GROWTH ACCELERATION PARTNERS

THE NEW RULES OF IOT SECURITY

Building Resilience for 2025

IOT & CONNECTED DEVICES

As the global IoT footprint surges past 19 billion connected devices in 2025, enterprises face a rapidly expanding attack surface. Spending on IoT security is projected to surpass $11 billion this year, with forecasts showing investments could reach $50 billion by 2026 to counter the growing risk. Yet despite these efforts, one in three data breaches globally now involves an IoT device, and over 50% of deployed devices still carry at least one critical vulnerability. These devices — from industrial PLCs to healthcare monitors and smart city sensors — deliver transformative value but bring a fundamentally different set of risks compared to conventional laptops, servers and cloud applications.

While traditional IT environments rely on uniform, general-purpose hardware with ample computing power and well-supported security tools, IoT devices are highly diverse, resource-constrained, and often lack standard operating systems. Many ships with default credentials, minimal update processes, and no capacity to run traditional endpoint security agents. Even the protocols these devices use — from CoAP to Zigbee to MQTT — were not designed with robust authentication or encryption in mind, leaving significant security blind spots.

Moreover, IoT attacks can quickly move beyond digital consequences into the physical world: disrupting manufacturing systems, altering chemical treatments in water facilities, or even threatening human safety. As attackers shift tactics to exploit these cyber-physical connections, the need for modern, IoT-specific security approaches is urgent.

In this article, we'll break down:

- **How IoT security challenges differ from traditional IT**
- **How emerging technologies like AI and edge computing are changing the security landscape**
- **Sector-specific best practices for industries like healthcare, manufacturing, smart cities and consumer IoT**
- **What a "2025-ready" IoT security posture really looks like**

How Is IoT Security Different from Traditional IT Security?

While traditional IT systems are built around standardized servers, workstations, and cloud infrastructure, the IoT world is far more fragmented. IoT devices account for an increasing share of connected-device vulnerabilities — climbing from 14% in 2023 to 33% in 2024 — and require far more rigorous compliance investments. Regulatory frameworks like the EU Cyber Resilience Act are already pushing enterprises to raise IoT security budgets by 20–30% in 2025, adding a layer of financial urgency to solving these security gaps.

Device Diversity and Constraints

Traditional IT assets are powerful, uniform and run mainstream operating systems with the ability to host mature security agents like EDR or antivirus. In contrast, IoT devices range from tiny sensors to industrial robots, often powered by microcontrollers with minimal memory or battery capacity. Many cannot support traditional endpoint security software or strong encryption, and they often ship with hardcoded or default credentials.

Complex, Fragmented Networks

Enterprise IT networks typically follow well-known architectures with predictable traffic, robust segmentation, and mature security controls. IoT environments, on the other hand, involve diverse protocols (e.g., Zigbee, LoRaWAN, Modbus) and often span multiple tiers: edge gateways, cloud APIs, private cellular, and even public internet channels. These pathways complicate traffic inspection and security monitoring.

Identity and Access Control Challenges

In IT, user identities are governed by well-integrated systems like Active Directory and MFA policies. IoT devices rarely fit these models, lacking standard directory integrations or user interfaces. As a result, they rely on static keys, shared credentials, or even unauthenticated interfaces. Building consistent, strong authentication for heterogeneous devices is an ongoing challenge.

Limited Visibility and Asset Management

Traditional IT has near-complete inventories thanks to CMDBs, endpoint agents, and robust discovery tools. IoT devices frequently slip through asset management processes because they might be connected to non-IT-owned networks, installed by facilities or engineering teams, or operate on protocols standard IT scanners don't understand. This creates dangerous blind spots and unmanaged risks.

Patch and Lifecycle Gaps

IT assets are patched monthly, often with automated tools. But many IoT devices need manual updates, might require physical access, or have no vendor support for critical fixes. That means years-old vulnerabilities can stay exploitable long after they are published, giving attackers a persistent foothold.

