Palo Alto Networks ML-Powered Next-Generation Firewall and Nozomi Networks Guardian

Securing Industrial Control System (ICS) and Internet of Things (IoT)

Benefits of the Integration
- Improve ICS cyber resiliency and provide real-time operational visibility with Nozomi Networks.
- Accelerate incident response with automated actions to cyberthreats with Palo Alto Networks NGFW.
- Extend Guardian’s passive monitoring and detection to automated enforcement through the integration with Palo Alto Networks NGFW.
- Simplify management of node and link blocking policies via removing blocked nodes and links through the Guardian graphical network maps and tables.

The Challenge
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) system networks. By integrating the Palo Alto Networks ML-Powered Next-Generation Firewall (NGFW) with Nozomi Networks Guardian®, joint customers can accelerate incident response and automate protective measures.

Nozomi Networks Guardian
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 consists of a suite of application modules to visualize, monitor, detect, and take remediation action against cyberthreats when integrated with a firewall. It works in real time to improve cyber resiliency and deliver consolidated operational technology (OT) 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.

Palo Alto Networks Next-Generation Firewalls
Palo Alto Networks Next-Generation Firewalls offer a prevention-focused architecture that is easy to deploy and operate. Palo Alto Networks NGFWs inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere. The user, application, and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies and write rules that are easy to understand and maintain.

Palo Alto Networks and Nozomi Networks
Palo Alto Networks and Nozomi Networks have integrated their technologies to offer enterprise and industrial cybersecurity stakeholders an intelligent, proactive, and 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 can 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 and Nozomi Networks integration, customers can reliably use Palo Alto Networks Next-Generation Security Platform with added benefits gained from Guardian’s hybrid ICS threat detection and dynamic learning capabilities.
Use Case 1: Power Substation
Malware is used to reprogram a Programmable Logic Controller (PLC) or Remote Terminal Unit (RTU) utilizing an approved protocol.

Challenge
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 a DNP3 payload.

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, Guardian’s behavior-based anomalous activity recognition capability will discover the malware’s commands. It will also coordinate with the Palo Alto Networks NGFW to flag, remediate, and block the attack. If this incident were merely a policy violation, DNP3 protocol access might remain limited, allowing for the monitoring function but not control access.

Use Case 2: Process Manufacturing/Oil and Gas
An unrecognized device is discovered and stays communicating.

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

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 Case 3: Discrete Manufacturing/Oil and Gas

A Human-Machine Interface (HMI) malware tries to adjust a PLC.

Challenge
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.).

Solution
Integration between Nozomi Networks and Palo Alto Networks enables the organization to discover this attack before it can gain full access to PLCs or extract manufacturing intelligence. Guardian identifies the attack, alerts, and initiates an automated action against the NGFW to block the IP address using a Palo Alto Networks Firewall and then takes packet captures (PCAPs) of the incident.

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. Deployed in the world’s largest industrial installations, customers benefit from advanced cybersecurity, improved operational reliability and enhanced IT/OT integration. Visit www.nozominetworks.com.

About Palo Alto Networks
Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.