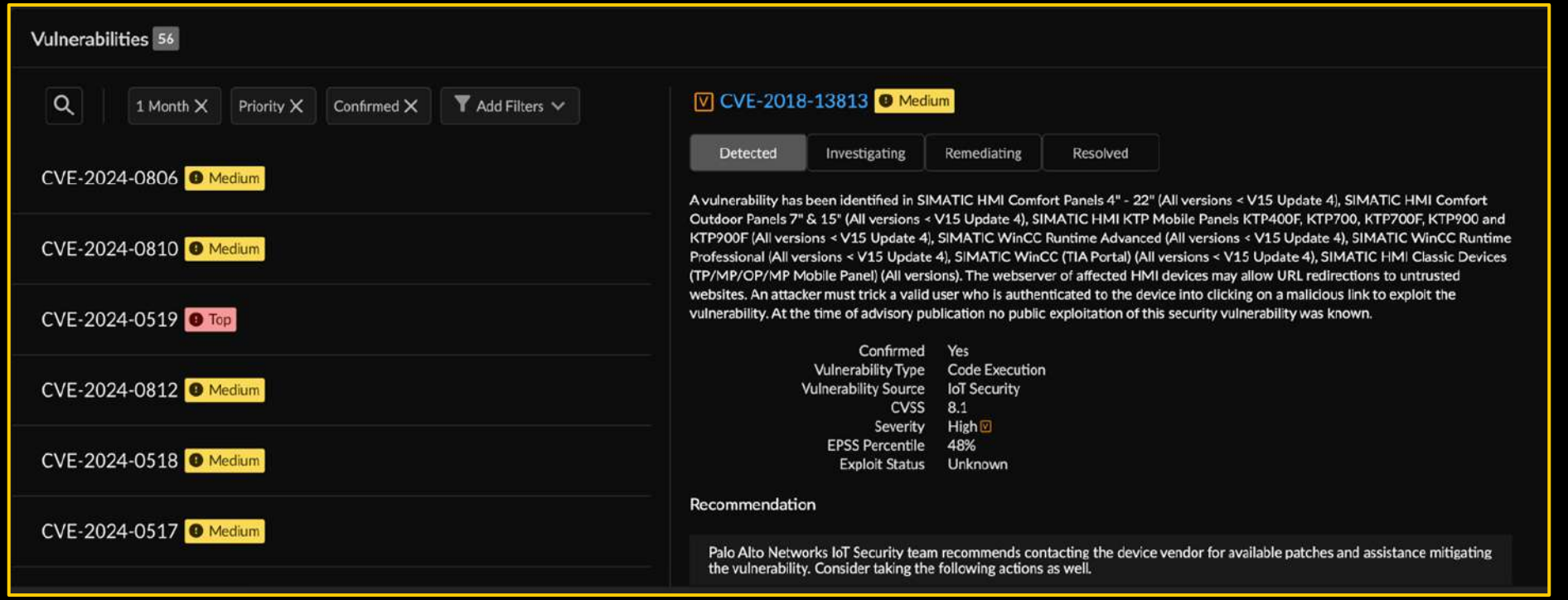
Vulnerability, Threat & Compensating Metrics

For severity and threat context
- CVSS metrics
- EPSS
- Exploitation Evidence
- Advanced Persistent Threats (APTs)
- PANW Threat Prevention Signature available

Impact View

For affected devices:
- View all affected devices
- View by criticality level, profiles or confirmed vulnerability matching status

CVE Remediation



Industrial OT Security enhancements

Continued Expansion of OT Discovery Techniques

Active Discovery

- 15+ protocols

  BACnet | CIP-IP | CodeSys V3 | FINS | FOCAS | Melsoft | MMS | Modbus | Reverse-DNS | S7 | S7-Comm-Plus | SNMP v1/2/3 | UMAS | UPnP | WinRM

NEW 6 new Protocols

- Native PanOS support without need to deploy additional hardware

Passive Discovery

NEW Sensor-only deployment mode for sensitive industrial environments

Integrations

NEW Parse inventory and configuration files from OT applications

Beckhoff | Rockwell | Schneider | Siemens

- Bi-directional integration with ServiceNOW OT module

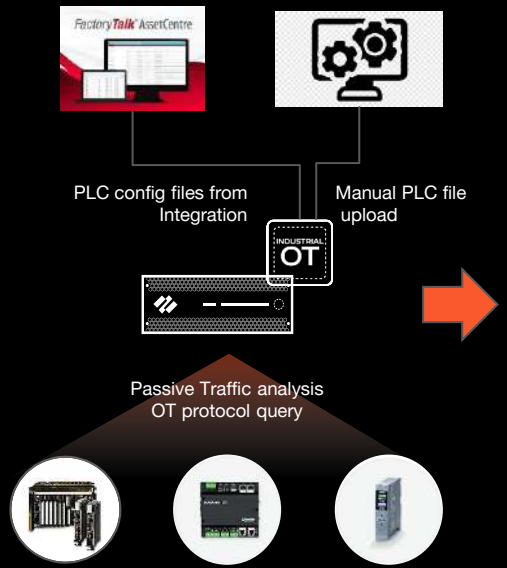
800+ unique OT asset profiles - ↑ 57% YoY