Expanded Attack Surface and Physical Risks

Where traditional IT security mainly protects data, IoT security protects both data and the physical processes these devices control. A breach can alter environmental systems, shut down safety-critical operations, or even put lives at risk — something traditional IT rarely needs to consider.

For enterprise security leaders, this means IoT cannot simply bolt onto existing cybersecurity playbooks. It requires purpose-built security architectures, tailored monitoring, and proactive governance to manage its unique risk profile.

GROWTH ACCELERATION PARTNERS

How Are Emerging Technologies Like Edge Computing and AI Reshaping IoT Security?

The pace of change in IoT is being matched by an evolution in security strategies. As organizations deploy billions of connected devices, they increasingly rely on advanced technologies like AI and edge computing to keep up with growing attack volumes and sophisticated threats.

AI/ML-Powered Threat Analysis

Artificial intelligence now helps enterprises profile “normal” device behavior in real time, flagging subtle anomalies as they happen. These models can spot deviations instantly and trigger automated responses, dramatically cutting dwell time compared to traditional rules-based tools. This shift toward AI-driven detection is essential in environments where attackers adapt malware to blend in with legitimate device traffic.

Adaptive Defenses and Prioritization

AI can also prioritize risks intelligently, correlating data across devices, sites, and timeframes to catch multi-stage or highly distributed attacks. In industrial cyber-physical systems, for example, advanced AI platforms offer not only detection but also automatic triage and risk ranking, making security operations faster and more efficient.

Federated Learning for Privacy

To respect data privacy while still building strong detection models, enterprises are adopting federated learning. This allows local IoT devices to train models on their own data, sharing only model updates with a central system, keeping raw data private while improving fleet-wide security insights.

Zero-Touch Automation

Edge computing and AI together enable “zero-touch” security approaches, where IoT devices can auto-register, obtain credentials, and be continuously verified with little human intervention. This minimizes configuration errors and accelerates secure onboarding for large device fleets.

Next-Generation Security Architecture

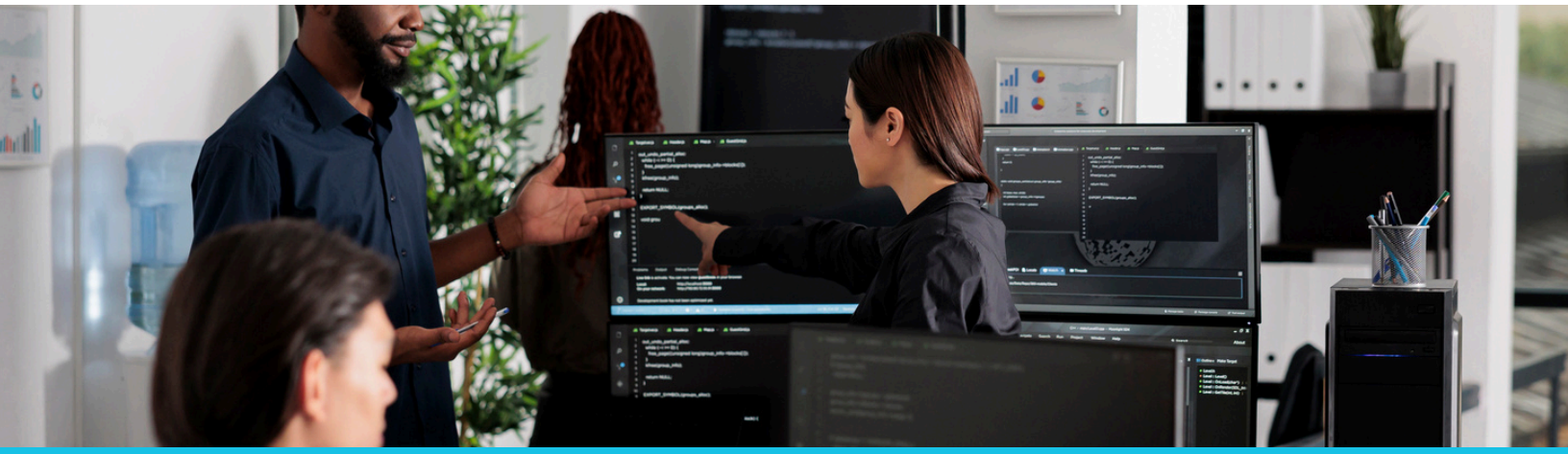
Edge computing brings security closer to where data is generated, allowing faster detection and containment of threats before they reach corporate or cloud infrastructure. Combined with micro-segmentation and zero trust, this architecture shrinks the attack surface and localizes breaches.

