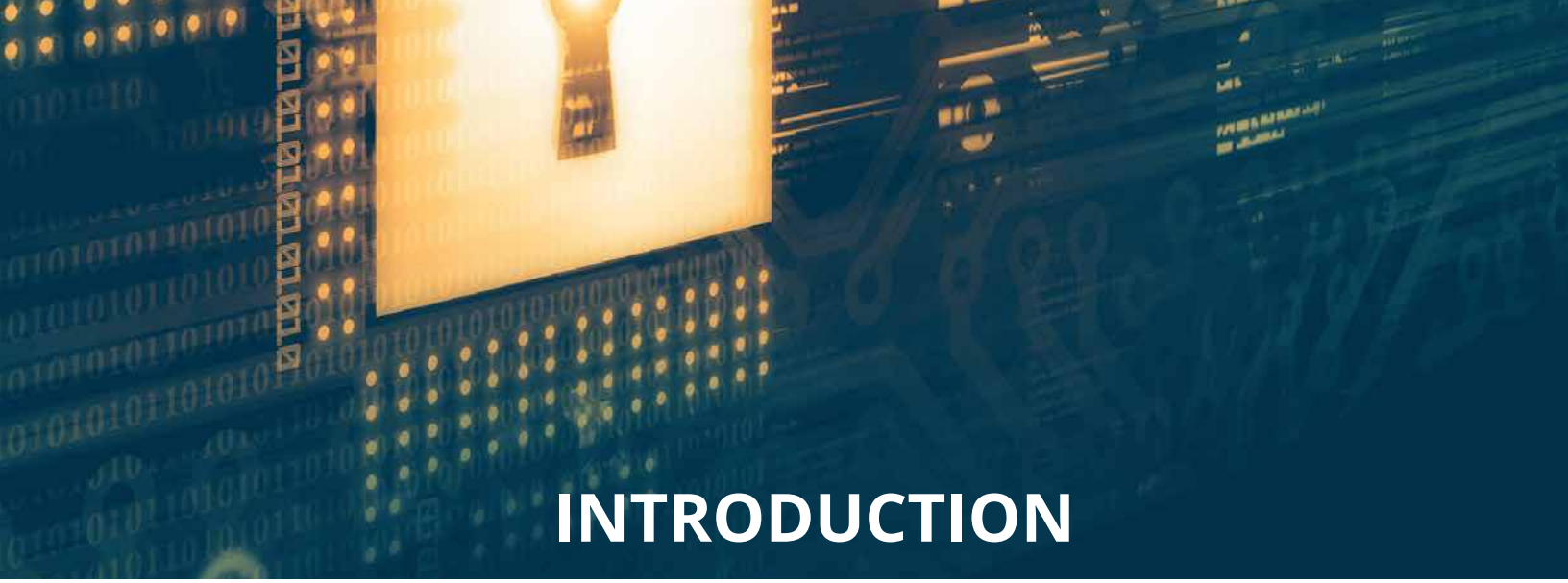
THE STATE OF CYBER & DIGITAL SECURITY

ABIresearch
THE TECH INTELLIGENCE EXPERTS℠



INTRODUCTION

Security is a complex, multi-layered discipline that touches upon many notions: from protection and trust to resilience and offense. In today's connected societies, security needs to permeate all aspects of modern technologies to support successful digital and cyber ecosystems. A weak link in a chain can present an open door to a threat or be at risk from misconfiguration.

Each link, each layer must be secured. And yet the way in which security has been implemented to date varies wildly, impacted by different prerogatives: cost, regulation, technology limitations, market demand. All of these impact security investments to various degrees.

The biggest challenges for security implementation lie in understanding the value of the technology as an enabler and then finding the right solution, before applying it effectively. There is unanimous agreement that security is needed; but where and how and when and to what degree are not as easily determined.

For example, what is the value of digital wallets beyond the smartcard? Which technologies can help secure a soft-wallet most cost-effectively? How can security best be leveraged within a trusted payment ecosystem? Or why is an identity important for a connected object? What is the differentiation that a hardware secure element can bring when compared to just a crypto-processor? What attributes of the chosen hardware security solution can be most efficiently integrated into a public key infrastructure? Or importantly, how will the chip shortage affect the provisioning of smart cards? Which verticals will be affected, in both the short and longer term? What applications will be prioritized and at what cost?

ABI Research understands that security, both digital and cyber, must remain relevant and adaptable to a challenging and complex reality. Especially one that is constantly being shaped by the rapid pace of technology evolution and digital transformation through cloud migration, IoT expansion, 5G rollout, AI advances, improved edge compute and increasing automation.

To help you better understand the state of digital and cyber security in 2022, ABI Research has highlighted key trends and forecasts in a number of sectors, including government, payment, industrial, telco and IoT, and across various form factors from hardware to software. This is complemented with a set of recommendations and action points for product solution and service providers to help navigate the opportunities and challenges of their industries. These insights come from throughout our seven research services and will help you better understand the role and the value of enabling digital and cyber security.

CITIZEN DIGITAL IDENTITY

TREND TO WATCH: GROWING PRESENCE OF MOBILE IDENTITIES

Driven by digital transformation and governments' growing appetites to extend digital platform offerings, significant uptake of mobile identities has resulted. Mobile identities, as a companion to physical documentation, once provisioned digitally via a dedicated application or web-based solution, enhance citizen use cases and allow for Identification (ID) verification using no superfluous citizen data.