500+ unique OT vendors - ↑ 54% YoY

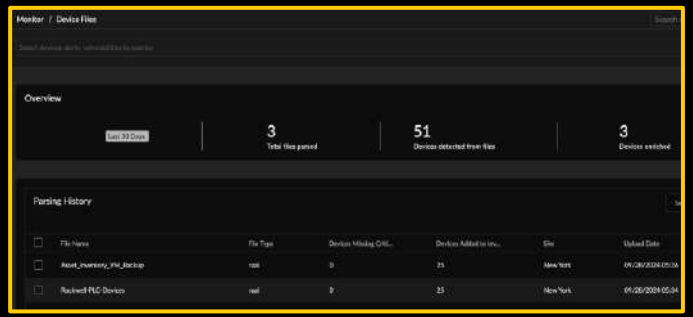
Asset Identity

Industrial OT Security enhancements

Enriching PLC device contexts using Configuration Files



Enriched PLC inventory device contexts



- Enrich PLC device context via the correlation of live traffic analysis and offline PLC config file parsing.
  - PLC Chassis and I/O Modules
  - Firmware
  - Model
  - Serial Number
  - Device Name
  - Downstream non-IP devices*
- Support files from leading ICS vendors

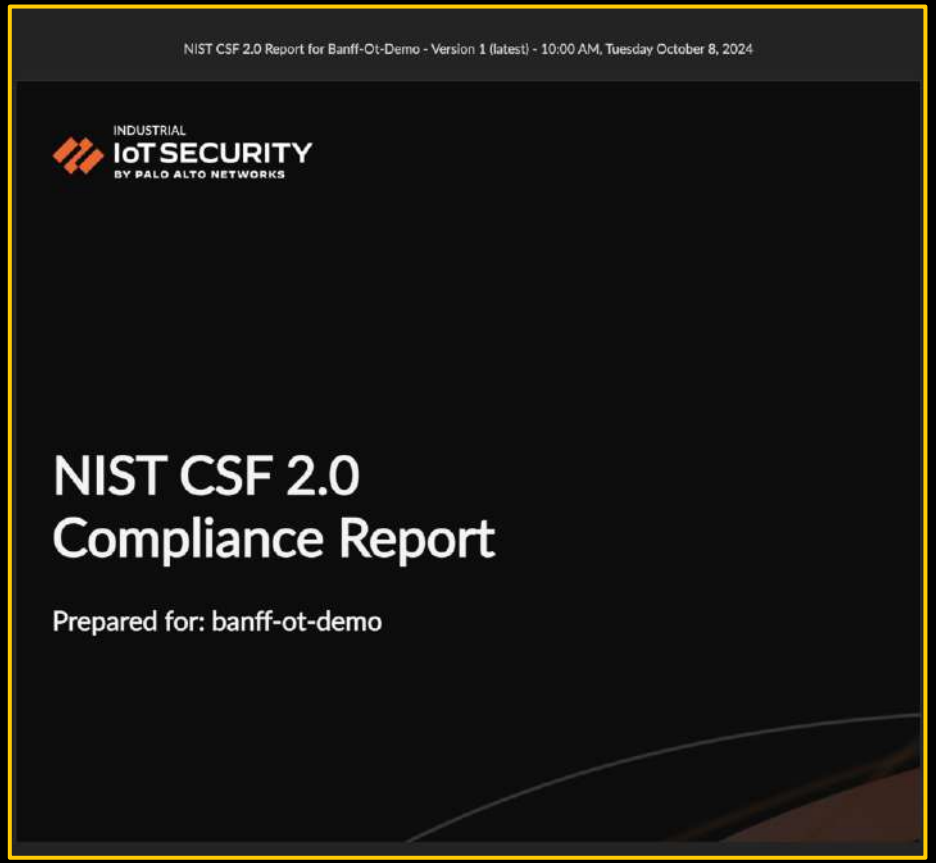
Rockwell	Siemens	Beckhoff	Schneider
.RAAI .L5X	.PLF .IDX .AP15_1	.TSPROJ .SLN .PLCPROJ	.XEF

Industrial OT Security enhancements

Out of Box NIST CSF Report

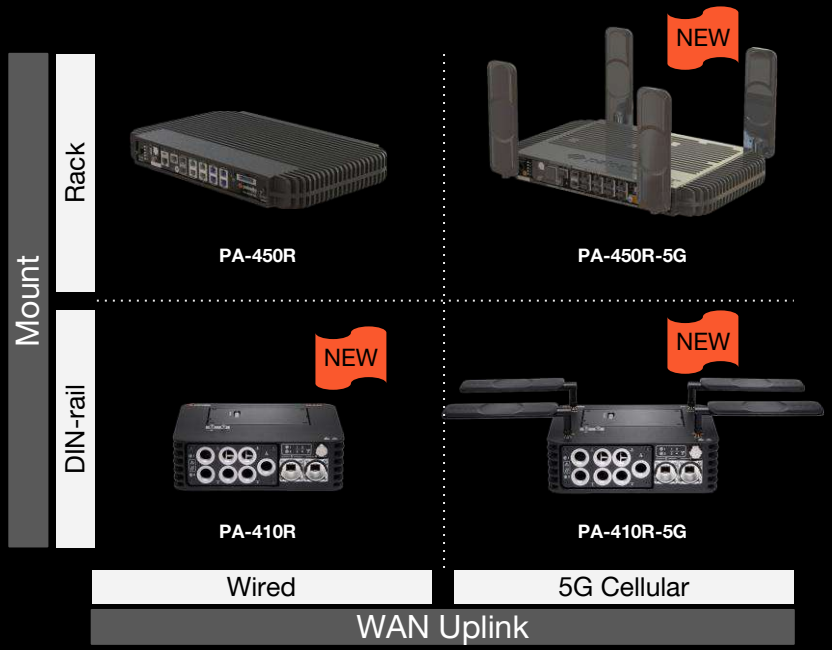
NIST CSF Report NEW

- New NIST CSF compliance report to map to the OT cybersecurity framework
- Compliance report matching various NIST guidelines
- All the key pillars of NISF framework are matched against the OT Security dashboards:
  - Identify
  - Protect
  - Detect
  - Respond



