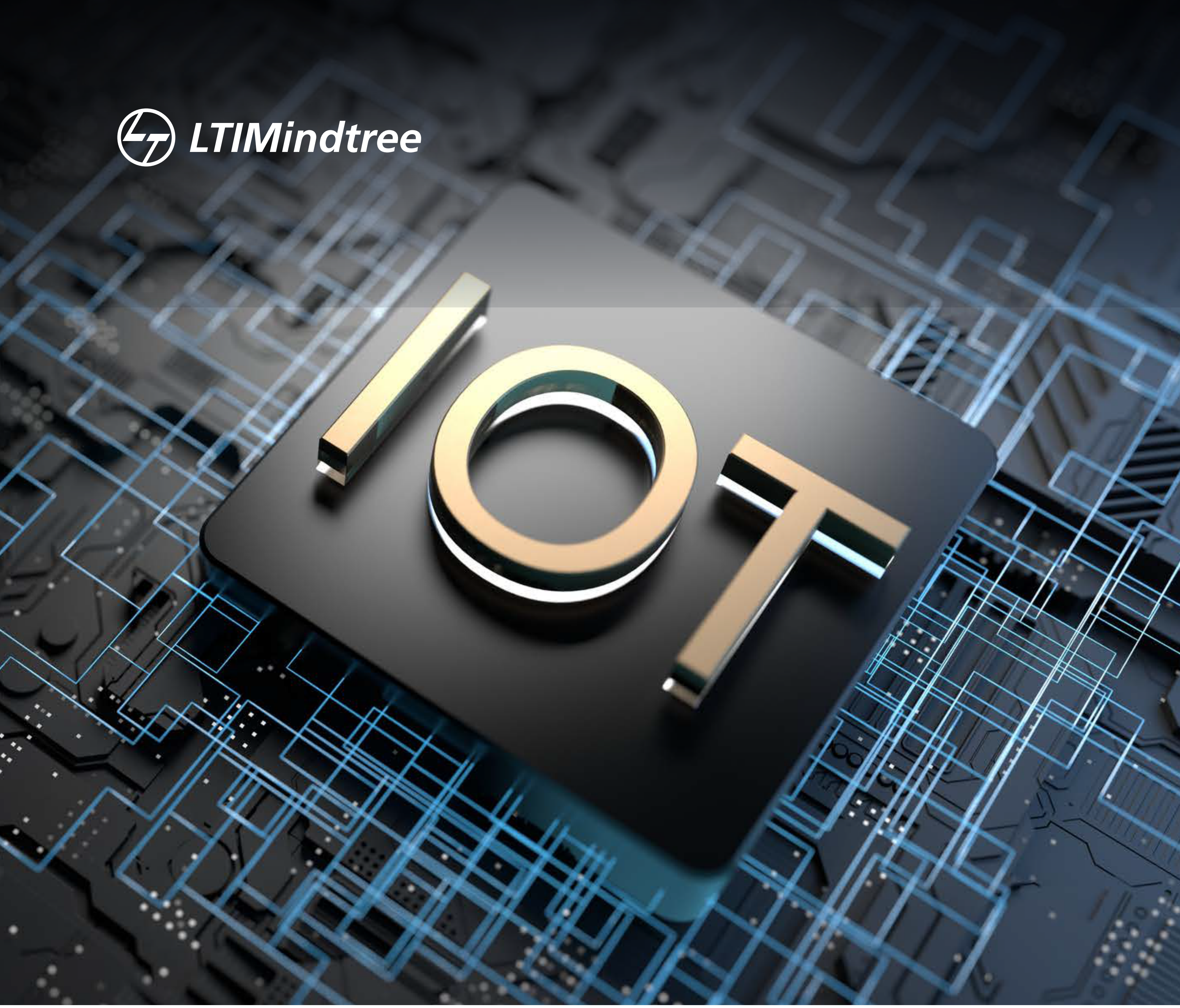
LTIMindtree



Brochure

LTIMindtree's Enterprise IoT/OT Security Offering

In the era of industry 4.0 evolution, with rapid adoption of new IoT-led services (e.g., connected car, smart device, smart home, medical device, digital twins), along with traditional legacy OT environment, has multiplied the complexities and cybersecurity challenges for an enterprise. Rapid convergence of IT/IoT/OT/IIoT network and exponential increase of security attacks, enterprises are facing an uphill task to find and implement the right solution robust enough to protect their IoT/OT landscape.

Top challenges for CIOs/CISOs

Adoption and Risk

68%
Organizations say IoT/OT is critical to supporting business innovation, other strategic goals

60%
With IoT/OT security as one of the least secured aspects of their infrastructure

31%
Organizations slowing, limiting or have stopped the adoption of IoT/OT projects due to security concerns

Technology Gaps

71%
lack complete inventory of its IoT/OT devices

70%
Have low or average confidence that IoT/OT devices are secure (e.g., vulnerability mitigated, securely configured)

61%
Have low or average confidence in the ability to identify whether IoT/OT devices are compromised

* The State of IoT/OT CyberSecurity in Enterprise Organizations, Ponemon Institute, October 2021

Security Complexities

- 360-degree Insight of IoT/OT device
- Identifying Vulnerabilities
- Little or no visibility into IoT/OT risk
- Security threat detection & response
- Safety & Availability & Integrity
- Traditionally air-gapped device
- Security hygiene
- Device update
- Specialized protocols, legacy devices, and OS

- Devices rarely built with secure boot and attestable integrity
- Off-the-shelf devices are not properly hardened
- Device builder to build security-by-design device
- 50% of IoT devices shipping devices with well-known vulnerabilities
- Vendors rarely provide automated means to patch devices
- Network traffic between devices rarely encrypted
- Zero-trust define for IoT/OT network

LTIMindtree's Enterprise IoT/OT Security Offering directly addresses prevalent industry challenges in IoT/OT environment and offers end-to-end security protecton solution to end-user organization, and device builders.