Mobile identities have given rise to a number of streamlined implementations both in government and in fields outside of the government context, such as in online finance, and remove the need for in-person verification in such cases, aligning with, and further enabling, mobilization across many industries. As well as solutions involved in the provisioning of a credential digitally, mobile verification and onboarding are equally growing technologies, forming part of a dynamic ecosystem of digital identity applications.

KEY ACTION POINTS

Vendors looking to implement mID solutions should seek to take advantage of existing infrastructure, where databases containing citizens information can be used to issue mobile credentials with ease. Additionally, leveraging the technical features already existing, and progressing, within mobile devices is key for mobile implementation. NFC technology in smartphones can be used to provision a smart document in a more secure manner than photo scans of the credential using the mobile devices camera. The strong biometric scanning capability of smartphones should also be considered, where in many cases, biometric scans on a mobile device match that of dedicated biometric hardware. This is of particular importance in the progression of secure mobile verification, as well as for the furthering of enrollment scenarios and credential reissuance via a mobile device.

Monitoring of developments in mobile networks is important to assess future opportunities and market potential for mobile identities. Where low network coverage is a current limitation, improvements of coverage in locations lacking beforehand gives rise to a broader global market. Where network coverage is sufficiently strong, mID can be permanently accessible. Likewise, development in blockchain and distributed ledger technologies should also be on the radar of mID players. This enables a more secure and tamper-proof backend system if utilized instead of existing alternatives, where replacing the use of hardware secure elements (SEs) negates some costs.

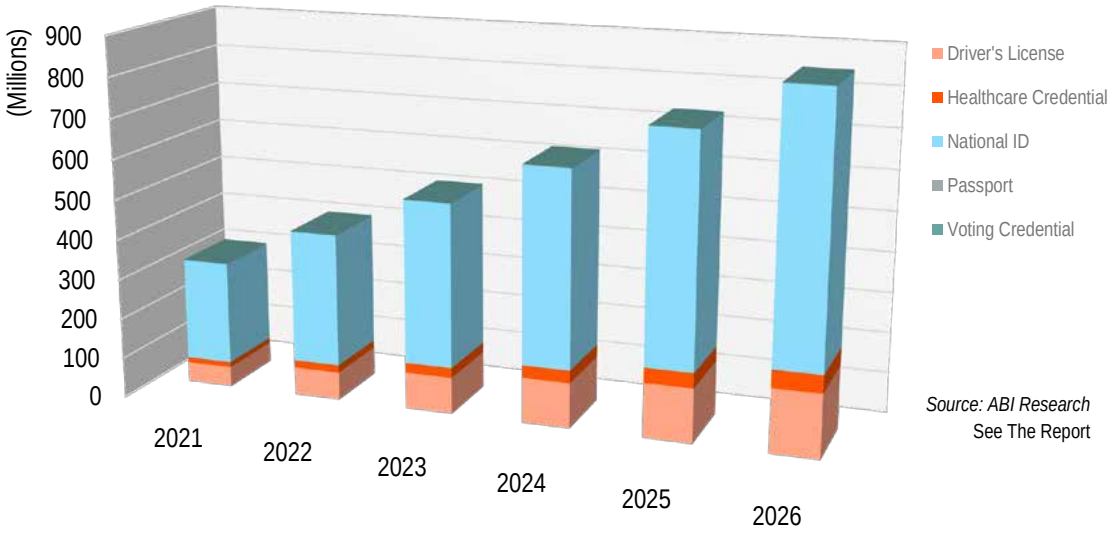
TREND TO WATCH: PHYSICAL DOCUMENTATION MOVEMENT TOWARDS POLYCARBONATE

The use of polycarbonate (PC) in the manufacturing of ePassports is growing, with ABI Research noting a tendency of governments moving toward PC in new credential projects in favor of alternative materials. The main driver of this migration is the increased physical security associated with a PC data page, which is structurally more difficult to delaminate, thus more difficult to tamper with, and additionally opens the door to more advanced personalization techniques. The enhanced security of PC documents paves the way to a more reliable ID infrastructure that is beneficial to citizens and governments alike, where processes like entry and exit in airports can be enacted in a more streamlined manner with less risk of a fraudulent identity.

KEY ACTION POINT

As PC migration increases further, ID players must ensure their solution offerings align with the changing market and reflect increasing PC demand requirements. From a research and development perspective, migration to PC is being augmented by developments in color-laser personalization. Smart card vendors and credential personalization solutions providers should seek to continually expand the total market available to them by increasing the accessibility of their solutions. This involves modularization of color-laser solutions to ease the installation process, and working to reduce ASPs of such solutions, including changeable laser images (CLIs) and Multiple Laser Images (MLIs).

MOBILE IDENTITIES AND DERIVED CREDENTIALS IN GLOBAL CIRCULATION



Source: ABI Research
See The Report

ABI Research's Citizen Digital Identity coverage provides critical insight into the domain of government to citizen issued identity credentials.

FEATURED FORECAST

The number of mobile identities in circulation is expected to grow rapidly. For the 2021 to 2026 period, ABI Research forecasts a 21.9% Compound Annual Growth Rate (CAGR), from an "in circulation" base of 319.1 million in 2021 to 857.6 million in 2026.

This growth is a result of significant expansion of digital platforms by governments concerning citizen credentials, enhancing many use cases and aligning with the general digital transformation across many industries and the mobile verification requirements within these. At present, mobile identities primarily consist of digital companions to physical documentation, provisioned via a dedicated application or web-based solution.