PA-400R Series

ML-Powered security across harsh industrial environments



Resiliency features ideal for rugged environments

- Fail-to-wire ports for continuous traffic in case of power/OS failure
- Redundant DC supply: 12-48VDC
- Industrial temperature range :-40 to 70 DC
- High IP rating: IP-40 (450R / 5G), IP-65 (410R / 5G)

High performance architecture for advanced security applications

- PA-450R / 450R-5G: 1.4G Threat / 3.2G App-ID
- PA-410R / 410R-5G: 0.7G Threat / 1.4G App-ID

Native 5G WAN uplink for geographically distributed use cases

- Built-in modem with dual SIM support saves rack/cabinet space and simplifies deployment

Expands coverage for harsh environment use cases (examples)

- 450R: Utility Substations, Warehousing & Distribution
- 450R 5G: Traffic Light Controllers, Renewable Energy sites
- 410R: Factory floor, Power plants
- 410R 5G: O&G mid/downstream monitoring, EV Hub sites

PA-410R: Replacement for the PA-220R

Fail-to-Wire. Supports data pass through in case of power failure

-40°C - 70°C

Extended operating temperatures

700 Mbps
Full L7 threat performance

64K
Concurrent L7 sessions

1.5 Gbps
App aware performance

IP65
Compliant

PA-410R: Cellular Ruggedized Appliance for Harsh Environments Fail-to-Wire. Supports data pass through in case of power failure

-40°C - 70°C

Extended operating temperatures

700 Mbps
Full L7 threat performance

64K
Concurrent L7 sessions

1.5 Gbps
App aware performance

IP65
Compliant

PA-450R: Rugged Performance for The Harshest Environments

Fail-to-Wire. Supports data pass through in case of power failure

-40°C - 70°C

Extended operating temperatures

1.4 Gbps
Full L7 threat performance

200K
Concurrent L7 sessions

3.2 Gbps
App-ID performance

IP40
Compliant

PA-450R-5G: Cellular Rugged Performance for Harsh Environments

Fail-to-Wire. Supports data pass through in case of power failure

-40°C - 70°C

Extended operating temperatures

1.4 Gbps
Full L7 threat performance

200K
Concurrent L7 sessions

3.2 Gbps
App-ID performance

IP40
Compliant

Deployment confidence: Design & Deployment Guides for validated reference architecture

Secure Remote Operations

The Need to Secure Remote Access on Unmanaged Devices

Contractor and BYOD Increase Risks

Unmanaged or untrusted devices expose organizations to risk. Installing agents on contractors' unmanaged devices and employees' BYOD is often NOT an option.

SSH, RDP, and VNC are Prime Target for Attackers

Attackers often target SSH, RDP & VNC apps through brute force attacks, credential theft, and by scanning for open default ports, exposing enterprises to risk.

General Use Cases

Admin Operations

Employees (OT and Corporate) managing internal systems and required access to devices below iDMZ.

Contractor Access

3rd Party contractors accessing critical OT devices and support workstations via RDP or SSH, below the iDMZ in the Industrial Zone.

Sensitive Access

Contractors and/or employees on personal devices accessing sensitive apps (e.g. HMI or SCADA), hosted on jump hosts accessible only via RDP.

Privilege Remote Access Benefits

Secure Access to SSH/RDP/VNC

- Eliminate agent installations
- Isolate RDP/SSH/VNC servers from untrusted endpoints
- Access from any modern HTML5 browser

Increased Security and Control

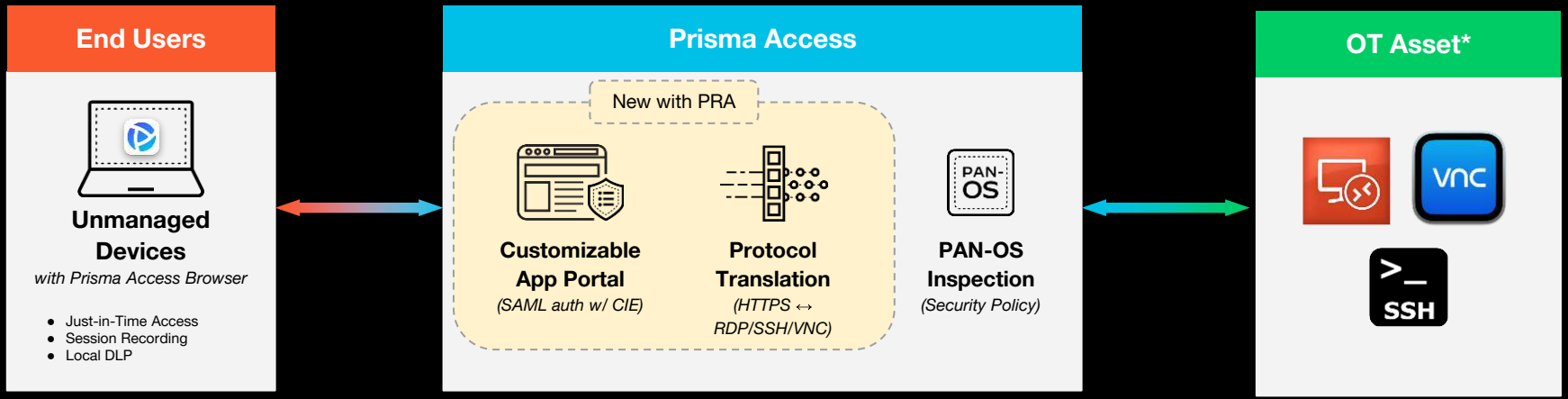
- Leverage Prisma Access for exploit prevention
- Extend Zero Trust to the browser with Prisma Access
- Gain granular last-mile DLP controls (e.g. file upload/download) and malware scanning with Prisma Access Browser

