industrial internet CONSORTIUM

Endpoint Security Best Practices

Executive Overview

WHY SECURITY BEGINS AT THE END

When securing industrial systems and applications, the first line of defense lies at the end: Endpoints. Endpoints represent key vulnerable points of entry for cybercriminals. This is where attackers exploit vulnerabilities, execute code and where there are assets to be encrypted. For decades, organizations have heavily relied on antivirus as a means to secure endpoints. As more enterprises adopt practices such as BYOD, workforces become more mobile and users connect to internal resources all over the world, endpoint security requires more than detection and response. It requires changing the security paradigm from detecting to preventing.

Security Levels

Endpoint security comprises the entire strategy and technology stack required to protect endpoints from threats and attacks. Endpoint protection supplements a centralized security framework with an additional layer of protection at points of egress. A thorough understanding of where vulnerabilities lie within your industrial system is crucial in addressing the architectural considerations required to protect and secure endpoints. Each endpoint should have an appropriate level of security.

The IIC Endpoint Security Best Practices white paper defines three levels of

ENDPOINT (Noun)

The IIC Vocabulary Technical Report defines an endpoint as a "component that has computational capabilities and network connectivity". Thus, endpoints may include edge devices (e.g., embedded medical devices, sensors and actuators in vehicle controls systems as well as pumps, heaters and flow meters in manufacturing systems), communications infrastructure, cloud servers or anything in between.

GUIDANCE AND COMPLIANCE FRAMEWORKS

The Endpoint Security Best Practices document distills existing industrial guidance and compliance frameworks documents down to the essentials (12 pages) with extensive footnotes so readers can find more details about topics that interest them within the source documents.

The security levels defined in the Endpoint Security Best Practices Document correspond to security levels 2, 3 and 4 as defined in IEC 62443 3-3.

IEC 62443, formerly known as ISA 99, is the global standard for the security of Industrial Control System (ICS) networks and helps organizations to reduce both the risk of failure and exposure of ICS networks to cyber threats. One could read these source documents for the industry standards IEC 62443 and NIST SP 800-53*, but that would require reading thousands of pages – much of which is not applicable for today's industrial internet environments.

security: basic, enhanced and critical. These levels correspond to some of the most mature of the industrial guidance and compliance frameworks (see Guidance and Compliance Frameworks sidebar).

1. ***Security Level Basic*** (SLB) provides protection against "intentional violation using simple means with low resources", such as an ordinary virus.
2. ***Security Level Enhanced*** (SLE) steps up to defend against "sophisticated means with moderate resources", such as exploiting known vulnerabilities in Industrial Control System (ICS) software or systems.
3. ***Security Level Critical*** (SLC) steps up further to defend against attackers with "sophisticated means with extended resources", such as the ability to develop custom zero-day attacks.

There are full-stack architectures for endpoint security offering increasing security levels. These are based on open standards and interoperability between multi-vendor multi-platform endpoints across architectural patterns such as three-tier, gateway-mediated edge or layered databus. Regardless of the architectural pattern employed, the endpoints must include resistance to attacks commensurate with the level of risk for those endpoints. Within the Endpoint Security Best Practices white paper, key elements and countermeasures selected for the three security levels defined are identified and discussed in detail.

ENDPOINT SECURITY BEST PRACTICES:
ELEMENTS DISCUSSED IN DETAIL

- ROOT OF TRUST
- SECURE BOOT
- CRYPTOGRAPHIC SERVICES
- ENDPOINT CONFIGURATION & MANAGEMENT
- SECURE COMMUNICATIONS
- CONTINUOUS MONITORING
- POLICY ACTIVITY & DASHBOARD
- SYSTEM INFORMATION & EVENT MANAGEMENT

Protecting Industrial IoT System

By applying Endpoint Security Best Practices, owners and operators can specify which security level they need. Insurers and policy makers may benefit from a common benchmark that can be used to analyze risk and encourage security improvements. Equipment manufacturers can build products that provide necessary security features efficiently. Governments can drive adoption of best practices for industrial security.

Success begins with laying a foundation. Start by securing endpoints. The IIC's Industrial Internet Security Framework and Endpoint Security Best Practices white paper provide the guidance to secure IIoT systems.

The Industrial Internet Security Framework *"Best Practices" Documents*

The IIoT is being shaped by many participants from the energy, healthcare, manufacturing, industrial transport systems and public sectors, each of which needs to consider security. To avoid security hazards, especially as systems from different sectors interoperate and exploitation attempts are made in the gaps between them, it is important and urgent to build early consensus among the participants on IIoT security.

The Industrial Internet Security Framework (IISF) Technical Document guides systems designers, integrators and security architects as they ensure security is a fundamental part of the new or existing IIoT architectures, rather than "bolted on" to it.

IIC Best Practices Documents cover aspects of industrial internet security, based on the six building blocks in the IISF. The IISF provides a secure design architecture for industrial internet security so that system designers can understand overall security architecture and context. For example, equipment manufacturers and integrators can define which security level their products, systems and solutions are designed to meet. Insurers and policy makers may benefit by having a common benchmark that can be used to analyze risk and encourage security improvements. All can benefit by obtaining a clear description of what countermeasures and controls are generally recommended for each level of security.

➢ Return to IIC Journal of Innovation landing page for more articles and past editions.

* Standards development organizations are most commonly known by their acronyms. These include International Standards Organization (ISO), Institute of Electrical and Electronic Engineers (IEEE), International Electrotechnical Commission (IEC), Internet Engineering Task Force (IETF) or National Institute for Standards and Technology (NIST).

The views expressed in the *IIC Journal of Innovation* are the contributing authors' views and do not necessarily represent the views of their respective employers nor those of the Industrial Internet Consortium.