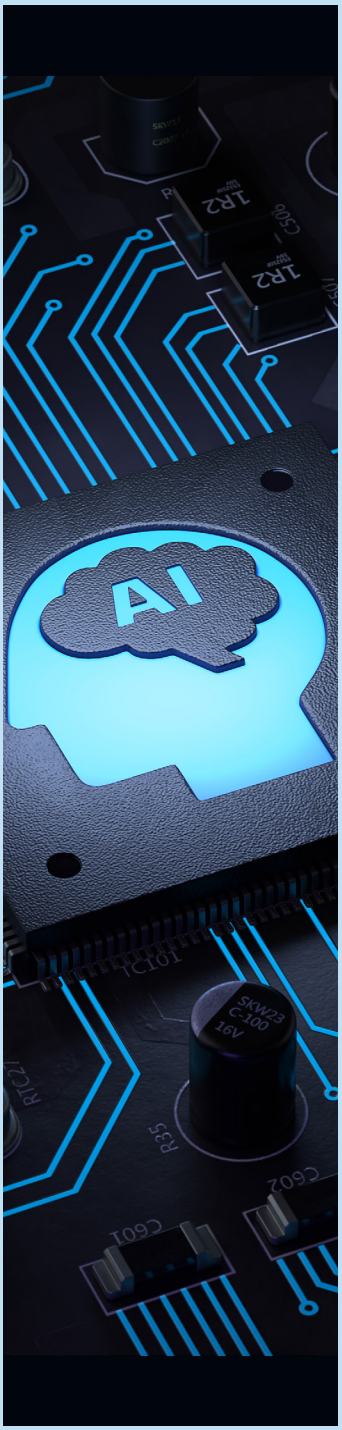
VIEW POINT



AI AT THE EDGE: SECURING IT/OT CONVERGENCE WITH MULTI-LAYERED DEFENSE

Abstract

The convergence of Information Technology (IT) and Operational Technology (OT) is reshaping industrial ecosystems, enabling real-time insights, predictive analytics, and operational efficiency. However, this integration introduces significant cybersecurity challenges, as traditionally isolated OT environments become exposed to IT networks and external threats. Centralized security models often fail to meet the low-latency and high-availability requirements of OT systems, creating a need for localized intelligence.

Infosys
Navigate your next

Contents

Executive Summary

The rapid convergence of Information Technology (IT) and Operational Technology (OT) is transforming industrial ecosystems, enabling real-time data exchange, predictive analytics, and autonomous decision-making. However, this integration introduces significant cybersecurity challenges, as traditional perimeter-based defenses are insufficient to protect distributed edge environments.

AI at the Edge emerges as a critical enabler for securing IT/OT convergence. By deploying artificial intelligence closer to data sources, organizations can achieve low-latency threat detection, context-aware anomaly identification, and autonomous response mechanisms without relying on centralized systems. This approach ensures resilience in environments where downtime or breaches can have severe operational and safety implications.

A multi-layered defense strategy is essential to address the complexity of edge security. Key components include:

- **Zero Trust Architecture**
  Enforcing identity-based access and continuous verification across IT and OT assets
- **AI-Driven Threat Analytics**
  Leveraging machine learning models to detect advanced persistent threats and insider risks in real time
- **Secure Edge Gateways**
  Implementing hardened devices with embedded security controls for data integrity and confidentiality
- **Network Segmentation & Micro-Segmentation**
  Isolating critical OT systems from IT networks to minimize attack surfaces
- **Continuous Monitoring & Adaptive Response**
  Using AI to dynamically adjust security policies based on evolving threat landscapes

The integration of AI-powered edge security with layered defense mechanisms not only mitigates cyber risks but also enhances operational efficiency, regulatory compliance, and business continuity. Organizations that adopt this paradigm will be better positioned to safeguard critical infrastructure while unlocking the full potential of IT/OT convergence.

