Palo Alto Networks and Nozomi Networks

IIoT and Industrial Control System (ICS) Security

Until now, realizing comprehensive, real-time visibility into the heterogeneous environment of ICS networks, devices and process variables has been difficult. Without that contextual insight, industrial operations are challenged to protect the control network from cyberattacks and avoid production disruptions. Nozomi Networks innovative technology solves these challenges in a way that is non-intrusive and safe for ICS and SCADA (Supervisory Control and Data Acquisition) networks. By integrating Palo Alto Networks **NGFW (Next-Generation Firewall)** with Nozomi Networks SCADAguardian, joint customers can accelerate incident response and automate protective measures.

Highlights

Improve ICS cyber resiliency and provide real-time operational visibility with Nozomi Networks.

Accelerate incident response with automated actions to cyber threats with Palo Alto Networks.

Nozomi Networks

Nozomi Networks is a global ICS cybersecurity solutions company providing comprehensive asset visibility, network monitoring and cybersecurity detection for industrial networks.

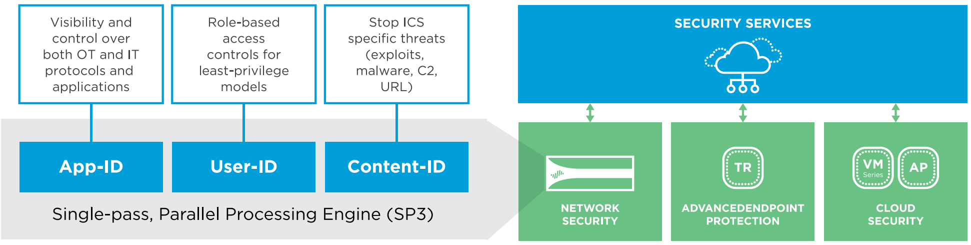
The Nozomi Networks solution set is comprised of a suite of application modules to visualize, monitor, detect and take remediation action against cyber threats when integrated with a firewall. It works in real-time to improve cyber resiliency and deliver consolidated OT (Operational Technology) visibility across SCADA networks, including multiple geo-separated plants.

Deploying non-intrusively, it automatically learns all assets within the host network, with no impact on control network latency, determinism or packet jitter. Once the learning phase is completed, the solution works in concert with the existing security infrastructure to automatically monitor and detect cyberattacks, cyber risks and process anomalies. When coupled with integration partner Palo Alto Networks, the joint solution extends IT/OT cybersecurity strategies to be more intelligent, protective and comprehensive.

Palo Alto Networks

Palo Alto Networks is leading a new era in cybersecurity serving more than 42,500 customers in 150+ countries by protecting thousands of enterprises, governments, service providers, and industrial networks from cyber threats.

Its Next-Generation Security Platform is comprised of the NGFW, Traps Advanced Endpoint Protection, VM-series and Aperture Cloud Security, and security services. It provides an integrated, multi-method approach focused on preventing attacks to OT across the entire attack lifecycle. The **NGFW**, with its innovative single-pass, parallel processing engine (SP3), provides granular traffic visibility even to ICS protocols, applications, and users. Plus, as the enforcing device, it allows users to segment their network using intuitive "layer-7" business policies that reduce the attack footprint.


Visibility and control over both OT and IT protocols and applications
Role-based access controls for least-privilege models
Stop ICS specific threats (exploits, malware, C2, URL)
App-ID
User-ID
Content-ID
Single-pass, Parallel Processing Engine (SP3)
SECURITY SERVICES
NETWORK SECURITY
TR
ADVANCEDENDPOINT PROTECTION
VM Series
AP
CLOUD SECURITY

Next-generation Firewall Layer-7 Classification Engine

Palo Alto Networks Security Platform

The App-ID component of the SP3 engine gives users the ability to enforce policies based on a set of standards-based ICS protocols such as Modbus, DNP3 and IEC-60870-5-104 and vendor-specific ICS protocols such as Siemens S7, Honeywell/Matrikon OPC Tunneller, and OSIsoft Pi. Through User-ID, organizations can easily realize role-based access controls where relevant within their OT.