RELATED RESEARCH

Government and Healthcare ID Cards Market Data

The Impact of the Global Chipset Shortage on Citizen Digital Identities

Government and Healthcare ID IC Technologies

CYBERSECURITY APPLICATIONS

TREND TO WATCH: THE UNLOCKING OF THE HARDWARE SECURITY MODULE (HSM) MARKET

Driven by digital transformation strategies, cloud migration, IoT expansion, and increased regulation, the HSM market is going through some turbulent changes. A traditionally closed and niche market selling high-value black-box technology, it is now opening up and witnessing new revenue opportunities. New industry demands in fintech, IoT manufacturing, and cloud security are pushing for new delivery models (service-based, flexible, and modular). This is also enabling new market entrants to challenge the status quo, creating a vibrant and competitive dynamic in the HSM space.

KEY ACTION POINT

New market opportunities means increased competition; incumbents have to respond quickly to the innovation presented by new entrants. A first place to start is understanding new sectoral demands: IoT manufacturing, automotive V2X, smart meter infrastructure and blockchain applications. Next is opening up that traditional black-box: abstracting the hardware layer to offer modular software offerings and API options, or transitioning to an opex-based model for clients through cloud based service propositions for payment or root-of-trust injection. HSM OEMs in particular need to focus on the innovation that they can bring to the underlying foundation on which those appliances are built and which cannot be easily replicated by new entrants like hyperscalers and cloud providers, i.e. implementation of cryptographic algorithms and development of the internal security architecture.

TREND TO WATCH: THE EMERGENCE OF NEXT-GENERATION CRYPTOGRAPHY

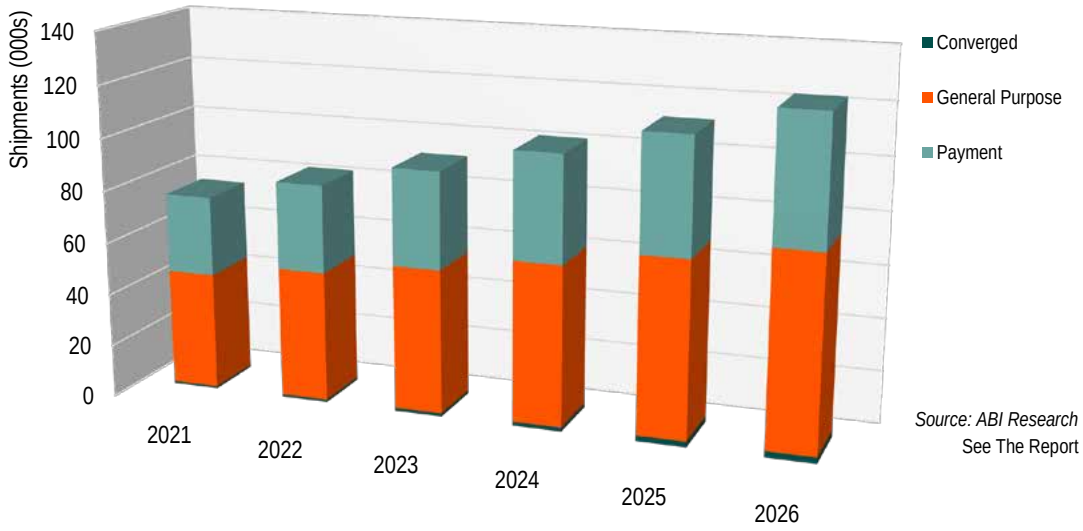
The concern with quantum-safe technologies is becoming a high priority as the advent of attack-capable quantum computers emerge on the horizon. The imminent release of draft quantum-resistant cryptographic algorithms (known as Post-Quantum Cryptography (PQC)) by the U.S. National Institute of Standards and Technology (NIST) has security and technology vendors on the starting line, ready to integrate and deploy them in their product lines. The eventual standards will significantly reshape the cryptographic status quo, as the world transitions from classic crypto to quantum-safe algorithms. In turn, this is driving the consulting opportunity for advising on PQC migration strategies, and especially within financial, government, and enterprise markets.

KEY ACTION POINT

For OEMs with devices that will be out in the field for more than 10 years, it is imperative to start integrating quantum-resistant technologies as soon as possible. Most semiconductors should already have a strategy in place and done preliminary research and testing of PQC algorithms with some of their products. OEMs should be identifying those semiconductors and software developers that will enable them to integrate PQC and quantum-resistant protocols and libraries. Service providers should be ensuring their underlying infrastructure is crypto-agile, so as to transition fairly quickly to hybrid and PQC technologies once the standards are finalized. All should be paying close attention to the international standardization processes and to national recommendations publishing on PQC to ensure they align themselves accordingly.

CYBERSECURITY APPLICATIONS

HSM GLOBAL SHIPMENTS BY APPLICATION



Source: ABI Research
See The Report

ABI Research's Cybersecurity Applications coverage looks beyond the device itself to explore how trusted device solutions and related security technologies can protect data, networks, cloud platforms, infrastructures, and service offerings.

FEATURED FORECAST

The HSM market is expected to grow at a stable, double-digit CAGR of 10% for the 2021 to 2026 period. From a shipment base of 75,000 in 2021, ABI Research expects total shipments to reach 125,000 by 2026. The most significant trends are the slow, but incremental merging of HSM applications. Traditionally split into payments and general purpose, the flexibility and modularity increasingly in demand from the market is driving abstraction of the underlying hardware in favor of firmware and software-based differentiation, which also plays well to HSM-as-a-Service propositions. The greatest growth rate is attributed to converged HSM formats (even though overall numbers represent a fraction of the Total Addressable Market (TAM)), whereby both payment and general-purpose functionalities reside on the same hardware. In general, the HSM market is set for a sustained and positive growth outlook over the next 5 years, with plenty of new business opportunities driving demand.

