

Hardware Encryption Market Set for Significant Growth as Revenue Nears USD 561.63 Million by 2035

Hardware Encryption Market Size, Share and Research Report By Technology (Advanced Encryption Standard, Elliptic Curve Cryptography, RSA Encryption, Quantum

NEW YORK,, NY, UNITED STATES,
August 4, 2026 /EINPresswire.com/ --
The Global [hardware encryption market](#) reached an estimated USD 355.85 Million in 2025 and is projected to grow from USD 371.47 Million in 2026 to USD 561.63 Million by 2035 by

2035, registering a CAGR of 4.70% during the forecast period. Two major catalysts are accelerating this trajectory: the escalating frequency and sophistication of data breach incidents targeting both enterprise and government infrastructure, and the tightening of global data protection mandates including GDPR, HIPAA, and the U.S. Federal Data Encryption Act that are

compelling organizations to move beyond software-only security frameworks. With over USD 200 billion in annual losses now attributed to data theft and ransomware globally, enterprises, cloud providers, and defense agencies face mounting urgency to embed encryption directly at the hardware layer.

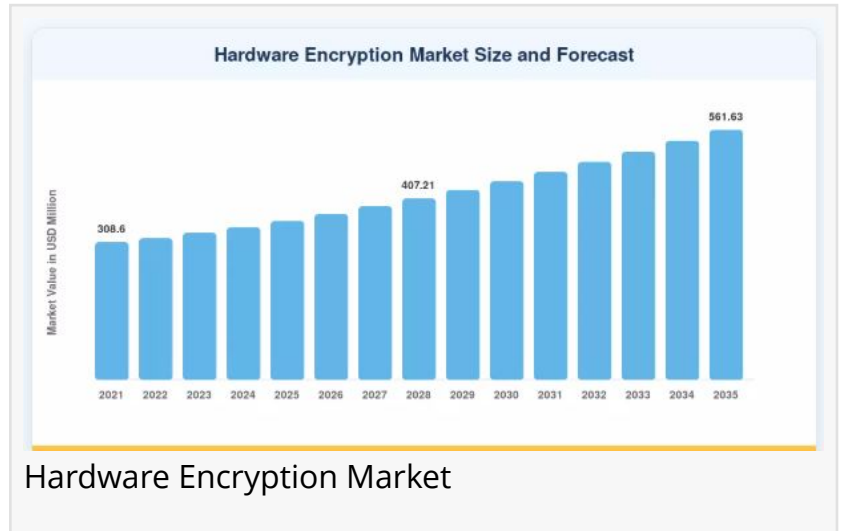
“

Hardware Encryption Market is growing steadily as organizations prioritize robust data security, regulatory compliance, and protection against evolving cyber threats.”

*Market Research Future
(MRFR)*

Legacy software-based encryption solutions vulnerable to side-channel attacks, memory scraping, and firmware exploits are rapidly giving way to dedicated hardware security modules (HSMs), self-encrypting drives (SEDs), and trusted platform modules (TPMs) that perform

cryptographic operations in isolated, tamper-resistant silicon. A recent Gartner security survey estimated that enterprises deploying hardware-rooted encryption architectures alongside zero-trust network frameworks experienced 31–37% fewer successful data exfiltration events than



peers relying exclusively on software controls. This security paradigm shift is not incremental it represents a foundational re-architecture of how organizations protect data at rest, in transit, and in use.

Get Full PDF Sample Copy of Report: (Including Full TOC, List of Tables & Figures, Chart) @ https://www.marketresearchfuture.com/sample_request/4857

□ How Significant Is the Hardware Encryption Market's Growth?

The hardware encryption market has demonstrated consistent and robust expansion, rising from approximately USD 2.18 billion in 2021 to an estimated USD 355.85 Million in 2025, representing a healthy historical growth trajectory. The market is expected to nearly triple over the next decade, driven by accelerating cloud adoption, proliferating IoT endpoints, quantum computing threat preparedness, and the widespread rollout of [5G infrastructure](#) requiring hardened encryption at the network edge.