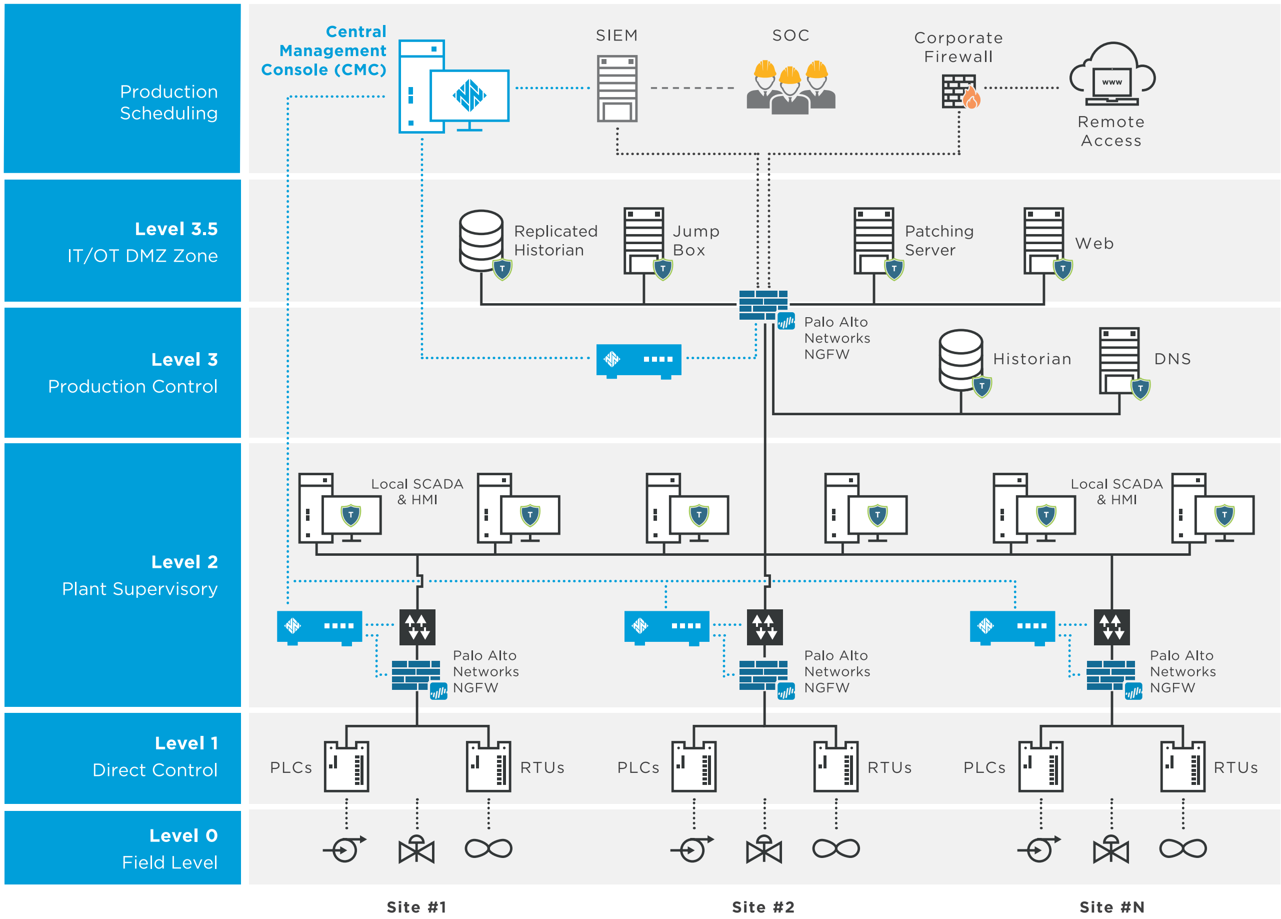
The Threat Prevention service works with Content-ID to further secure the allowed traffic by natively blocking known threats to both IT and OT including ICS-specific exploits, malware, and associated command and control (C2) traffic. This helps organizations protect their currently unpatched or unpatchable systems until they can be updated or replaced. For more sophisticated unknown threats, the Wildfire service quickly analyzes files to determine their malicious/benign nature then quickly send protections back to the firewall to prevent malware propagation and C2 communications.

The NGFW runs the PANOS operating system which includes a powerful XML-based API which can be used to access and manage the firewall through a third-party service, application, or script. This allows for the realization of closed-loop and fully automated OT threat detection and response.

Palo Alto Networks with Nozomi Networks

Palo Alto Networks and Nozomi Networks have integrated their technologies to offer enterprise and industrial cybersecurity stakeholders a scalable cybersecurity solution that seamlessly bridges the gap between IT and OT operations.

With the Palo Alto Networks API and the Nozomi Networks Open API, both solutions are able to work in concert to extend threat detection and remediation actions beyond what was once possible. In addition, both Palo Alto Networks and Nozomi Networks offer powerful threat hunting capabilities using rule-based signature analysis, allowing customers to extend policy enforcement proactively. With the Palo Alto Networks / Nozomi Networks integration, customers can reliably use Palo Alto Networks Next-Generation Security Platform with added benefits gained from SCADAguardian's hybrid ICS threat detection and Dynamic Learning capabilities.