Introduction

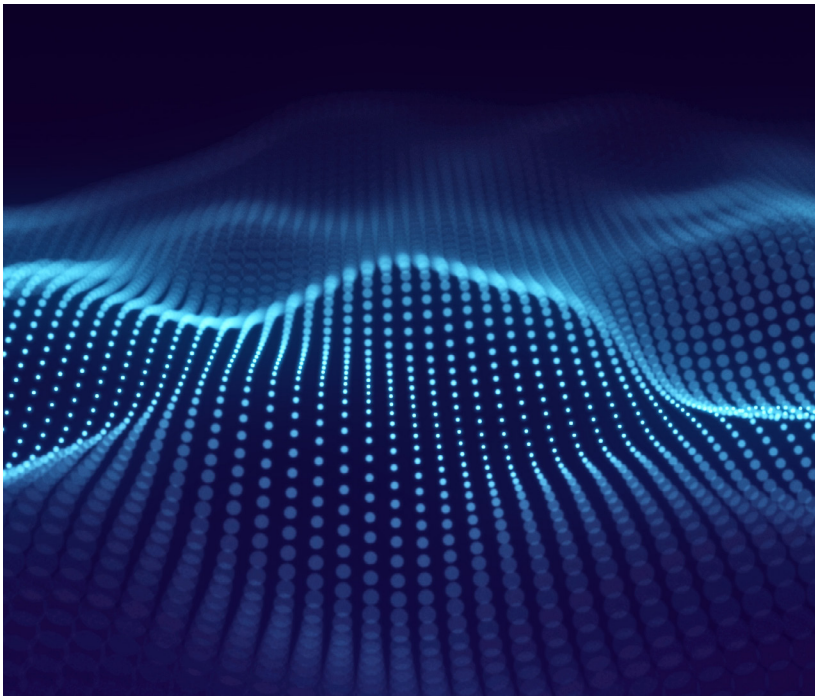
The digital transformation of industrial environments is driving the convergence of Information Technology (IT) and Operational Technology (OT), creating a unified ecosystem that enables real-time insights, predictive maintenance, and optimized operations. While this integration delivers significant business value, it also introduces unprecedented cybersecurity challenges. Traditional security models, designed for isolated IT or OT environments, struggle to protect the expanded attack surface created by interconnected systems, edge devices, and critical infrastructure.

As organizations push intelligence closer to the edge, Artificial Intelligence (AI) at the Edge becomes a game-changer. By processing data locally and applying advanced analytics in real time, AI empowers rapid threat detection, anomaly identification, and autonomous response—capabilities essential for safeguarding mission-critical operations. However, securing IT/OT convergence requires more than just AI; it demands a multi-layered defense strategy that combines Zero Trust principles, network segmentation, and continuous monitoring to ensure resilience against sophisticated cyber threats.

Market Context

According to independent research farm, the Edge AI Security market is emerging as a critical segment, projected to grow by **$11.7 billion** between 2024 and 2029, at a CAGR of **35.5%**. Key drivers include the proliferation of IoT devices, expansion of the attack surface, and adoption of Zero Trust architectures for distributed edge environments.

Complementing this, the AI in Cybersecurity market which underpins multi-layered defense strategies—is expected to grow from **$25.35 billion** in 2024 to **$93.75 billion** by 2030, at a CAGR of **24.4%**. AI-driven security solutions are increasingly integrated into IT/OT systems to provide real-time threat detection, anomaly identification, and automated response.



Challenges in IT/OT Convergence

1. Expanded Attack Surface

- Connecting IT systems (enterprise networks, cloud) with OT systems (industrial control systems, SCADA) introduces new entry points for cyberattacks
- Legacy OT devices often lack modern security features, making them vulnerable

2. Legacy Infrastructure & Compatibility

- OT environments typically run on outdated hardware and proprietary protocols
- Integrating these with modern IT systems creates compatibility and security gaps

3. Lack of Unified Security Framework

- IT security focuses on data confidentiality, while OT prioritizes availability and safety
- Aligning these priorities under a single governance model is complex

4. Real-Time Operational Constraints

- OT systems require continuous uptime; applying patches or updates can disrupt operations
- Security measures must be implemented without impacting production

5. Skills Gap

- Few professionals have expertise in both IT cybersecurity and OT operations
- Organizations struggle to build cross-functional teams for convergence projects