Reduced Operational Overhead

- Eliminate on-prem components to install and configure
- Leverage existing Prisma Access Service Connection or ZTNA Connector deployments
- Grow with cloud-native auto-scaled service—no need for ongoing capacity planning activities

Privileged Remote Access Data Flow

Privileged Remote Access (PRA) *enables secure agentless access to non-web apps (RDP/SSH/VNC) from unmanaged devices (e.g. devices owned by contractors, BYOD)*



*RDP/VNC/SSH connectivity may be to a on-prem jump server at the iDMZ to comply with internal architecture/standard

Context Setting: Palo Alto Networks OT security solution

Comprehensive coverage, consistent zero trust security, simplified operations

1 Secure OT Networks & OT Assets

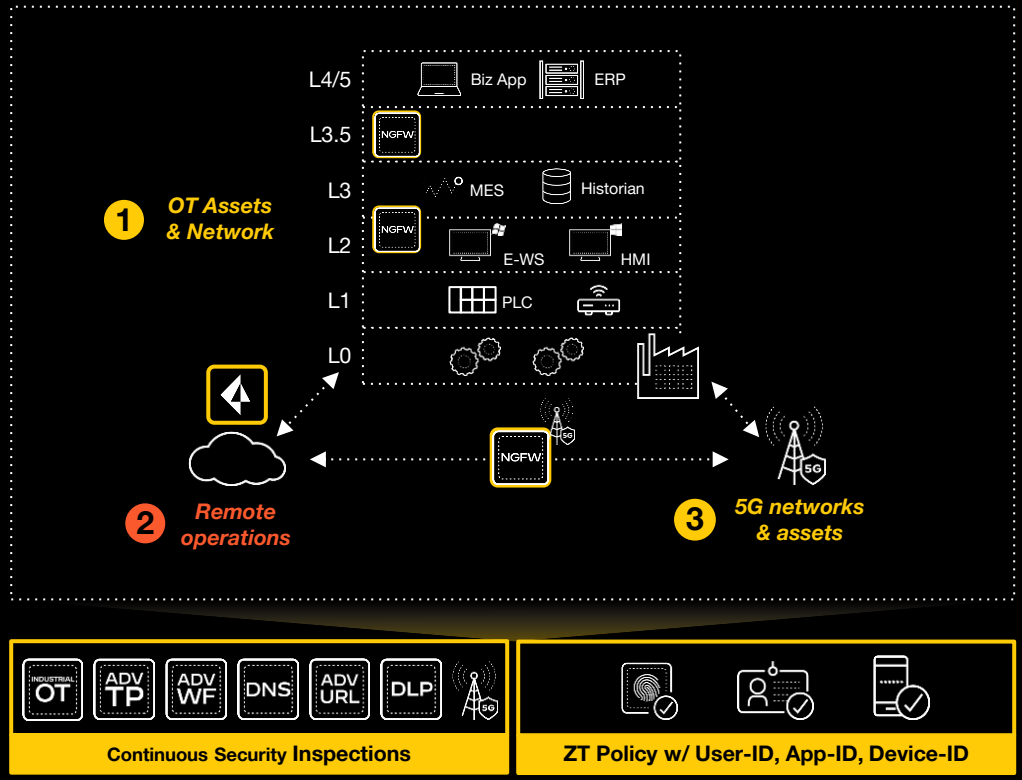
- Visibility into OT assets and risk factors
- IT/OT (iDMZ) and OT segmentation
- Continuous security inspections

2 Secure Remote Operations

- Secure OT remote access (with ZTNA)
- Centralized SCADA operations (with SD-WAN)

3 Secure 5G Assets & 5G Networks

- Mobile device (4G/LTE/5G) visibility
- Mobile identifier based security policy
- Advanced security inspections



Innovations across key solution use cases

Secure OT Networks and Assets

Risk-based Guided Virtual Patching

- Prioritize & mitigate critical CVEs for hard-to-patch OT assets w/o disruption

Industrial OT Security enhancements

- **Flexible OT Asset Discovery** techniques
  - Virtual Metadata Collector
  - 6 new Active OT Polling modules
  - Integrations
- **Enriched OT Asset Contexts**
  - New PLC insight: modularity, config file analysis, IEC-62443 analytics
- **Compliance** - Out-of-the-box NIST CSF compliance reporting

PA-400R Series Ruggedized NGFWs

- Expanded, 4-member family, featuring built-in **5G connectivity** provides reliable security for distributed harsh industrial environments