Sample Palo Alto Networks / Nozomi Networks Deployment Architecture

Use Cases

Power Substation - Malware is used to reprogram a Programmable Logic Controller (PLC) or Remote Terminal Unit (RTU) utilizing an approved protocol.

A node inside a highly-trusted subnet (the Process Network, governing the Control Network) tries to perform an anomalous, and perhaps malicious, action in the form of a permissible command, for example, reprogramming a PLC. Using different backdoors, the malware beacons out to an external C2 server, and initiates an attack using an DNP3 payload.

Attack vector: Unauthorized personnel, social engineering, tailored malware installed during system updates.

Details: Two known machines in two different network segments start to communicate utilizing a previously unseen protocol or application. For example, malware is injected onto a SCADA (Supervisory Control and Data Acquisition) machine and is able to read state conditions / context and send commands. This machine is now trying to reprogram the PLC or RTU in a malicious or anomalous manner.

Solution: Integration between Nozomi Networks and Palo Alto Networks solutions enables the organization to take automated action to limit DNP3 protocol access to 'read only' status in response to the misbehaving, albeit trusted, SCADA asset. First, the malware is immediately recognized using rule-based analysis. If the malware is a new version, not yet accounted for within a rule, SCADAguardian's behavior-based anomalous activity recognition capability will discover the malware's commands. It will also coordinate with Palo Alto Networks NGFW to flag, remediate and block the attack. If this incident were merely a policy violation, DNP3 protocol access may remain limited, allowing for the monitoring function, but not control access.

Coupling the Nozomi Networks API and the user ID function within the Palo Alto Networks NGFW, administrators can apply user ID to limit or block suspicious users.

Process Manufacturing / Oil and Gas - An unrecognized device is discovered and starts communicating.

In this scenario an unknown node belonging to a trusted subnet is completely isolated from control within the extensive DCS (Distributed Control System) network.

Attack vector: Unauthorized personnel, social engineering, brownfield system integration error, and tailored malware installed during system updates.

Details: A machine plugs into the LAN and starts to communicate with another machine in another network segment. Since it's a new source node, the operator wants to block any communication originating from it. Moreover, no other machines should connect to this one. The operator does not know how long the node has been there, its manufacturer nor why it was deployed.

Solution: Integration between Nozomi Networks and Palo Alto Networks enables the organization to discover the device immediately, examine the details of the devices and take automated remediation actions via the NGFW. This includes blocking the IP address and examining it for malicious intent and level of risk. Moreover, this scenario can be incorporated into a standard operational approach for future scenarios.

Use Cases

Discrete Manufacturing - A Human-Machine Interface (HMI) malware tries to adjust a Programmable Logic Controller (PLC).

A node inside a highly-trusted subnet (the Process Network, governing the Control Network) tries to perform an anomalous and perhaps malicious action in the form of a permissible command (e.g. reprogramming a PLC.)

Attack vector: Unauthorized personnel, social engineering, tailored malware installed during system updates.

Details: Two known machines in two different network segments start to communicate with a previously unseen protocol/application. In one case the malware is injected onto a MES (Manufacturing Execution System) application or SCADA, allowing it to read state and send commands in order to reprogram the PLC itself. This could be an act of corporate espionage or sabotage.

Solution: Integration between Nozomi Networks and Palo Alto Networks enables the organization to discover this attack before it is able to gain full access to PLCs or extract manufacturing intelligence. SCADAguardian identifies the attack, alerts and initiates an automated action against the NGFW to block the IP address using Palo Alto Network's firewall and then takes PCAPs of the incident.

Additional Resources

Nozomi Networks SCADAguardian Solution Brief

DOWNLOAD

Nozomi Networks SCADAguardian Data Sheet

DOWNLOAD

Palo Alto Networks Next-Generation Firewall

LEARN MORE

About Palo Alto Networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyber threat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at *www.paloaltonetworks.com*

About Nozomi Networks

Nozomi Networks is revolutionizing Industrial Control System (ICS) cybersecurity with the most comprehensive platform to deliver real-time cybersecurity and operational visibility. Since 2013 the company has innovated the use of machine learning and artificial intelligence to secure critical infrastructure operations. Amid escalating threats targeting ICS, Nozomi Networks delivers one solution with real-time ICS monitoring, hybrid threat detection, process anomaly detection, industrial network visualization, asset inventory, and vulnerability assessment. Deployed in the world's largest industrial installations, customers benefit from advanced cybersecurity, improved operational reliability and enhanced IT/OT integration. Nozomi Networks is headquartered in San Francisco, California. Visit *www.nozominetworks.com*

NOZOMI NETWORKS

www.nozominetworks.com

@nozominetworks