- Discovery
- Assessment
- Detection
- Mitigation

Our offering enables secure and accelerate IoT/OT transformation with complete security solution across IoT/OT environment (Brownfield, Greenfield) to establish converged security operation with salient capabilities:

- Discover the devices
- Risk assessment and identify vulnerability
- Detection of threats/incidents
- Identify attack vector paths
- Mitigation of threats/incidents
- Seamless integration with SIEM, SOAR, ITSM

Our Security Offering

delivers three solutions to an enterprise for securing yours IoT/OT environments.

IoT/OT Security – Strategy

- Discovery of IoT/OT landscape
- Assess the IoT/OT landscape against security standards (NIST, CIS, Purdue model)
- Strategize roadmap for establishing Converged Managed Security Operations

IoT/OT Security – Implementation

- Design IoT/OT Solution architecture
- Implement Agentless, Agent-based Security solution in flexible deployment model
- Implement Security framework (NIST, CIS)
- Establish security-by-design for new IoT/OT device builders
- Establish security monitoring for end-user organization using IoT/OT devices
- Establish zero-trust access for IoT/OT environment
- Configuration and integration of IoT/OT security solution

IoT/OT Security – Managed Security Operation

- Integration with SIEM, SOAR and ITSM
- Implement MITRE ATT&CK rule, threat intelligence for detection of IoT/OT attacks
- Real-time security threat/malware monitoring and automated response
- Establish converged managed security operation for IT/IoT/OT environment
- Discovery of Authorized/Unauthorized - device, software, protocol
- Identify vulnerability, perform risk assessment, and device updates, patching
- Attack vector path identification, performing regular hunting

Key Benefits

- Discovery of devices
- Risk assessment & identify vulnerability
- Identify attack vector paths
- Detection of threats/incidents
- Mitigation of threats/incidents
- Mitigation of threats/incidents

- Seamless integration with SIEM, SOAR, ITSM
- Embed threat intelligence
- Event timeline order view
- Run analytics query with data mining
- Supports agent-based and agentless solution
- Supports on-premise & cloud deployment

- End-user organizations: Protect IoT/OT environments with agentless monitoring
- Device builders: embed security into new IoT/OT initiatives with microsoft defender IoT lightweight agent
- Framework, platform, industry expert, and global footprint
- Strong strategic OEM Partnership, CoE-skilled resource

Key Service Features

- Protection coverage: solution caters to both end-user organization and device builder
- Flexible solution: supports agentless, agent-based solution
- Hybrid deployment: supports on-premise (offline), cloud (online) deployment model
- Discovery of devices
- Risk assessment with risk score
- Attack vector paths identification
- Vulnerability identification, device update, and patching
- Security threat detection and automate response
- Integrated threat intelligence for attacks, malware, anomalies behaviour, policy violation, protocol violation
- Supports all standard protocols, custom/proprietary/restricted protocols
- Event Timeline series chronological view
- Seamless integration with technologies
  - SIEM (Azure Sentinel, Splunk, IBM QRadar, ArcSight, LogRhythm, RSA)
  - SOAR (Playbooks, IBM Resilient)
  - ITSM (ServiceNow)
  - Secure remote access solutions such as CyberArk Privileged Session Manager (PSM) and BeyondTrust
  - Secure network access control (NAC) systems such as Aruba ClearPass and Forescout CounterACT
  - Firewalls such as Fortinet and Check Point

Our Value Proposition

- Protecting end-to-end IoT/OT environment (End-user Organization, Device builder)
- Supports flexible deployment with agentless, agent-based
- Security-by-design incorporate at time of IoT/OT device builder
- 360-degree, real time insight view IoT/OT device
- Device risk and mapping and connection (wrt Purdue model)
- Integrated threat intelligence, data mining with threat hunting
- Establish Digital SOC with MITRE ATT&CK rule, theat intelligence, ML, SOAR
- Real-time security incident detection and automated-response
- Attack vector path identification and mitigation
- Vulnerability identification, risk assessment with risk score
- Security hygiene score and recommendation
- Compliant with standards (CIS, NIST)
- Remote management of air-gapped device
- Firmware vulnerability, weak authentication, and firewall rule detection
- Detection of unauthorized bridges between subnets
- Authorized/Unauthorized - protocol, device, software detection
- Identification of unauthorized remote access connections

Service Package

Standard

IoT/OT Security Strategy

Gold

Standard + IoT/OT Security Implementation

Premium

Gold + IoT/OT Managed Security Operation

Technology Stack

Microsoft Defender for IoT (CyberX, ReFirm Labs)

Partner Ecosystem

Microsoft (CyberX, ReFirm Labs)

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 84,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit **https://www.ltimindtree.com/**