6. Regulatory & Compliance Pressure

- Industries like energy, healthcare, and manufacturing face strict compliance requirements
- Ensuring compliance across converged environments adds complexity

7. Insider Threats & Third-Party Risks

- Increased collaboration with vendors and contractors expands trust boundaries
- Insider misuse or compromised third-party access can lead to severe breaches

8. Limited Visibility & Monitoring

- OT networks often lack advanced monitoring tools
- Detecting anomalies across IT and OT in real time is challenging without integrated solutions

9. Data Integrity & Latency Issues

- Edge devices and sensors generate massive data streams
- Ensuring secure, low-latency data transfer between IT and OT systems is critical

Role of AI at the Edge

AI at the Edge refers to deploying artificial intelligence capabilities directly on edge devices or gateways, close to where data is generated (e.g., sensors, controllers, industrial machines). This approach is critical for IT/OT convergence because it enables real-time decision-making and security enforcement without relying on centralized systems.

Real-Time Threat Detection

- AI models at the edge can analyze network traffic, device behavior, and operational data instantly
- Detect anomalies such as unauthorized access, abnormal machine behavior, or malware propagation before they escalate

Low-Latency Response

- Edge AI eliminates delays caused by sending data to cloud or central servers
- Enables immediate isolation of compromised devices or execution of automated response protocols

Context-Aware Security

- AI can correlate IT and OT data streams to understand operational context
- For example, distinguishing between a legitimate maintenance shutdown and a malicious attempt to halt production

Predictive Maintenance & Risk Mitigation

- AI-driven analytics predict equipment failures and security vulnerabilities
- Reduces downtime and prevents cascading failures that attackers could exploit

Adaptive Defense Mechanisms

- AI continuously learns from new threats and adapts security policies dynamically
- Supports Zero Trust principles by validating every device and transaction at the edge

Data Privacy & Compliance

- Processing sensitive data locally minimizes exposure to external networks
- Helps meet regulatory requirements for data sovereignty and confidentiality

Scalability for Distributed Environments

- Edge AI scales across thousands of devices in industrial plants or remote sites
- Provides uniform security posture without overwhelming central infrastructure

Multi-Layered Defense Framework

A robust security architecture for IT/OT convergence must combine **preventive, detective, and responsive controls** across multiple layers. Below is a structured framework:

1. Device & Endpoint Security

- **Hardened Edge Devices**
  Secure boot, firmware integrity checks, and encrypted storage
- **AI-Powered Endpoint Protection**
  Detect malware and anomalous behavior locally

2. Network Security

- **Segmentation & Micro-Segmentation**
  Isolate IT and OT networks to limit lateral movement
- **Zero Trust Network Access (ZTNA)**
  Enforce identity-based access and continuous verification
- **Encrypted Communication**
  TLS/IPSec for data-in-transit between edge and core systems

3. Identity & Access Management

- **Multi-Factor Authentication (MFA)**
  for all users and devices
- **Role-Based Access Control (RBAC)**
  aligned with least privilege principles
- **Continuous Authentication**
  using AI-driven behavioral analytics

4. Data Security

- **Edge Data Encryption**
  Protect sensitive operational data at rest and in transit
- **Data Integrity Validation**
  AI models detect tampering or unauthorized changes

5. Threat Detection & Response

- **AI-Driven Anomaly Detection**
  Real-time monitoring of IT and OT traffic for deviations
- **Behavioral Analytics**
  Identify insider threats and compromised accounts.
- **Automated Response**
  AI triggers isolation, patching, or rollback actions instantly

6. Application & Workload Security

- **Secure Containers & Virtualization**
  Protect workloads running at the edge
- **Runtime Protection**
  AI monitors application behavior for exploits

7. Governance & Compliance

- **Policy Enforcement**
  Unified security policies across IT and OT
- **Continuous Auditing**
  AI assists in compliance reporting and risk scoring