Governance Considerations

These new capabilities come with new governance demands. Organizations are developing AI use policies, ethical reviews, and data-classification rules for IoT telemetry. Regulatory frameworks are catching up, but proactive governance will be critical to avoid compliance or ethical missteps.

The Business Advantage

AI and edge-enabled security unlock faster response, richer visibility, and stronger resilience. Some industrial environments are already seeing near–real-time responses that used to take hours, thanks to AI analyzing terabytes of sensor data daily. This is no longer a theoretical upgrade — it is a business advantage for security and operational continuity.



Sector-Specific IoT Security Patterns

The financial stakes are undeniable: nearly 60% of organizations worldwide now use IoT solutions, and among those, a staggering 84% report experiencing at least one IoT-related security breach. With these numbers, sector-specific controls are no longer optional — they are essential to safeguard revenue, resilience, and reputation.

Securing IoT is not a one-size-fits-all challenge. Each industry has unique devices, safety priorities, and compliance pressures. Here are patterns drawn from the latest research to guide risk-mature security strategies across key sectors:

Healthcare

- Isolated Medical VLANs: Keep medical IoT devices — infusion pumps, imaging systems, bedside monitors — on dedicated, firewalled VLANs to block access from general IT networks.
- Certificate-Based Device Identity: Hospitals increasingly issue X.509 certificates through internal PKI to authenticate devices before joining the network.
- Encrypted Clinical Data: HL7 and FHIR messages moving between monitors and EHR systems should use mutual TLS to protect patient data.
- FDA-Cleared OTA Updates: Manufacturers are delivering signed firmware updates through hospital-controlled consoles, with rollback capability for safety-critical systems.
- AI-Powered Anomaly Detection: Behavioral analysis tools can flag, for example, a pump that suddenly pushes unexpected data volumes, helping clinical security teams catch tampering early.

Manufacturing & Industrial

- IEC 62443 Zones/Conduits: Plants group PLCs, robotics, and SCADA systems into secure zones and apply policies on conduits between them, limiting what protocols can pass through.
- Hardware Root of Trust: Leading PLC vendors embed TPM modules to verify firmware signatures, preventing unapproved code from running.
- Secure Edge Gateways: Protocol translators at the edge convert legacy protocols into secure, authenticated messaging (e.g., MQTT over TLS).
- Controlled Remote Access: Third-party support teams use tightly scoped, MFA-protected VPN sessions via jump hosts, never accessing OT networks directly.
- Predictive AI for Maintenance & Security: Vibration or telemetry sensors using embedded ML can detect early signs of compromise alongside mechanical failures.

Smart Cities & Logistics

- PKI Provisioning at Manufacture: Streetlights, cameras, and smart meters get certificates at production, registering automatically with a municipal IoT hub on first boot.
- Encrypted Mesh Networks: LoRaWAN or 5G-based systems apply AES-128 or stronger encryption on every hop to resist interception.
- Dynamic Network Slicing: Critical public-safety telemetry — for example, from drones or emergency responders — is isolated from general traffic using 5G slices with unique SLAs.
- Signed OTA Rollouts: Traffic-control systems use cryptographically signed firmware updates, piloted in test districts before city-wide rollout.
- Federated AI Anomaly Detection: Waste-bin sensors or traffic sensors push only summarized anomalies to a central SOC, preserving bandwidth and reducing risk of a full compromise.

