Quantum IoT Embedded Nano Agent

Securing the Industrial Edge

Regulations

- **IEC 62443** (Series of standards for secure design and operation)
- **SANS 20** (List of 20 security controls)
- **NIST 800-82 (**ICS guidelines**)**
- **DPA** (Data Protection Act)
- **UK GDPR** (General Data Protection Regulation)
- **NIS** & **NIS2** (Network and Information Security)
- **NERC CIP** (North America's requirements for electric systems)
- **NEI 08-09**, **CFATS** and much more

THE COMPLEXITY OF ENHANCING ICS SECURITY

Operational technology (OT) environments face unique challenges when it comes to enhancing the security of Industrial Control Systems (ICS). The need to ensure uninterrupted service, maintain data integrity, comply with regulations and protect public safety requires proactive security controls to secure these mission-critical processes and assets.

COUNTERING THE RISING THREATS TO INDUSTRIAL INFRASTRUCTURE

The industrial attack surface is expanding rapidly and the threat landscape is growing massively. The industrial attack surface is growing for several reasons, the involvement of nation-state actors, advancements in technology and the convergence of IT and OT (Operational Technology). To combat these evolving threats, a comprehensive security solution with a proactive strategy is needed. This approach aims to eliminate risks by effectively blocking threats before they can impact critical assets. This will seamlessly enhance industrial operations.

REVOLUTIONIZING RESILIENCE, THE NANO AGENT

Check Point's Nano Agent is specifically crafted to harden devices through on-device runtime protection, effectively preventing zero-day attacks. Once installed, it monitors the inputs, outputs and overall status of the mission-critical device and it's processes. Its primary objective is to identify both known and unknown attack patterns and unusual behaviours that might signify an exploit targeting a zero-day vulnerability. Should it detect such an attack, the Nano Agent will block the attack and alert the organization's security team. The Nano Agent can be incorporated on various OT devices running Linux, think of field devices, intelligent assets, SCADA controls systems, PLC, RTU, HMI, industrial gateways and more.

ICS SECURITY AT SCALE WITH THE BENEFITS OF A CLOUDBASED MANAGEMENT

With the Infinity portal, you can effectively manage the security of OT, IIoT and IoT mission-critical assets from the cloud. Utilizing the Management API, administrators can define and enforce security settings of the Nano Agent. The Open Management API, available on swagger.io, supports both internet-connected devices and those in air-gapped environments. This allows administrators to have a complete oversight of the IoT device communication, ensuring both inbound and outbound data transmission is secured. Administrators can also establish and enforce security practices for devices protected by the Nano Agent, further enhancing their protection. Offering a robust security posture, ensuring comprehensive protection across the entire device fleet. Additionally, the Infinity portal offers full reporting, logging and alerting capabilities, enabling administrators to stay informed about security incidents.

THE POWER OF ZERO TOLERANCE

The incorporation of the Nano Agent offer benefits like:

- **Runtime Protection |** Detecting and protecting vulnerabilities during the active use of devices in production environments and any deployment scenario. This ensures the capability to safeguard against potential exploitation of vulnerabilities.
- **Zero-Day Protection |** The Nano Agent constantly monitors for abnormal inputs, outputs, and device behavior that may indicate a potential attack. It doesn't depend on signature-based methods for detecting exploits. This

Author: Antoinette Hodes

allows it to offer efficient protection, even in deployment scenarios where updates and patching are rare or not feasible.

- **No Dependency on Source Code |** The Nano Agent functions as a wrapper around a binary executable, eliminating the need for access to the source code. This empowers consumers and organizations to implement device-level protection against cyber-attacks without requiring the source code.
- **Complete Firmware Coverage |** The Nano Agent security provides comprehensive firmware coverage for supported platforms, such as Linux over ARM32/ARM64. This coverage extends to all third-party components as well, ensuring robust protection across the entire firmware ecosystem.
- **Device Agnostic |** The security design is device-agnostic. Due to this design, it is compatible with a wide range of devices across various deployment environments.
- **Open Management API |** Being a device-agnostic solution, Nano Agent incorporates an open management application programming interface (API) to facilitate seamless integration with DevOps continuous deployment and integration practices. This API enables efficient management and control of the solution, aligning with modern development methodologies.
- **Minimal Impact on Device Performance |** The Nano Agent software agents are specifically designed to have minimal impact on device performance. This includes utilizing less than 10% of CPU and memory resources, as well as requiring only 1-50 MB of storage (depending on the deployed security policies). This small footprint and low resource requirements make Nano Agent security suitable for resource-constrained environments, such as OT environments.
- **Consolidated Management, Visibility, and Logging (Optional) |** Nano Agent offers seamless integrations with Check Point Infinity, enabling users to benefit from consolidated management, visibility and logging capabilities for OT devices across different deployment scenarios. However, the Nano Agent can also operate in standalone mode, making it suitable for isolated environments with no network or Internet connectivity.
- **Comply with Legislative Acts |** Nano Agent is addressing key elements in legislative acts. In addition, it reduces cost.

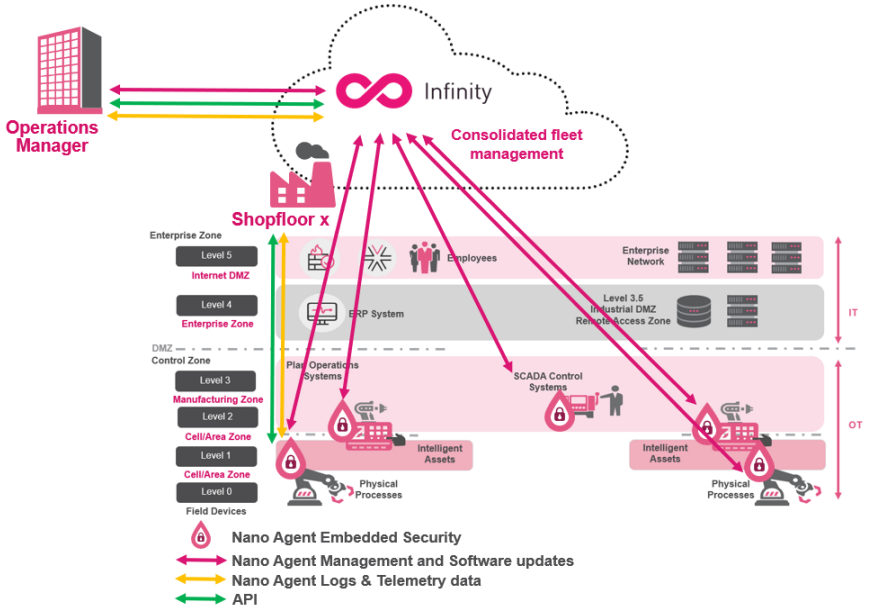

Figure 1: Nano Agent deployment overview, mapped on the Purdue model.

ICS environments are challenged by the growing attack surface and exposed to a rapidly evolving threat landscape. All OT assets must be secured with appropriate security controls. By addressing the “Zero Tolerance” principle, OT operators don’t have to worry about the lack of administrative resources on remote locations, patching and/or upgrades. Check Point Nano Agent enforces access control, prevent attacks, threats and critical data, with a minimal footprint. Making sure mission critical assets keeps on working without downtime. The Nano Agent will allow OT environments to comply with key elements in regulations. Read more about how to use Nano Agent to addresses these challenges with the best **ROI** (Return on Investment) and a low **TCO** (Total Cost of Ownership).