RELATED RESEARCH

Secure Data Management in Automotive Telematics

Blockchain and Distributed Ledger Technology

Critical Infrastructure Security

DIGITAL PAYMENT TECHNOLOGIES

TREND TO WATCH: NEXT-GENERATION PAYMENT CARDS ARE HERE

The biometric payment card is gaining ground in global markets and key pilot programs are now fully active. Key players in the ecosystem are working toward a common goal in terms of readying for mass production and significant volume orders. Significant ecosystem efforts continue to be placed on expanding partner ecosystems, targeting Tier Two smart card vendors to add biometric payment cards to their respective portfolios, as well as payment network certification. On top of this is a continuation in developing next-generation products and architectures, improving integration to help reduce card manufacturing complexities and reduce components with the ultimate goal of achieving a significant ASP reduction.

KEY ACTION POINT

As a recommendation, to truly unlock the potential of the biometric payment card, vendors must pay close attention to remote enrollment solutions. Remote enrollment is a critical pillar that will drive stronger growth and uptake of the solution, with a focus on the standardization required in order to bridge the gap. Secondly, Fintechs forge strategic partnerships with lower-tiered smart card vendors and utilize them to launch an end-to-end service from card creation to personalization. The issue with this is that neo and challenger banks cannot sustain the necessary higher issuance levels required to grab the attention of many of the Tier One smart card suppliers, while many Tier Two and Tier Three vendors do not have the biometric payment card solutions within their product portfolios. An opportunity remains to assist lower-tiered smart card vendors integrate biometric payment card products into their respective product portfolios.

TREND TO WATCH: CENTRAL BANKS EMBRACING DIGITAL CURRENCY

The digitization of a country's fiat currency involves the central bank of the economy in question issuing electronic tokens, instead of the usual process of minting coins and printing paper bills. There can be no doubt that recent years have seen the concept of Central Bank Digital Currencies (CBDCs) explored with great intent by many global economies. Many governments across the world are exploring the drivers and pain points of issuing a digital currency. While the majority of these are currently only in the prospective phase, a number of active trials have begun and concluded, with many more on the way.

KEY ACTION POINT

CBDC's operate in a somewhat liminal space at the present time, somewhere between a national and unregulated monetary system. As such, there are several factors to consider in their use. Firstly, currencies should be issued without infringing upon the mandates of the central banks and also must meet stringent standards of privacy, transparency and accountability for protection of user data, something which is increasingly critical in the current year. Central banks must shoulder the responsibility of leveraging gathered data on payment habits and trends to better understand the role a CBDC would play in filling the gaps both in normal times and in times of struggle, such as during the COVID-19 pandemic, and should set the operational requirements to deliver a CBDC solution that ensures trust, interoperability, and scalability.

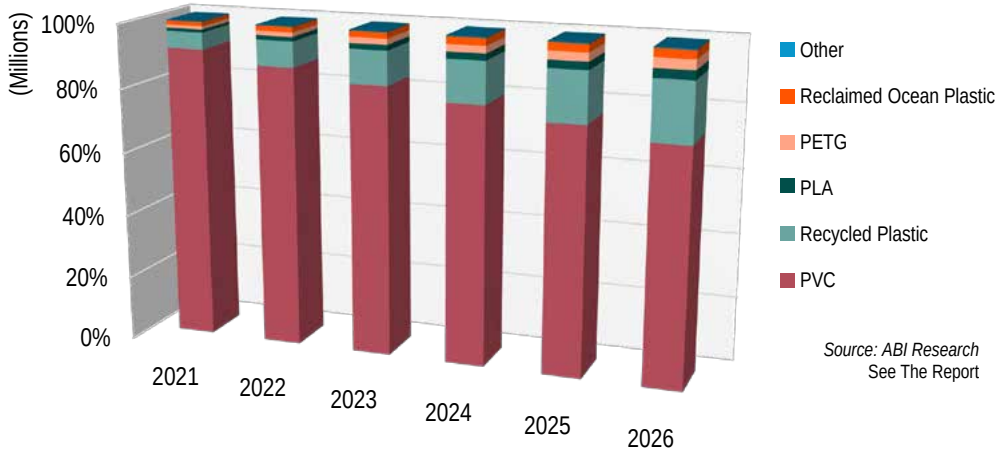
TREND TO WATCH: FOCUS ON SUSTAINABILITY

The increase in sustainable banking and the drive toward more sustainable materials is a telling indicator about the values that are held in high regard in modern society and especially around what banks looking at their Environmental, Social, and Governance (ESG) goals need to do to earn the trust and loyalty of today's conscious consumers. The ever-growing expectations of ecologically-conscious consumers are forcing financial institutions to examine how to implement a new future for the payments market as it relates to innovation in new services and practices.

KEY ACTION POINT

While alternative materials have seen significant developments over the past few years, there is still the presence of greenwashing around "biodegradable" substrates and other offerings. When incorporating alternative materials into a payment card portfolio, smart card vendors and issuing banks must ensure it is being accurately represented and perform due diligence around educating potential customers about which material will best fit the requirements to avoid the risk of further wastage down the project roadmap. Also, while the majority of the focus so far has been placed heavily on the card material, with a significant push toward materials like rPVC and PETG; this is only one side of the coin. Reducing reliance on first-use plastics only has a lasting impact if that plastic is kept out of a landfill. This issue is made worse by the lack of universal regulation in the industry to manage end-of-life smart card offerings. Players active in the space should explore the option of setting up intermediary recycling and disposal programs closer to the card issuers to reuse as much waste material as possible at a proximity location to reduce the need for transportation.