Rising incidences of supply chain attacks, nation-state cyber espionage, and insider threats across critical infrastructure sectors have created acute demand for silicon-level trust anchors. Financial institutions, healthcare networks, defense contractors, telecommunications carriers, and hyperscale cloud operators are all investing heavily in hardware encryption solutions to enforce data sovereignty, achieve regulatory compliance, and reduce the attack surface exposed to increasingly capable adversaries.

□ What Does the Future Hold for the Hardware Encryption Market?

Post-quantum cryptography (PQC) readiness stands at the forefront of the market's next growth phase. As the National Institute of Standards and Technology (NIST) finalizes its suite of quantum-resistant algorithms including CRYSTALS-Kyber and CRYSTALS-Dilithium hardware encryption vendors are racing to embed PQC-capable accelerators into next-generation HSMs, SEDs, and network encryption appliances. Organizations with long data-retention requirements government, defense, financial services are already procuring crypto-agile hardware platforms capable of algorithm updates without physical replacement.

The growing emphasis on confidential computing protecting data while it is actively being processed is another defining force shaping the market's future. Trusted Execution Environments (TEEs) implemented in hardware, such as Intel SGX, AMD SEV, and ARM TrustZone, are enabling encrypted computation in cloud and edge environments, creating entirely new deployment models for sensitive AI workloads, financial transaction processing, and healthcare analytics.

[Edge computing](#) proliferation is also redefining the hardware encryption deployment landscape. As processing shifts from centralized data centers to distributed IoT gateways, industrial controllers, and autonomous vehicle platforms, purpose-built hardware encryption ICs and

secure elements are becoming mandatory components of the embedded systems architecture expanding total addressable market well beyond the traditional enterprise data center.

Direct Purchase this Research Report:

https://www.marketresearchfuture.com/checkout?currency=one_user-USD&report_id=4857

□ Who Are the Key Players in the Hardware Encryption Market?

The hardware encryption landscape is characterized by a mix of semiconductor giants, specialized security hardware vendors, storage OEMs, and emerging silicon security startups. Key participants shaping the competitive dynamics include:

- Thales Group
- IBM Corporation
- Samsung Electronics
- Seagate Technology
- Western Digital Corporation
- Micron Technology
- Intel Corporation
- Kingston Technology
- Kanguru Solutions
- Maxim Integrated (now Analog Devices)

Competition in the market is intensifying as vendors race to embed post-quantum algorithm support, achieve FIPS 140-3 and Common Criteria EAL4+ certifications, and expand crypto-agile platform architectures capable of adapting to evolving threat landscapes. Strategic acquisitions of key management software firms and partnerships with hyperscale cloud providers are also reshaping the competitive landscape.

□ What Are the Emerging Trends in the Hardware Encryption Market?

Several transformational trends are redefining how the hardware encryption market evolves through 2035:

Post-Quantum Cryptography (PQC) Hardware Readiness: NIST-standardized quantum-resistant algorithms are driving a hardware refresh cycle, with HSM and SED vendors integrating PQC accelerators and crypto-agile firmware architectures to future-proof enterprise encryption infrastructure.

Confidential Computing Expansion: Hardware-enforced Trusted Execution Environments (TEEs) from Intel, AMD, and ARM are enabling encrypted in-use data processing, unlocking new cloud workload security models for AI inference, financial services, and regulated healthcare analytics.

Zero-Trust Security Architecture Adoption: Hardware root-of-trust components including TPM 2.0, secure enclaves, and hardware attestation modules are becoming foundational elements of zero-trust frameworks, shifting security enforcement from the network perimeter to the device and data layer.

IoT and Edge Hardware Security: The proliferation of connected industrial, automotive, and consumer IoT devices is driving demand for ultra-low-power hardware security ICs, secure elements, and embedded encryption processors capable of operating within constrained edge environments.

Regulatory-Driven Hardware Compliance Mandates: FIPS 140-3 certification requirements, NIS2 Directive obligations in Europe, and U.S. Executive Order 14028 on cybersecurity are compelling public sector and critical infrastructure operators to standardize on certified hardware encryption platforms.