Secure OT Remote Operations

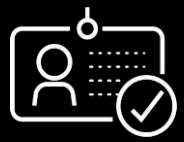
Enhanced OT remote access solution

- Honors the Purdue Model of Control for OT environment segregation
- Streamlined user experience for end user and administrator. No jump server required
- Supports OT-specific workflow and compliance
- End-to-end security from endpoint to infrastructure
- Fully encrypted tunneling for data in transit to the end device
- Simplified operations with consistent remote access across IT and OT for any user, any location and any application
- Visibility and posture assessment for last mile

New OT Design & Deployment Guides for Validated Reference Architecture

OT personas requiring remote access

Corporate Users



Corporate Asset
High Posture

- IT controlled asset
- Corporate (L4) user
- Access OT systems & devices (L3.5 or below)
- Additional authentication using OT identity provider (AD)
- Typically, will utilize a jump server or VDI environment

Field Technician

Field Asset
High-Medium Posture

- OT/IT controlled asset
- OT remote field user
- Access OT systems & devices (L3 or below)
- Authenticate using OT identity provider (AD)
- Direct connectivity to OT devices and/or systems

3rd Party Support

Vendor Asset
Low Posture

- 3rd party or BYOD asset
- Vendor technicians
- Access OT systems & devices (L3 or below)
- Authenticate using OT identity provider (AD)
- Typically, will utilize a jump server or VDI environment

Common Use Cases for OT Environments

Operational Data Access

Corporate users that need access to operational data in the OT domain. The data is contained within OT historians and used for analytical and forecasting purposes.

Remote Field Support

Field support staff that may not be on the corporate network when traveling between sites. These staff need to connect to applications and devices that are located in remote plants.

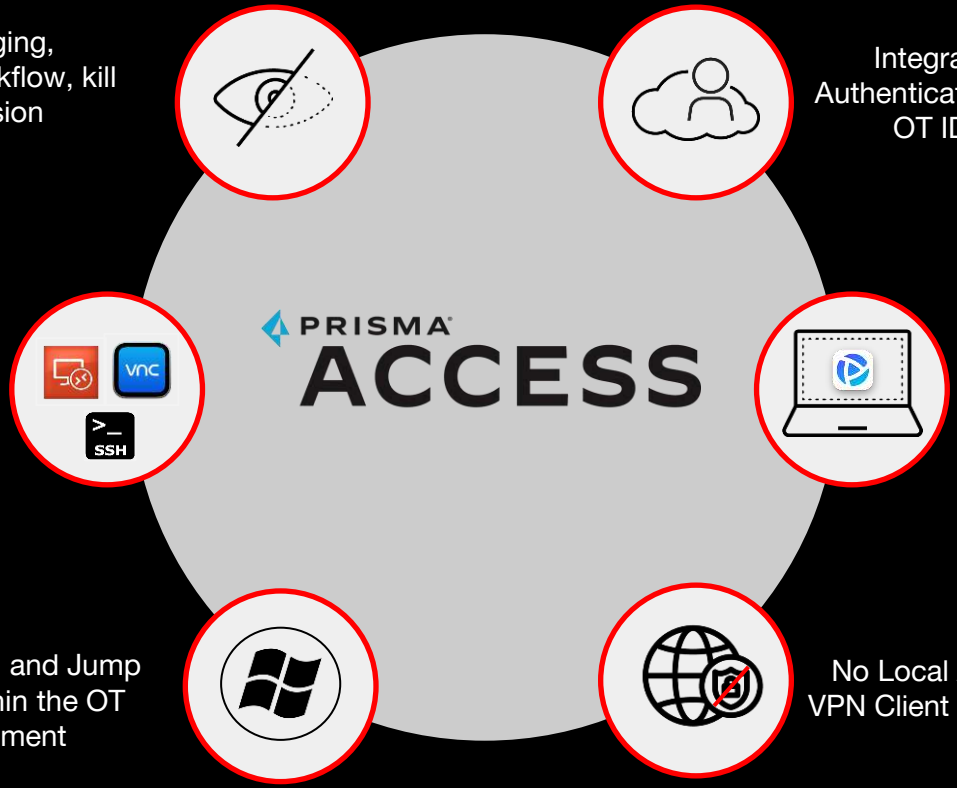
ICS Support Vendors

ICS vendors need to connect to applications and devices for remote support. Most commonly to diagnose issues with data collection and process logic. These vendors also may have new configurations and patching that may need to be uploaded.

Distributed Workflows

Simple workflow and authorization steps to allow distributed plant managers or support personnel to provision and approve access.