TOTAL PAYMENT CARDS GLOBAL SHIPMENTS BY MATERIAL



Source: ABI Research
See The Report

ABI Research's Digital Payment Technologies service provides in-depth content covering current and future payment methods and the acceptance of technologies that will shape the future payments market.

FEATURED FORECAST

Recycled PVC (rPVC) will become the largest replacement for first-use PVC in the payment card market, especially in Europe, where the presence of a high number of major card vendors, such as Thales, IDEMIA, and Giesecke+Devrient (G+D) have established rPVC as a mainstay material. Driven by large issuing banks in Europe and spreading across all regions, the convenience, price point, availability, and integration with existing personalization infrastructure will lend itself well to seeing rPVC shipments increase from 177.5 million shipments in 2021 to 638.0 million in 2026.

With a higher recycle rate and less environmentally toxic manufacturing and disposal process than PVC, coupled with a more accessible price point than Polylactic Acid (PLA), Polyethylene Terephthalate Glycol (PETG) has found a niche in the payments card market, growing from 33.1 million shipments in 2021 to 105.1 million in 2026.

PLA has also seen higher growth than originally anticipated. ABI Research forecasts PLA to increase from 31.7 million shipments in 2021 to 97.1 million in 2026. Reclaimed and ocean-bound plastic will see the majority of its growth in the North American region, where there is a higher appetite for the material among card issuers and consumers. Championed by CPI Card Groups offering of the Second Wave card, reclaimed and ocean-bound plastic cards are very appealing from an end-user perspective, due to the removal of waste plastic from the environment, though smaller card vendors may struggle with unstable supply chains of raw materials. Nevertheless, reclaimed and ocean-bound plastic cards will see shipment volumes increase from 44.7 million in 2021 to 89.9 million in 2026.

RELATED RESEARCH

Biometric Payment Card Developments, Projects and Market Opportunities

Alternative Solutions for Sustainability in the Payments Market

Payment and Banking Card Technologies Analysis

INDUSTRIAL CYBERSECURITY

TREND TO WATCH: THE EMERGING VENDOR ECOSYSTEM FOR SUPPLY CHAIN MANAGEMENT PROTECTION IN OPERATIONAL TECHNOLOGY (OT)

While asset visibility and protection are increasingly maturing technologies for industrial operators, the secure management of the OT supply chain is still nascent. Third-party risk management and supply chain governance are emerging disciplines, with new solutions focused on due diligence exercises, regular audits, security assurance plans, Firmware Over-the-Air (FOTA) update integrity, and access management for suppliers and service providers. In large part, these concepts are directly tied to improving industrial operators' overall cyber resilience and are part and parcel of lifecycle management of assets, networks, and operations that comes with Industry 4.0 integration.

KEY ACTION POINT

For industrial OEMs, the key is to apply security assurance mechanisms in their dealings with all supply chain partners: contractors, all Tier parts suppliers, service providers, and resellers. Ensuring integrity and attestation of the various components is important both at manufacture, and post-production and throughout the device's lifecycle. OEMs are well placed to be integrating secure OT supply chain technologies as these are lucrative marketing propositions for industrial operators faced with rising threats and costly liabilities.

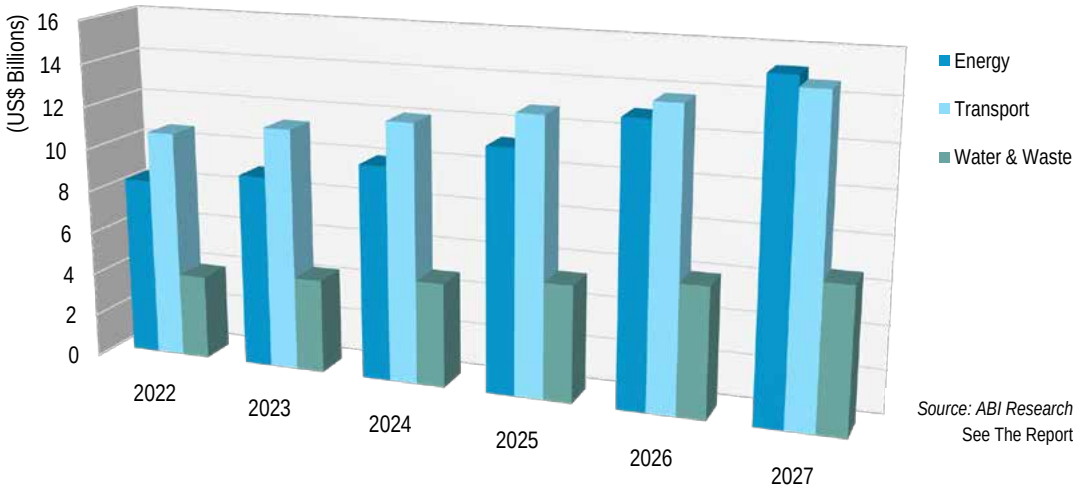
TREND TO WATCH: CRITICAL INFRASTRUCTURES PRIMED TO ADOPT ENABLING CYBERSECURITY SOLUTIONS

Industrial operators are increasingly incorporating disruptive technologies in their migration to Industry 4.0, driving better appreciation of cybersecurity requirements for cyber-physical systems, Industrial IoT (IIoT), smart production, and additive manufacturing, among others. This demand is having a knock-on effect on industries classed as critical infrastructure, where the transition to Industry 4.0 is slower, and cybersecurity continues to rely on traditional Information Technology (IT) security toolsets to protect OT (i.e., remote access management, OT asset inventory, industrial firewalls, etc.). However, the emergence of Artificial Intelligence (AI) and Machine Learning (ML), automation, and orchestration to enable new security applications, such fast user switching, hot patching, Industrial Control System (ICS) cloudification, network probes, and secured Programmable Logic Controller (PLC) programming, are slowly but surely appealing to critical infrastructure operators.