8. Resilience & Recovery

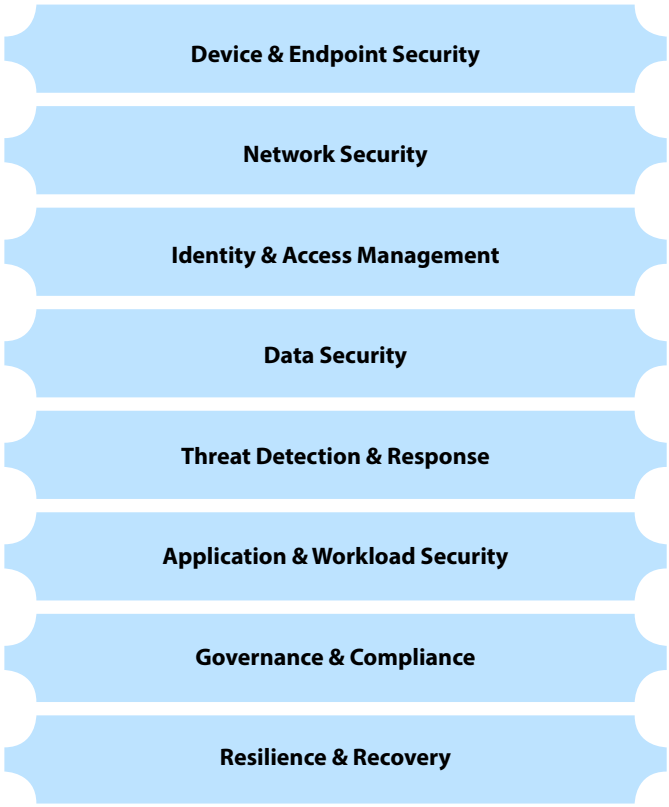
- **Backup & Disaster Recovery**
  Secure, immutable backups for OT systems
- **AI-Assisted Incident Response**
  Accelerates root cause analysis and recovery

Integration with AI at the Edge

- **AI acts as the intelligence layer across all these defenses, enabling:**
  - Predictive threat modeling
  - Adaptive policy enforcement
  - Autonomous remediation

Multi-Layered Defense Framework

Securing IT/OT Convergence with AI at the Edge



Requirements of the hours:

Insights from the Graph

AI-Led Attacks occur far more frequently (120 per hour) compared to traditional attacks (45 per hour)

Response Time for AI-led attacks is significantly shorter (2 minutes) due to automation and adaptive strategies, while traditional attacks average around 15 minutes

This demonstrates how AI-driven threats are **faster, more adaptive, and harder to mitigate** without advanced defense mechanisms

Strategic Recommendations

1. Adopt a Zero-Trust Architecture Across IT and OT

- Enforce identity-based access controls for all devices and users
- Implement continuous authentication and least-privilege principles for OT systems

2. Deploy AI-Powered Threat Detection at the Edge

- Use machine learning models on edge gateways to monitor OT traffic and detect anomalies in real time
- Enable autonomous response capabilities to isolate compromised nodes without central intervention

3. Implement Network Segmentation and Micro-Segmentation

- Separate IT and OT zones with strict firewall policies
- Apply micro-segmentation within OT environments to limit lateral movement of threats

4. Secure Device-Level Operations

- Ensure secure boot, hardware root of trust, and firmware integrity for all edge devices
- Encrypt data in transit and at rest across IT/OT networks

5. Integrate Federated Learning for Privacy-Preserving Analytics

- Train AI models locally at the edge without transferring raw data to the cloud
- Reduce exposure of sensitive operational data while maintaining predictive capabilities

6. Establish Policy-Driven Governance and Compliance

- Align security policies with standards like IEC 62443 and NIST CSF
- Automate compliance monitoring and reporting across IT/OT environments

7. Enhance Visibility Through Unified SOC Integration

- Correlate edge-level security insights with enterprise Security Operations Center (SOC).
- Use AI-driven analytics for holistic threat intelligence and faster incident response.

