IoT Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-07-01 | 150 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

IoT Security Market Analysis

The IoT Security Market size is estimated at USD 8.81 billion in 2025, and is expected to reach USD 37.41 billion by 2030, at a CAGR of 33.53% during the forecast period (2025-2030).

Enterprises are accelerating spending because regulators now mandate security-by-design for every connected product, operational technology is converging with IT networks, and AI analytics deliver real-time detection across massive device fleets. The United Kingdom's Product Security and Telecommunications Infrastructure Act and the European Union's Cyber Resilience Act have transformed security from a best practice into a legal requirement, diverting budgets from discretionary projects to mandatory compliance. Perimeter-centric defenses retain priority as millions of unmanaged endpoints widen attack surfaces, yet the move toward cloud-delivered controls is reshaping procurement criteria. Vendor differentiation increasingly depends on evidence of automated, standards-aligned protection that scales from factory floors to remote edge nodes.

Global IoT Security Market Trends and Insights

Data-breach-led Regulatory Scrutiny

Regulators moved from voluntary guidelines to punitive enforcement, exemplified by the EU Cyber Resilience Act that can impose EUR 15 million penalties for non-compliant devices entering the bloc. The United Kingdom's PSTI Act, effective April 2024, bans

default passwords and mandates defined update windows, forcing manufacturers to redesign firmware pipelines. Consumer-facing labels introduced by the US Federal Communications Commission in 2024 allow buyers to compare security maturity, shifting competitive advantage toward compliant vendors. High-profile incidents, such as the March 2025 cyberattack that exposed 5.5 million Yale New Haven Health patient records, illustrate regulatory urgency and intensify oversight. Tier-one assemblers now obligate component suppliers to hold third-party certifications, raising entry barriers for firms lacking documented secure-development processes.

Convergence of OT + IT Security Stacks

Operational technology networks that once ran in isolation now connect to corporate clouds to support predictive maintenance and analytics. Ransomware targeting the IT-OT interface surged 84% during Q1 2025 in North American plants, prompting unified visibility mandates in procurement documents. Legacy industrial protocols such as Modbus and DNP3 require security tools that understand deterministic traffic and strict latency thresholds, pushing vendors to integrate deep packet inspection tailored for factory environments. Cisco's security revenue more than doubled in its Q2 FY2025 results as customers consolidated on converged networking and security platforms. Implementation complexity has triggered demand for professional services that can migrate brown-field plants without prolonged downtime. As converged deployments mature, chief information security officers seek solutions that correlate anomalies across process controllers, corporate laptops, and remote maintenance links from a single console.

Fragmented Firmware-Update Ecosystem

Analysis of 53,000 firmware images across common microcontrollers showed 99.43% stored in plaintext, offering attackers direct access to boot loaders and secrets. Only one-third of vendors maintain an automated over-the-air update pipeline, leaving outdated components unpatched for an average of 1.34 years. EU rules now force automatic updates, compelling redesigns of remote-flash processes. Industrial operators hesitate because downtime for updates can cost hundreds of thousands of USD per hour, so unpatched assets persist inside critical infrastructure. The result is a widening security debt that slows the adoption of advanced authentication frameworks.

Other drivers and restraints analyzed in the detailed report include:

Shift-left Product-design Mandates / AI-powered Adaptive Threat Analytics / Legacy Brownfield Device Refresh Lag /

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Network Security generated 42% of IoT security market revenue in 2024, driven by enterprises that still treat the network edge as the only uniformly controllable enforcement point. Firewall, micro-segmentation, and secure SD-WAN policies restrict east-west traffic among heterogeneous endpoints that often lack chip-level safeguards. As production lines connect legacy programmable logic controllers to analytics clouds, inspection engines now parse industrial protocols alongside standard IP, demanding specialized threat-intel feeds. Adoption also benefits from the FCC rule requiring vendors to illustrate cloud-enabled update paths, nudging buyers toward providers that integrate firewall and proxy telemetry to verify patch status.

Cloud/Virtual Security is projected for a 35.45% CAGR through 2030 as platforms shift to security-as-a-service. Elastic capacity aligns with bursts from massive firmware-update pushes or backhaul from video sensors. Enterprises balance latency by keeping enforcement near the device while forwarding logs to centrally hosted analytics for correlated anomaly detection. Lightweight cipher suites such as LEA consume 30% less energy than AES-128, allowing real-time encryption even in coin-cell-powered tags.