KEY ACTION POINT

OT cybersecurity providers need to ensure they have differentiated product solutions and service offerings for the various critical infrastructures, as they are guided and shaped by distinct regulatory and standard requirements. They are also at differing levels of Industry 4.0 adoption, and therefore the priority of protecting legacy vs smart assets can vary wildly. On the slower to transition sectors, vendors will have to have more specialized knowledge regarding proprietary control systems, while in those industries with smarter infrastructure, focus should be on the new capabilities offered by secure microcontrollers (e.g. trusted execution environments) for example or the security mechanisms inherent in 5G networks (e.g. mutual authentication).

INDUSTRIAL CRITICAL INFRASTRUCTURE GLOBAL SECURITY SPENDING BY SECTOR



Source: ABI Research
See The Report

ABI Research's Industrial Cybersecurity service takes a deep look at how digital security can be applied for Industry 4.0 systems and processes.

FEATURED FORECAST

Global cybersecurity spending in industrial critical infrastructure sectors (e.g., energy, transport, and water & waste management) is expected to hit US$23 billion by the end of 2022, but will grow over the forecast period at a CAGR of 10%. While the transport sector is the most advanced in terms of integrating and deploying cybersecurity tools, the pandemic has slashed budgets and cut investment in the sector.

The industry most affected going forward, however, will be the energy sector. The current armed conflict between Russia and Ukraine is forcing Western countries to wean themselves off oil & gas, and accelerate the transition to more sustainable energy, a plan that had been on their climate change agendas, albeit on a much longer phase-out timescale. This is set to directly impact cybersecurity, both in oil & gas initially within the context of the war and going forward in securing the energy transition and new modes of electricity generation.

RELATED RESEARCH

Industrial Blockchain and Distributed Ledger Technologies

Critical Infrastructure Security: Industrial Cybersecurity

IoT CYBERSECURITY

TREND TO WATCH: OPTIMIZING DATA SECURITY IN TELEMATICS TO ENABLE INTELLIGENCE-DRIVEN MONETIZATION

Secure data management for automotive telematics is becoming increasingly important for vehicle manufacturers (VMs), Tier One suppliers, telcos and insurance companies. Almost every aspect of the software-defined vehicle is set to include constantly evolving cybersecurity technologies at the hardware, software and network level, with telematics data security being one of the core operations. The drive to increase reliability of telematics data, understand how to better monetize it and enable intelligence-driven autonomous vehicle operations is fueling vehicle digitization, fleet management and Vehicle-to-Everything (V2X) applications. In the telematics security market this is reflected through the steady evolution of telematics control units (TCUs) and the networking functionalities they enable.

KEY ACTION POINT

Services for secure data management in connected vehicle telematics is vital to further hone intelligence operations and unlock the V2X horizon for VMs. Security service providers need to carefully align with the VMs objectives around functional safety and physical security. This can enable new IoT security monetization streams in connected vehicles through the offer of identity and access management and secure communications. Cloud security providers need to develop security-optimized fleet management platforms offering various levels of device lifecycle management based on encryption credentials available in TCUs. For higher-tier applications this can extend to the development of more sophisticated vehicle-specific security operation centers (SOCs). Embedded hardware vendors can help shape the market by developing unique value propositions around Embedded Subscriber Identity Modules (eSIMs), Trusted Platform Modules (TPMs) and Hardware Security Modules (HSMs), adapting their products to future connectivity needs based around data collection (e.g. speed, location, mileage, etc.) to tackle in-vehicle data management and to secure Firmware Over-the-Air (FOTA) updates for TCUs.

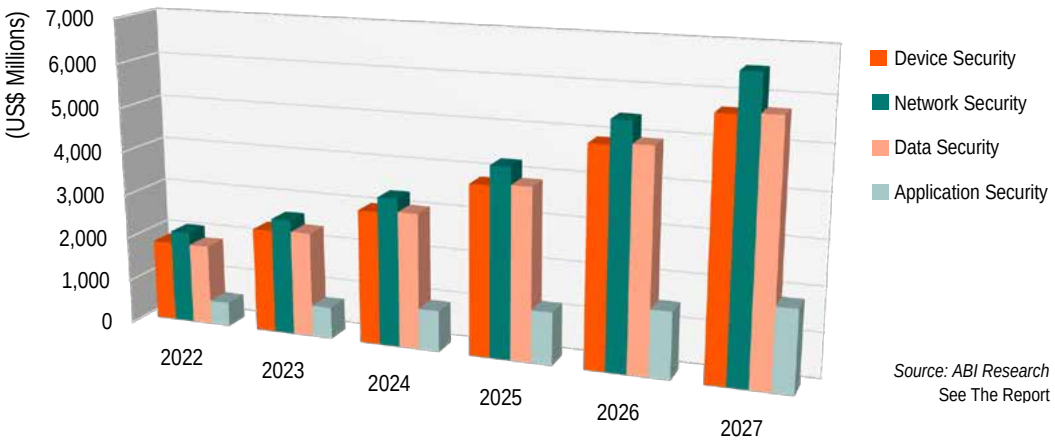
TREND TO WATCH: SECURE SMART ELECTRICITY METERING

The growing deployment of smart electricity meters worldwide due to the transition toward Advanced Metering Infrastructure (AMI) is increasing secure device identity management demands for cellular and Low-Power Wide-Area (LPWA) smart meters.

