CIRRO

Managed OT Security with Industrial Defender

Service Name

Private Cloud–Hosted Industrial Defender Software-as-a-Service (SaaS)

OT Cyber Security - Baseline Health Check

Taxonomy	
F-205-302-000	Private Cloud–Hosted Industrial Defender Software-as-a-Service (SaaS) OT Cyber Security - Baseline Health Check
F-205-303-000	
F-205-304-000	

Service Overview

As the worlds of IT and OT merge, OT assets are at greater risk than ever of cyber security attacks. Identify OT assets, even non-networked ones, and build a risk picture. Protect Critical Infrastructure and Industrial Operations with Risk-Based Vulnerability Management for OTIntegrating Wasabi

Industrial Defender – *The* leading player in Industrial OT Cyber Security

Industrial Defender is a purpose-built cybersecurity and compliance platform designed to protect industrial control systems (ICS), operational technology (OT), and critical infrastructure environments. It provides organisations with the visibility, governance, and risk management capabilities required to secure complex industrial operations while maintaining safety, reliability, and regulatory compliance.

At its core, Industrial Defender delivers a comprehensive system of record for OT environments. It enables organisations to maintain accurate inventories of industrial assets, configurations, firmware, and software versions, forming the foundation for effective risk and vulnerability management. By contextualising vulnerabilities within industrial environments, Industrial Defender helps security and operations teams prioritise remediation based on operational risk rather than IT-centric scoring alone.

The platform also supports robust compliance and governance capabilities, mapping technical and procedural controls to industry standards such as IEC 62443, NERC CIP, NIST, and ISO frameworks. Built-in workflows support incident management, change management, risk acceptance, and audit evidence collection, improving accountability and traceability across OT security programs.

Industrial Defender's offerings can be deployed on-premises or delivered as a managed or private cloud–hosted service, providing flexibility to meet regulatory, operational, and data residency requirements. Together, these capabilities enable organisations to strengthen their OT security posture, streamline compliance, and improve resilience across critical industrial operations.

Industrial Defender´s Platform

The platform acts as a system of record for OT environments, consolidating asset inventories, system configurations, firmware levels, and software versions into a single authoritative view. This foundational visibility enables effective vulnerability management by allowing organisations to understand exposure in the context of operational criticality, safety impact, and regulatory obligations.

Industrial Defender integrates policy, risk, incident, and change management workflows tailored for industrial operations. These capabilities support structured governance processes, enabling organisations to manage exceptions, track remediation activities, and maintain audit-ready evidence aligned to standards such as IEC 62443, NERC CIP, NIST, and ISO frameworks.

Designed with availability and safety in mind, the platform supports secure integration with industrial networks without disrupting operations. Flexible deployment options—including on-premises, private cloud, and managed service models—allow organisations to align the platform with regulatory, data residency, and operational requirements. Together, these capabilities enable consistent, scalable, and defensible OT cybersecurity and compliance management.

Private Cloud–Hosted Industrial Defender Software-as-a-Service (SaaS)

Overview

Our Private Cloud–Hosted Industrial Defender Software-as-a-Service (SaaS) offering delivers the full power of Industrial Defender's cybersecurity and compliance platform within a dedicated, securely isolated private cloud environment. Designed specifically for industrial, operational technology (OT), and critical infrastructure organisations, this service combines enterprise-grade security, regulatory compliance, and operational resilience with the flexibility and scalability of a managed SaaS model.

This service enables organisations to reduce the complexity and cost of deploying and maintaining Industrial Defender infrastructure on-premises, while retaining the control, data ownership, and security assurances required for high-risk industrial environments. The result is a robust, compliant, and operationally aligned cybersecurity platform delivered as a fully managed service.

Purpose-Built for Industrial and OT Environments

Industrial Defender is purpose-built for OT, ICS, and industrial control environments where availability, safety, and regulatory compliance are paramount. Our private cloud SaaS deployment preserves these principles while extending them with modern cloud operational practices.

The service supports a wide range of industrial sectors, including energy, utilities, manufacturing, oil and gas, transportation, pharmaceuticals, and other safety-critical industries. It is designed to align with standards and frameworks such as IEC 62443, NERC CIP, NIST CSF, ISO 27001, and other industry-specific regulatory requirements.

Private Cloud Architecture

Unlike public multi-tenant SaaS offerings, this service is hosted within a dedicated private cloud environment, logically and operationally isolated for each customer or customer group.

Core Service Capabilities

The service provides the full Industrial Defender platform as a managed SaaS solution, including asset management, vulnerability management, compliance tracking, incident management, and reporting.

Fully Managed Service Model

This offering is delivered as a fully managed SaaS service, removing the burden of infrastructure management from the customer.

Security and Compliance by Design

Security is embedded at every layer of the service, including encryption, access control, monitoring, and audit support.

Data Ownership and Residency

Customers retain full ownership of their data at all times, with clear contractual commitments governing data handling.

Availability and Resilience

The service is architected for high availability and resilience with defined SLAs.

Support and Service Management

Customers receive enterprise-grade support delivered by OT cybersecurity specialists.

Conclusion

Our Private Cloud–Hosted Industrial Defender SaaS service delivers a secure, compliant, and operationally aligned approach to OT cybersecurity and compliance management.

OT Cyber Security - Baseline Health Check

The Baseline Health Check proposition for Operational Technology (OT) environments and the Industrial Defender platform provides organisations with a structured, low-risk assessment of their current OT cybersecurity posture and platform effectiveness. It is designed to establish a clear and defensible baseline from which security improvements, compliance activities, and risk reduction initiatives can be planned and prioritised.

The engagement begins with a focused review of the OT environment and the existing Industrial Defender deployment, including asset inventories, system configurations, vulnerability data, policies, and workflows. This assessment validates the accuracy, completeness, and currency of data within Industrial Defender, ensuring the platform is operating as an effective system of record for OT security and governance.

The health check evaluates alignment with recognised standards and regulatory frameworks such as IEC 62443, NIST CSF, and relevant sector-specific requirements. Particular attention is given to asset visibility, vulnerability and risk management processes, change and incident management workflows, and evidence collection for audit readiness. Gaps, inconsistencies, and areas of elevated risk are identified and contextualised against operational criticality and safety considerations.

In parallel, the proposition assesses the technical health of the Industrial Defender platform itself, including configuration, access controls, data integrations, reporting, and operational usage. This ensures the platform is optimally configured to support both security and compliance objectives.

The outcome is a concise, actionable report providing a clear baseline view of OT cyber maturity and Industrial Defender effectiveness. It includes prioritised recommendations, quick-win improvements, and a practical roadmap to enhance security posture, compliance assurance, and long-term value from the Industrial Defender investment.