Compelling Features for OT Environments



Auditing, logging, approval workflow, kill switch & session recording***

Integrated Authentication with OT IDP

Multi-Protocol Support for Devices & Applications

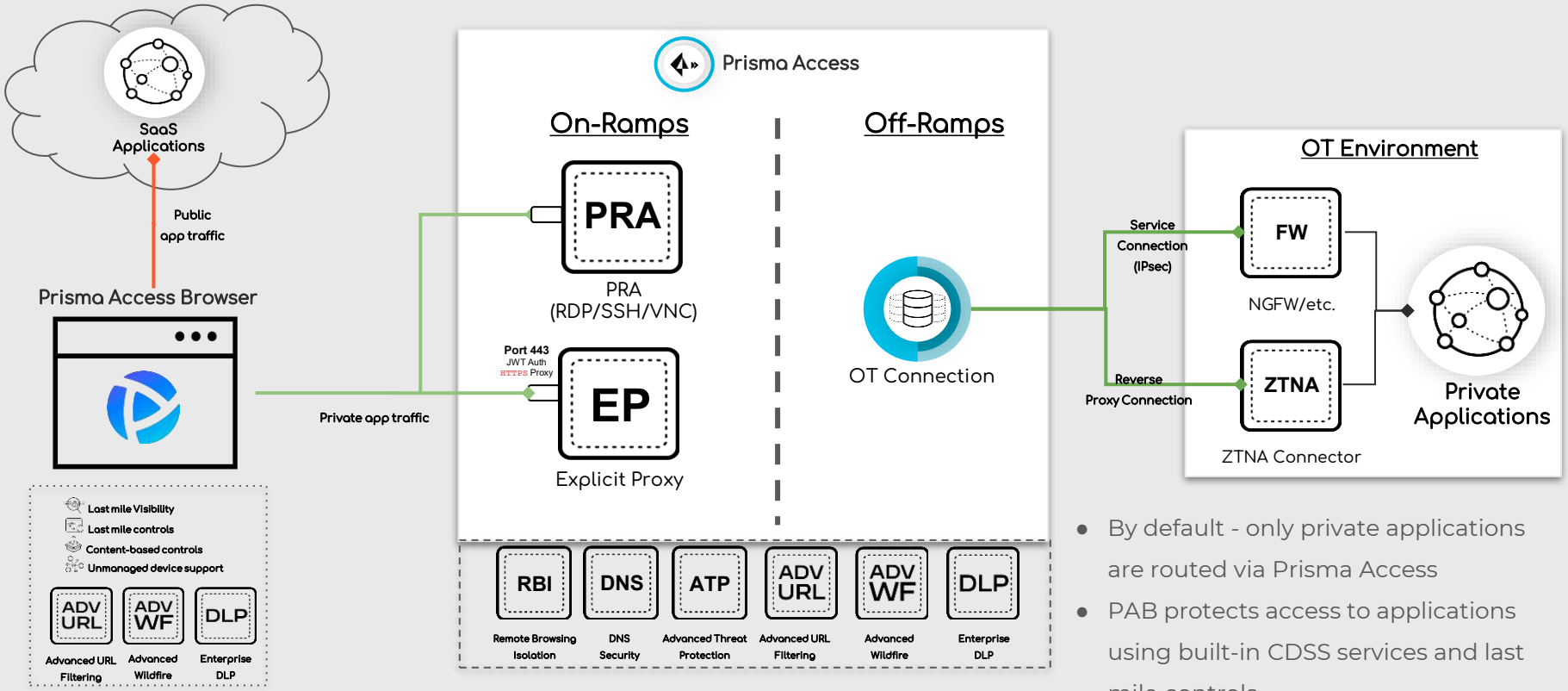
Security Posture & Last Mile Control for Unmanaged Assets

Eliminate VDI and Jump Servers within the OT Environment

No Local Admin or VPN Client Installation

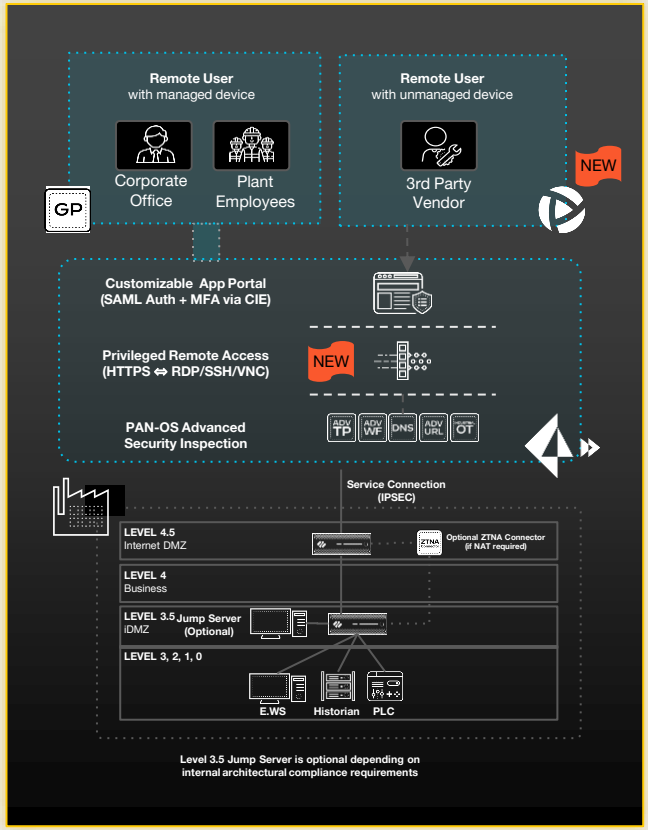
*** Not all features are generally available at launch

Understanding the Technical Architecture



- By default - only private applications are routed via Prisma Access
- PAB protects access to applications using built-in CDSS services and last mile controls

OT PRA Design Considerations



Clientless Endpoint

- Any modern browser, nothing to additional to install
- PRA portal and policy provides enforcement
- No last mile control or posture assessment
- Minimal browser enforcement features (e.g. watermarks)

Secure Browser (PAB)

- Install secure browser on any device, no admin privileges required
- Collects insights from browser for threat hunting & forensics
- Last mile posture, identity and privilege access for all apps
- MFA and JIT authorization workflows
- Customizable security features and enforcement (e.g. watermarks)

Service Connection

- For larger sites with many devices and applications
- Dedicated IPSec Tunnel for maximum performance

ZTNA

- Simple deployment for smaller sites
- Call home connectivity (inside-out)
- Policies enforced from Prisma Access