Vendors that fuse cloud policy engines with local enforcement agents are poised to capture additional IoT security market share once 5G RedCap widens bandwidth on factory floors.

Solutions retained a 58% share of the IoT security market size in 2024, spanning encryption libraries, identity platforms, and runtime anomaly detection agents packaged into device SDKs. Pre-certified stacks shorten compliance audits under ETSI EN 303 645 or ISO 27400, so buyers still allocate budget to software licenses that tick regulatory checklists. However, Services, especially managed detection and response, will rise at a 36.08% CAGR because talent shortages push operators to outsource 24?7 monitoring.

Professional consulting demand climbed after the EU began a phased enforcement of the Cyber Resilience Act in January 2025, forcing manufacturers to document supply-chain risk assessments before product launch. Managed Security Services Providers centralize tooling and share threat intel across customers, giving midsize utilities access to capabilities once reserved for global brands. As SOC teams integrate AI co-pilots that triage alerts, service margins expand even while headcount stays flat, reinforcing the structural shift from product sales to recurring revenue models.

The Internet of Things (IoT) Security Market Report is Segmented by Security Type (Network Security, Endpoint/Devices Security, Application Security, and Cloud/Virtual Security), Component (Solutions and Services), End-User Industry (Smart Manufacturing, Connected Healthcare, Automotive and Mobility, Energy and Utilities, and More), Deployment Mode (On-Premise, Cloud/SECaaS, and Hybrid Edge), and Geography.

Geography Analysis

North America retained 35% of global revenue in 2024, anchored by federal initiatives such as the FCC labeling scheme that favor vendors prepared to document secure-update mechanisms. Enterprises adopted AI-enabled analytics early, leveraging extensive cloud infrastructure and mature SOC staffing. The Department of Homeland Security specifically names foreign intrusions into critical infrastructure as a top risk, driving federal grants toward water-utility and pipeline monitoring pilots. Canada mirrors the US approach, while Mexico's near-shoring boom requires integrated security across cross-border logistics hubs. Startups cluster around Silicon Valley and Austin, funneling patented firmware-integrity and post-quantum crypto solutions into Fortune 500 supply chains.

Asia Pacific is the fastest-growing territory, forecast for 35.49% CAGR, propelled by aggressive smart-city rollouts and massive consumer IoT adoption. China reported 2.57 billion connected terminals by August 2024, stretching local operators' capacity to authenticate traffic and block botnet activity. Japan's Ministry of Internal Affairs and Communications issued secure smart-city guidelines in 2024, catalysing municipal procurements that embed zero-trust from the outset. South Korea's 6G research includes quantum-resistant key exchange for IoT endpoints, positioning domestic vendors to capture export contracts once standards stabilize. Governments in Indonesia and Vietnam now bundle cyber-hygiene audits into manufacturing incentives, compelling foreign investors to purchase certified security platforms.

Europe leverages regulatory pull rather than raw volume. The Cyber Resilience Act obliges every connected product sold in the bloc to document threat modeling, vulnerability disclosure, and lifelong update policies. Manufacturers outside Europe comply to avoid market exclusion, exporting the regulation's influence worldwide. The United Kingdom's PSTI Act removes default passwords from consumer electronics shelves, enhancing baseline resilience. Germany's Industrie 4.0 projects emphasize deterministic networking secured by IEC 62443 controls, while France's metropolitan data platforms require end-to-end encryption between edge gateways and centralized analytics. Funding from the EU's Digital Europe Programme subsidizes SME adoption of certified security stacks, broadening the addressable market for managed service providers.

List of Companies Covered in this Report:

Cisco Systems / IBM / Broadcom (Symantec) / Palo Alto Networks / Check Point / Fortinet / Microsoft / Trend Micro / Armis / Infineon Technologies / ATandT Cybersecurity / Darktrace / SecureWorks / Rapid7 / Trustwave / Thales / RSA Security / Qualys / Kaspersky / Zscaler /

Additional Benefits:

 The market estimate (ME) sheet in Excel format /
3 months of analyst support /

Table of Contents:

IoT Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-07-01 | 150 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-03
		Signature