KEY ACTION POINT

Cloud providers can offer cybersecurity value propositions to utilities for their smart meters by offering a wide array of digital certificate and device lifecycle management options, including Certificate Authorities (CAs) and Public Key Infrastructure (PKI) services. On the other hand, for utilities opting for on-premise smart metering management, the opportunity is for identity and access management providers to offer dedicated solutions around device lifecycle management software, as well has secure hardware OEMs (such as HSM providers) to offer products for encryption key generation and management.

IoT CYBERSECURITY REVENUES BY TECHNOLOGY



Source: ABI Research
See The Report

ABI Research's IoT Cybersecurity service focuses on the secure design, development, operation, and management of devices, platforms, and services in IoT markets.

FEATURED FORECAST

Wide-Area Network (WAN) IoT connections, including cellular 2G, 3G, 4G, 5G, analog fixed line, LPWA Long Term Evolution (LTE), LPWA proprietary, and satellite-connected IoT, are expected to generate the primary concentration of security revenue versus non-WAN connections (Bluetooth, Wi-Fi, or 802.15.4). The amount of IoT security revenue, however, is not always correlated with the amount of IoT connections and some markets are expected to experience disproportionate revenue. This is due to the multi-faceted level of security and management requirements that provide the foundation for other key operations and valuable services, including for intelligence operations and analytics, lifecycle management and predictive maintenance, firmware updates, and device and data integrity.

Device security revenue will be primarily attributed to secure device provisioning and management followed by encryption and hardware security services (secure Root of Trust (RoT), bootstrap, System-on-Chip (SoC) secure firmware, and eSIM management). Additionally, most markets will be subject to increased oversight and data protection endeavors by IoT vendors, partly due to established IT-borne regulations crossing over slowly to the IoT like the European Union (EU) General Data Protection Regulation (GDPR) and the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), but also due to increased mobility from policy makers and standardization entities like NIST and the International Organization for Standardization (ISO). Data security will be driven primarily by secure data hosting/storage, compliance, and data management/governance. Security analytics and data privacy/anonymization services will also see an increase in more user-focused IoT markets.

RELATED RESEARCH

Digital Authentication and Embedded Security: IoT Cybersecurity

IoT Security Services in Electricity Utilities

Secure Data Management in Automotive Telematics

TELCO CYBERSECURITY

TREND TO WATCH:
THE DRIVE TOWARD EMBEDDED CELLULAR CONNECTIVITY CONTINUES

With the hyper-connected world on the horizon, the drive toward embedded cellular connectivity continues, served via Subscriber Identity Module (SIM) form factors, such as eSIM and Integrated SIM (iSIM). From consumer electronics, cutting across a variety of device types from smartphones, tablets, laptops, and wearables to myriad Machine-to-Machine (M2M) and IoT applications, including smart meters, asset trackers, and automobiles, cellular connections are significantly on the increase and how these connections are being activated, managed, and serviced is transforming.

SIM hardware vendors are shifting business models and dynamics, moving away from one-off revenue streams associated with SIM card supply, toward reoccurring revenue models driven by eSIM management platforms to manage the complete lifecycle of devices and things from first activation to end of life.

KEY ACTION POINT

With further emphasis being placed on the eSIM, thanks to its remote provisioning and life-cycle management capabilities, vendors who have yet to make the required investments into eSIM need to do so. Although the traditional removable SIM market will bounce back, it will likely only be a momentary recovery and a second market impact wave should be expected, once the eSIM becomes more prominent.

TREND TO WATCH:
THE DRIVE TOWARD EMBEDDED CELLULAR CONNECTIVITY CONTINUES

Ecosystem players have been extremely proactive in developing end-to-end contactless enrollment and activation methods via fully digitized approaches, as well as looking toward both the M2M and consumer eSIM specifications, and merging the best of both worlds to enable full connectivity and Over-the-Air (OTA) management capabilities on device types without an interface, while enabling the use of Mobile Network Operator (MNO) Subscription Manager-Data Preparation (SM-DP) infrastructure.

KEY ACTION POINT

The development and support of new converged consumer and M2M eSIM specifications cannot be underestimated. The ability for a service provider to utilize existing SM-DP infrastructure will significantly break down market entry barriers, specifically related to the required infrastructure investment cost and create a scenario whereby cellular enablement becomes more viable. Vendors active in the support and management of eSIM profiles, activation and lifecycle management will need this capability within their wheelhouse in order to unlock and accelerate IoT cellular enablement opportunities.

TREND TO WATCH:
THE DRIVE TOWARD EMBEDDED CELLULAR CONNECTIVITY CONTINUES

As the eSIM market increases, the removable SIM card market remains a challenge and a market in which the challenges are becoming increasingly more evident. Although the impact of eSIM is yet to truly make itself known on the removable SIM card market, the impact is considered inevitable. Paired with the shorter-term chip shortage challenge means that ecosystem players are having to react, looking extremely closely at their SIM strategies, supporting services, and product portfolios, as the pressure on manufacturers and SIM card sourcing continues.

KEY ACTION POINT

The rise of the chipset shortage has raised a number of questions and strategy shift requirements. Although adding to an already challenged market, it is a great opportunity for smart card vendors to reassess the markets to which they are active. They may opt out of lower end opportunities in order to focus on more profitable sectors. Alongside this is the ability to further pivot towards the reoccurring revenue streams associated with eSIM.