PAB Features for OT Privilege Remote Access

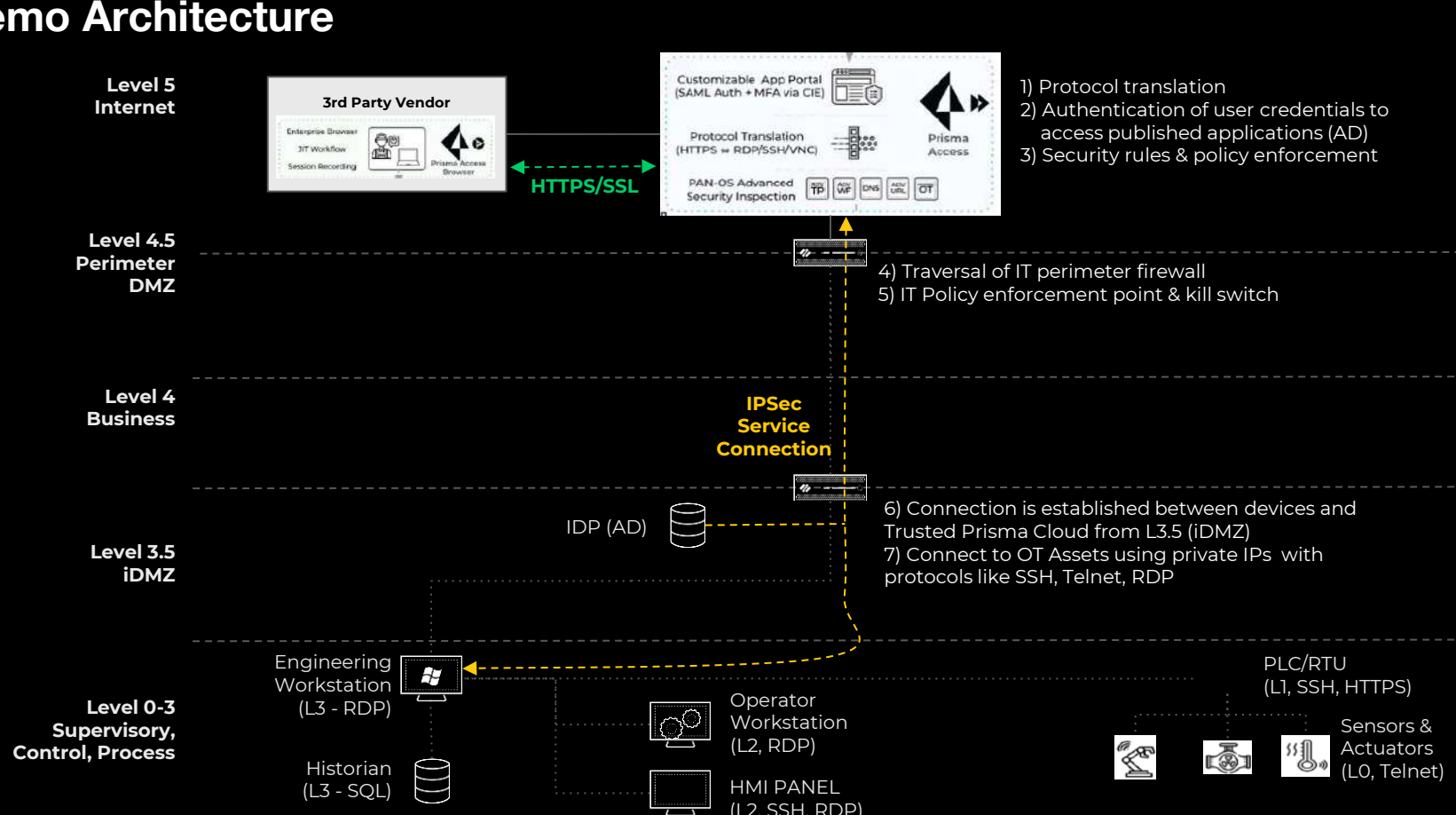
Secure Environment		Last-Mile Data and Identity Controls		User-First Workspace	
Device isolation	Advanced URL filtering	>1K data classifiers	Watermarks	Private app access	
Keylogger protection	Multilayered anti-phishing	ML, OCR, EDM, IDM	Screenshot/Sharing control	SSH/RDP support	
Screen scrapers protection	Advanced malware prevention	Regulation profiles	Camera/Mic control	Sync across devices	Quick offboarding
Trusted certificate store	Advanced threat protection	Directional-based DLP	Login restrictions	App acceleration	User privacy
Network security and isolation	Extension visibility and protection	Any control on any app	Tenant restriction	Extension management	Productivity suite
Device posture	Audit trails	File protection	Password manager	Automated DEM	Integrated apps
Browser hardening	User timeline	Clipboard control	Step-up MFA	Enterprise branding	Deploy in minutes
Anti-tampering	Session recording	Typing guard	Passkeys	Internet Explorer mode	Zero infra changes
Attack surface reduction	Threat hunting and forensics	Data masking	Admin approval	Secure AI assistant	
Browser isolation	Shadow IT	Printing control	Just-in-time	SSO integration	

Cross-platform integrations: SIEM | SOAR | IdP | ZTNA | EDR | Threat intel | Asset management