8. Invest in Resilient Edge Infrastructure

- Deploy ruggedized edge hardware with built-in security features for harsh industrial environments
- Ensure redundancy and failover mechanisms for critical OT processes

9. Continuous Training and Simulation

- Conduct regular cyber drills simulating IT/OT attack scenarios
- Train operational teams on AI-driven security tools and incident response protocols

10. Secure Third-Party and Supply Chain Integrations

- Validate security posture of vendors and partners before connecting to OT networks
- Implement zero-trust principles for external data sources and remote maintenance

Conclusion

The convergence of IT and OT systems is a cornerstone of modern industrial transformation, enabling real-time insights and operational efficiency. However, this integration introduces complex cybersecurity challenges that traditional centralized models cannot address.

AI at the Edge offers a powerful solution by delivering localized intelligence, rapid anomaly detection, and autonomous response capabilities directly where data is generated.

A multi-layered defense strategy combining device-level security, network segmentation, zero-trust principles, and AI-driven analytics is essential to protect critical infrastructure from evolving threats. By embedding security into every layer of IT/OT architecture and leveraging edge AI for predictive and adaptive protection, organizations can achieve resilience without compromising performance.

Ultimately, securing IT/OT convergence is not just a technical necessity, it is a strategic imperative for sustaining trust, ensuring compliance, and enabling innovation in an increasingly connected industrial ecosystem. Organizations that invest in edge AI security today will be better positioned to defend against tomorrow's cyber threats while unlocking the full potential of digital transformation.

Digital Reference:

- **Edge AI: Paving the Way for Intelligent, Resilient Deployments** (IDC/Intel, Oct 2025)
  Discusses integration of edge AI in enterprise systems, emphasizing architecture, resilience, and real-time analytics. [cdrdv2-pub....intel.com]
- **ITOT Convergence Whitepaper** (host.sg, Oct 2023)
  Explores how edge computing bridges IT and OT, addressing cybersecurity, data management, and operation modernization. [cdrdv2-pub....intel.com], [host.sg]
- **Edge AI Security | Defense in Depth White Paper** (AAEON)
  Presents a multi-layered security framework for edge AI deployments, including hardware, communications, and centralized controls. [aaeon.ai]
- **Securing Industry 4.0: A Systematic Review of AIDriven Intrusion Detection** (Journal of Reliable Intelligent Environments, Dec 2025)
  Reviews AI-enabled intrusion detection in IIoT/OT, highlighting edge-enabled architectures and defense strategies. [link.springer.com]
- **Cybersecurity Solutions for Industrial IoT–Edge Computing Integration** (Sensors, MDPI, Jan 2025)
  Examines IIoT/edge cybersecurity threats and defense mechanisms including ML, federated learning, and blockchain.

Author

Rajesh Kumar Mohapatra is a Cyber Security leader with 14+ years of experience in managing and architecting security portfolios for enterprises across India and global markets, with a growing focus on AI-driven security and responsible AI adoption. He brings deep expertise in securing complex hybrid environments while addressing emerging risks introduced by automation, intelligent systems, and AI-enabled platforms. He has led and delivered security solutioning across Azure Cloud Security and on-premises infrastructures, covering technologies such as Firewalls, Proxies, Cisco ISE, EDR, XDR, Email Security, and Data Security. His work increasingly intersects with AI security domains, including AI assisted threat detection, identity centric security, intelligent endpoint protection, and governance frameworks for secure and ethical AI usage.

In addition to his technical strengths, Rajesh plays a key role in security governance, risk, and compliance, helping enterprises embed security and compliance controls into AI-enabled digital transformation initiatives. His approach emphasizes trust by design, resilience, and alignment with evolving regulatory and ethical standards.

He is currently working as Principal Consultant – Infrastructure Management and Technology Manager specializing in Cyber Security, based in Bhubaneswar. He brings extensive experience in designing, securing, and managing enterprise IT infrastructure with a strong focus on cyber risk management, security architecture, and operational resilience. Rajesh has worked closely with leadership and cross functional teams to drive secure digital transformation initiatives, strengthen security postures, and align technology strategies with business objectives. His expertise spans infrastructure modernization, cybersecurity governance, and risk mitigation across complex enterprise environments.

For more information, contact askus@infosys.com

Infosys®
Navigate your next