Consumer IoT

- Baseline Security by Default: Smart-home brands now ship devices with unique passwords, vulnerability disclosure processes, and a minimum five-year update commitment in line with ETSI EN 303 645.
- Home Network Segmentation: Many consumer routers default to a “guest” SSID for IoT, isolating devices like smart speakers from user laptops or phones.
- Secure Boot & Firmware Signing: Smart TVs and wearables increasingly use bootloaders that reject unsigned firmware, rolling back if integrity fails.
- MFA for Mobile Control: Apps controlling smart locks or cameras demand multi-factor authentication, often with biometrics, to prevent remote takeovers.

Pattern Takeaways

- Security by default — no more universal default passwords
- Segmentation and micro-segmentation to limit blast radius
- Signed OTA updates for resilience
- End-to-end encryption at every layer
- Intelligent, ML-driven monitoring to catch subtle anomalies

What Does a 2025-Ready IoT Security Posture Look Like?

Leading enterprises in 2025 no longer treat IoT devices as second-class IT assets — they integrate them fully into modern, multi-layered cybersecurity programs. A “2025-ready” IoT security posture is built on these pillars:

Zero Trust for IoT

Every device, user, and data flow is assumed untrusted until continuously proven otherwise. Identity verification, micro-segmentation, and strict policy enforcement ensure that even if one IoT device is compromised, the blast radius is contained.

Hardware-Backed Device Identity

Each IoT device should carry a cryptographically verifiable identity, secured with TPMs, secure elements, or certificate-based provisioning. This prevents impersonation and allows only authenticated devices to join the network.

Encryption by Default

All data, from edge sensors to cloud backends, should be encrypted in transit and at rest with strong algorithms like TLS 1.3 and AES-256. This protects sensitive telemetry and control messages from interception or manipulation.

Automated Patch and Firmware Management

Organizations must proactively manage IoT vulnerabilities through automated over-the-air updates, robust rollback plans, and continuous vulnerability scanning, even for constrained or remote devices.

AI-Driven Monitoring and Threat Detection

Modern IoT security leans on behavioral baselines powered by machine learning to catch unusual patterns in device traffic. Integrated with SIEM and SOAR platforms, these systems automate responses and reduce the time to contain attacks.

Full Lifecycle Security and Governance

A 2025-ready program secures the entire IoT lifecycle, from procurement and secure onboarding to decommissioning and disposal. Strong third-party risk controls, supply-chain verification, and secure deprovisioning (e.g., revoking certificates, wiping data) ensure no shadow devices slip through.

Integrated Security and Compliance

IoT-specific policies and controls should be mapped to standard frameworks like NIST SP 800-213, ISO 27001, and industry regulations (e.g., HIPAA, GDPR), so IoT data and systems are part of the organization’s unified risk and compliance posture.

In practice, this means IoT security is woven directly into the same processes, tools, and governance structures that protect traditional IT — but with its own tailored controls for device diversity, physical safety, and operational resilience.

Final Word

The explosive growth of IoT has unlocked enormous business potential — but it has also created unprecedented exposure across operations, customers and physical environments. In 2025, simply extending legacy IT security to billions of diverse, resource-constrained and highly distributed devices is no longer enough.

Securing IoT means rethinking your architecture, monitoring for threats in real time across the edge and the cloud, and using AI that can keep up with attackers. Most of all, it means treating IoT not as an afterthought but as a first-class citizen in your security, risk and compliance programs — today, before regulators and threat actors force your hand.

GAP is ready to help you build a 2025-ready IoT security strategy that fits seamlessly into your broader enterprise architecture. From risk assessments to full lifecycle protection, our experts are here to support you.

REACH OUT TODAY

To find out more, please visit www.WeAreGAP.com