Unique Zero Trust & Identity Concepts

Concept	Definition
Just-in-time (JIT) Identity Controls	In Zero Trust, JIT is the concept of enforcing principle of least privileges by only allowing sensitive actions to be done in a given time frame, usually with direct approval of an admin and an expiration of the privilege. In PAB, admin approval can be required for performing specified actions: 1. Access to website 2. Clipboard actions 3. File actions 4. Typing guard The approval can be under the following restrictions: 1. Warn but allow the user to proceed 2. Require a reason (for audit logging) 3. Require approval by an admin - approval request is sent and can be approved for a given time frame
Step-up MFA	Presenting MFA challenge to the user before critical actions, for example: 1. Accessing websites 2. Downloading files 3. Performing actions
Device posture	Status of software and security controls on the endpoint - used to determine if the endpoint complies with the organization\regulatory requirements and used as an indication on how secure the endpoint is
Typing guard	Preventing typing in of specific content in specific context - application, device, network, location
Login restrictions	Set of capabilities to restrict login to defined websites

Demo Architecture



Secure 5G Assets & 5G Networks

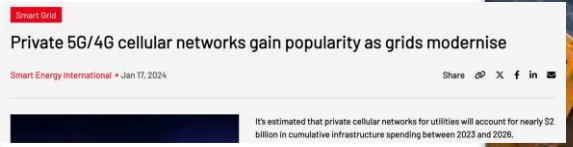
AGENDA

Secure 5G Assets & 5G Networks

1. Recap of Private Networks Solution Architecture
2. Current Capabilities 5G/IoT
3. Visibility and Security of devices behind 5G Wireless Gateways

GBM
paloalto NETWORKS | STRATA

The industry is moving towards Private Networks

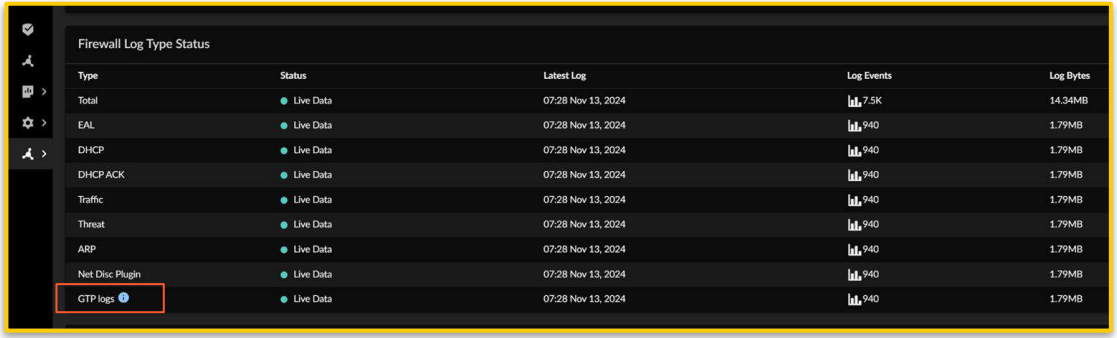


Telefonica Germany has implemented the world's first 5G mobile network for automobile production for Mercedes Benz, in "Factory 56" in Sindelfingen, covering an area over 20,000 m2

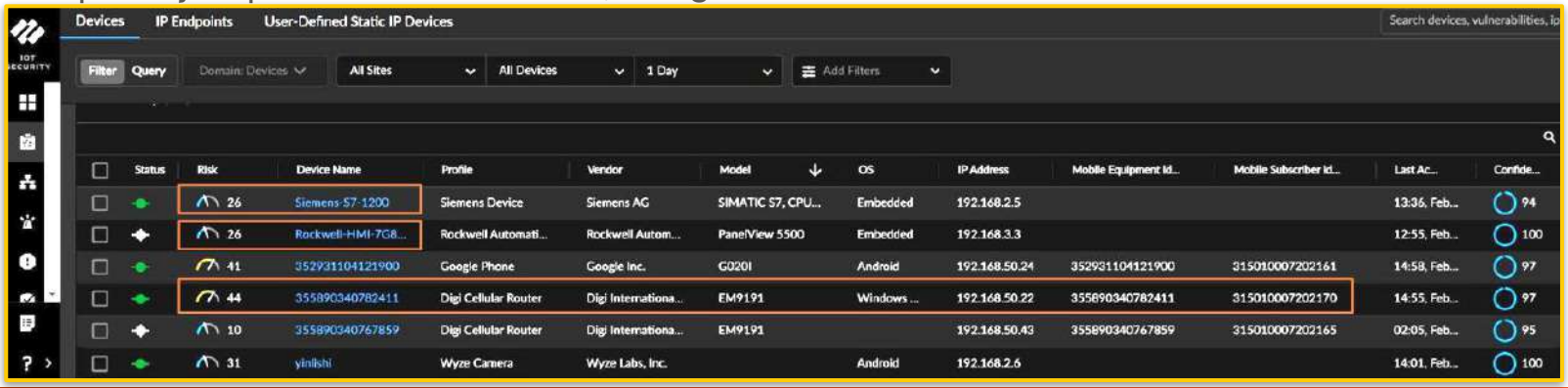
Container terminal operator Eurogate Terminals has recruited Deutsche Telekom to build private 5G networks at port terminals in Hamburg, Bremerhaven, and Wilhelmshaven in Germany

OT Asset Visibility - IoT and 5G devices in Single pane of glass

The NGFW sends the **GTP logs** that has the IMEI, IMSI, and IP correlation corresponding to the 5G device



IoT has the capability to profile the 5G devices, using the 5G mobile identifiers



OT Asset Visibility - Trusted 5G device identification details and traffic