Cloud HSM and Bring Your Own Key (BYOK) Growth: Enterprises migrating workloads to multi-cloud environments are increasingly deploying cloud-based HSM services and BYOK/HYOK key management architectures to maintain cryptographic control without sacrificing cloud operational agility.

Get access to the full description of the report @

<https://www.marketresearchfuture.com/reports/hardware-encryption-market-4857>

□ How Is the Hardware Encryption Market Segmented?

The hardware encryption market report provides a comprehensive segmentation framework:

- 1 By Product Type: Hardware Security Modules (HSMs), Self-Encrypting Drives (SEDs), Trusted Platform Modules (TPMs), Encrypted USB Drives, Network Encryption Appliances
- 2 By Algorithm: AES, RSA, Elliptic Curve Cryptography (ECC), Post-Quantum Algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium)
- 3 By Architecture: ASIC-Based Encryption, FPGA-Based Encryption, Embedded Secure Element
- 4 By End-Use Vertical: Banking, Financial Services & Insurance (BFSI), Government & Defense, Healthcare, IT & Telecommunications, Retail & eCommerce, Industrial & Manufacturing
- 5 By Organization Size: SMEs, Large Enterprises, Hyperscale Cloud Operators

□ What Are the Regional Insights from the Hardware Encryption Market?

North America commands approximately 38% of global hardware encryption market share, underpinned by the scale of U.S. federal government encryption mandates, FIPS compliance requirements across defense and intelligence agencies, and the concentration of hyperscale cloud and financial services infrastructure. The region's mature cybersecurity ecosystem and

high enterprise security spending per employee further reinforce its leading position.

Europe holds the second-largest share at approximately 28%, with Germany, the United Kingdom, France, and the Netherlands representing the primary markets. The GDPR's stringent data protection obligations, combined with the NIS2 Directive's expanded scope across critical infrastructure sectors, are compelling European enterprises and public sector organizations to invest heavily in certified hardware encryption platforms with full audit-trail and key management capabilities.

Asia-Pacific represents a rapidly growing region, driven by digital transformation across China, India, Japan, and Southeast Asia, alongside rising cyber threat activity targeting financial services and government networks. National data localization laws and expanding domestic semiconductor manufacturing ambitions in China and India are further accelerating hardware encryption adoption across the region's enterprise and public sector markets.

Middle East & Africa is projected to register the highest CAGR at approximately 11.4% through 2035. National cybersecurity strategies across Saudi Arabia, UAE, and South Africa, alongside Vision 2030 digital infrastructure investment programs, are creating substantial demand for enterprise-grade hardware encryption and HSM deployments across government, banking, and critical infrastructure sectors.

South America rounds out the global picture, with Brazil and Mexico representing the most active markets for hardware encryption procurement, particularly within financial services, telecommunications, and government verticals responding to escalating cyber threat environments.

□□□ Industry Analysis Reports by Market Research Future:

It Asset Reuse Market-

<https://www.marketresearchfuture.com/reports/it-asset-reuse-market-10935>

Non-Destructive Inspection Equipment Market-

<https://www.marketresearchfuture.com/reports/non-destructive-inspection-equipment-market-11068>

Network Engineering Services Market-

<https://www.marketresearchfuture.com/reports/network-engineering-services-market-11087>

Travel Insurance Market-

<https://www.marketresearchfuture.com/reports/travel-insurance-market-11161>

Intruder Alarm System Market-

<https://www.marketresearchfuture.com/reports/intruder-alarm-system-market-11504>

Refurbished Smartphone Market-

<https://www.marketresearchfuture.com/reports/refurbished-smartphone-market-11690>

Signal Generators Market-

<https://www.marketresearchfuture.com/reports/signal-generators-market-11736>

Fintech Technologies Market-

<https://www.marketresearchfuture.com/reports/fintech-technologies-market-11881>

Io Link Market-

<https://www.marketresearchfuture.com/reports/io-link-market-11897>

Capacitor Market-

<https://www.marketresearchfuture.com/reports/capacitor-market-11905>

Sagar Kadam

Market Research Future

+ +1 628-258-0071

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/930758157>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.