

# OT Security at the Core of Enterprise Resilience

Empowering and securing enterprises  
through HCLTech and Armis' Unified  
cybersecurity expertise



# Overview

In today's rapidly evolving digital landscape, Operational Technology (OT) environments are the backbone of critical industries such as manufacturing, energy, healthcare, transportation and utilities. However, as OT systems become more integrated with IT networks to drive efficiency and innovation, the attack surface for cyber threats has expanded significantly. Traditional security approaches alone cannot adequately protect these highly specialized systems, which are often vulnerable due to reliance on legacy architecture and minimal downtime tolerances.

To address these critical challenges, HCLTech and Armis have partnered to offer an advanced and holistic OT security solution. Combining HCLTech's expertise in digital transformation and managed services with Armis's agentless, AI-powered asset visibility and security solutions, this collaboration provides comprehensive visibility, proactive threat detection and real-time protection for OT environments. Together, we empower organizations to secure their OT assets while ensuring operational resilience and uninterrupted productivity.

## Challenges

OT environments face unique challenges that make them increasingly susceptible to cyber threats. These challenges include:

**Convergence of IT and OT:** As organizations integrate OT and IT systems for improved operational efficiency and data sharing, cyber threats initially targeting IT environments are now beginning to exploit OT vulnerabilities. IT-OT convergence creates new attack vectors that require specialized security strategies.

**Operational constraints:** Ensuring cybersecurity in OT environments is incredibly complex due to strict uptime requirements. Any disruption to OT processes during security implementation or monitoring could result in financial losses, downtime or even safety incidents.

**Sophisticated cyber threats:** Cyber attackers leverage advanced tactics, such as ransomware targeting Industrial Control Systems (ICS), supply chain compromise and zero-day vulnerabilities. OT-specific threats can cause physical disruptions, data breaches, reputational damage and regulatory compliance failures.

**Legacy infrastructure:** Many industries rely on legacy OT equipment designed without cybersecurity in mind. These systems often lack updates, patches and modern security features, making them easier targets for attackers.

**IoT device proliferation:** As organizations increasingly adopt connected IoT devices to enhance operations, the sheer scale of unmanaged, untracked assets continues to grow exponentially. This lack of device visibility creates blind spots that attackers can exploit.

**Regulatory and compliance pressures:** Stringent industry regulations require organizations to prioritize OT system reliability, integrity and security. Non-compliance could lead to penalties, reputational damage or loss of market access.



# Our Solution

The HCLTech-Armis joint OT Security solution provides a robust and forward-looking approach to protecting, monitoring and managing OT environments. Our solution is tailored to meet the specialized needs of OT ecosystems without compromising operational efficiency and uptime.

## **Holistic visibility across OT and IoT assets:**

Armis's agentless AI-powered platform is the cornerstone of our offering. It provides 100% visibility into all assets across OT, IoT, IT and ICS environments. By delivering real-time asset inventory, organizations can identify all connected devices—including managed, unmanaged and rogue assets—and classify them in granular detail.

## **Proactive threat detection:**

Our solution leverages Armis's behavioral threat detection capabilities, powered by machine learning and contextual intelligence. The platform continuously monitors device interactions to identify anomalous activity indicative of cyber threats such as ransomware, phishing, insider risks or supply chain attacks.

## **Non-disruptive security management:**

Understanding the criticality of uptime, our solution operates non-intrusively, ensuring 24/7 operational continuity. With agentless monitoring and passive security deployment, organizations can secure their OT environments without risking productivity downtime.

## **Vulnerability management and risk profiling:**

Through constant assessment of vulnerabilities across devices, firmware and protocols, our solution provides actionable insights to mitigate risks before attackers can exploit them. Our risk profiling capabilities help organizations prioritize responses based on criticality and impact.

HCLTech enhances the Armis platform with complementary services, including **Universal Managed Detection and Response (UMDR)**, bespoke threat modeling, compliance assessments and incident response capabilities. This comprehensive approach ensures end-to-end protection for OT-centric industries. Our scalable solution enables enterprises to align their cybersecurity measures with evolving risks and regulations dynamically.



# Value delivered

By combining HCLTech's strategic expertise and operational excellence with Armis's state-of-the-art platform, our joint OT Security offering delivers quantifiable value across several dimensions:



**Complete asset visibility for risk reduction:** Organizations benefit from full-spectrum visibility into all assets connected across their IT-OT-IoT environments. By eliminating blind spots, businesses can proactively secure endpoints, identify rogue devices and minimize the likelihood of successful cyberattacks.



**Improved operational resilience:** Our solution's agentless and non-intrusive nature ensures organizations can deploy advanced cybersecurity measures without impacting uptime, productivity or process reliability. This boosts operational efficiency while safeguarding business continuity.



**Strengthened threat detection:** Our real-time threat detection capabilities empower organizations to stop cyber threats at the earliest stage. By proactively identifying risks and preventing damage, we protect OT environments from physical disruptions, monetary losses and reputational harm.



**Faster incident response:** Through integrated incident response strategies managed by HCLTech and Armis, organizations benefit from streamlined remediation processes. Businesses build robust defenses against persistent and repeat attacks, from comprehensive forensic investigations to automated threat containment.



**Alignment with regulatory standards:** Our solution helps meet stringent compliance requirements for industries such as energy (NERC CIP), healthcare (HIPAA), manufacturing (ISO 27001) and others. By adhering to regulatory security mandates, organizations eliminate risks of penalties, fines or reputational damage.



**Cost efficiency and scalability:** Our joint solution enables businesses to minimize cybersecurity costs by consolidating efforts under unified architecture. Our scalable approach allows organizations to extend visibility and protection seamlessly as their OT and IoT ecosystems grow.



**Future-ready security:** Our offering empowers organizations to innovate confidently by staying ahead of emerging threats. Whether integrating new technologies, adopting Industry 4.0 principles, or enhancing connected systems, businesses can grow without exposing themselves to unnecessary risks.

The partnership between HCLTech and Armis brings unparalleled depth and expertise in OT security. Together, we address the challenges OT environments face today, providing organizations with a trusted solution to fortify their critical systems, safeguard productivity and adapt to an ever-changing threat landscape. Let HCLTech-Armis transform your approach to OT cybersecurity because, in an interconnected world, protecting operational technology protects the future of your business.



**HCLTech** | Supercharging  
Progress™

[hcltech.com](https://hcltech.com)