In addition, the chip shortage is beginning to create a market supply imbalance, with a future prospect of some IC vendors exciting the SIM cards market, which should be tackled by not only increasing IC/foundry relationships, but increased emphasis on in-house SIM chip design in order to reduce reliance on IC vendors and place SIM card manufacturers in the strongest possible position.

Finally, MNOs need to use the chip-set shortage to audit themselves and use as an opportunity to streamline processes related to SIM card inventory management alongside eSIM readiness and at the same time accelerate eSIM readiness and support. New connections should now utilize the eSIM, with new customers offered eSIM activation. This will help reduce the likelihood of an MNO not being able to replace or supply a removable SIM card and reduce market strain and help minimize operational disruption.

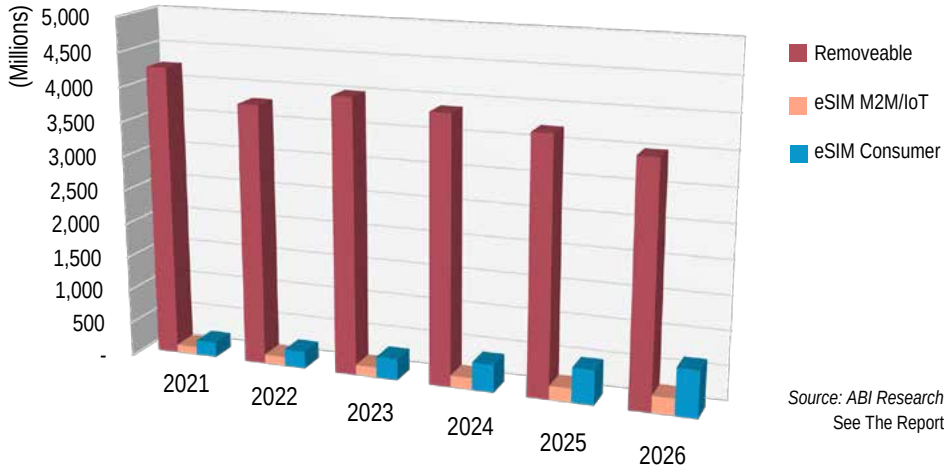
TREND TO WATCH:
THE ADVENT OF 5G NETWORKS

For operators, targeting new enterprise markets, through slicing or private networks, will mean that they have the opportunity to offer tailored network security solutions for the wide variety of use cases that will present themselves in Ultra-Reliable Low-Latency Communication (URLLC), Enhanced Mobile Broadband (eMBB), and Massive Machine-Type Communication (mMTC). This also provides an opportunity for third parties, from network equipment operators to pure-play cybersecurity vendors, to start targeting enterprise customers in this 5G telco space.

KEY ACTION POINT

Operators will face stiff competition in a cloud-native, API-based software-defined telco network from hyperscalers, network equipment providers, and also pure-play cybersecurity providers. They can leverage the sunk security costs that were part of the capex when building out the networks to offer services and cloud solutions. But that will require operators to implement new processes (Shift Left and CI/CD methodologies) and the training and acquisition of new talent (e.g. software developers as opposed to network engineers). Security assurance of third party providers, as well as continuous risk assessment and threat intelligence will also need to be regularly and continuously applied to these new enterprise security offerings.

GLOBAL EMBEDDED SIM VERSUS TRADITIONAL REMOVEABLE SIM SHIPMENTS



Source: ABI Research
See The Report

ABI Research's Telco Cybersecurity service explores security technologies in new radio, telco cloud and the mobile edge for communication infrastructure and operations.

FEATURED FORECAST

The SIM card market is expected to remain relatively stable, albeit a declining market from a removable SIM perspective, counterbalanced by the growing presence of eSIMs.

The market trajectory for the removable SIM card market has already been defined and the chip shortage impact will only exacerbate the situation as OEMs continue on their path of eSIM integration to enable out-of-the-box and digital-first activation strategies and MNOs accelerate their respective support for eSIM platforms.

Over the course of the forecast period, these dynamics are expected to have an impact on removable SIM supply, forecast to decrease from 4.18 billion in 2023 to 3.95 billion in 2026. Overall, the reductions in removable SIM card demand will be offset by eSIM issuance across the consumer and M2M markets, which is forecast to reach more than the 872 million by 2026, resulting in a market capable of achieving a minor CAGR of 0.2% between 2021 and 2026.

The SIM market is transforming and evolving at an accelerated rate. A combination of market challenges related to the removable SIM is paired with significant opportunities from an eSIM perspective. Ecosystem players need to look closely at their respective strategies as they relate to SIM card product portfolios, relationships with customers, allocation, supplier collaboration, and inventory management processes to ensure minimized operational impact driven by the chipset shortage, while preparing and building upon operations related to eSIM/iSIM and digital-first approaches.

RELATED RESEARCH

Network Transformation with Secure Access Service Edge and 5G

SIM Card and eSIM Market Overview and Chipset Shortage Analysis

SIM Card ICs

TRUSTED DEVICE SOLUTIONS

TREND TO WATCH:
SMART CARDS CONTINUE TO BE A CHALLENGING MARKET

The market continues to be one of challenge and limited growth opportunity, given the largely saturated and mature nature of large-scale volume opportunities, most notably within the SIM and payment card markets. However, the high levels of market maturity are just one underlying market factor, which is being further exacerbated by the increase in embedded form factors used to enable applications like mobile payments via Near Field Communications (NFC) and secure element functionality, and digital MNO network profile delivery and management, as is the case with eSIM. Digitization remains a key theme and the drive toward this and subsequent growing demand for embedded form factors is creating market tension and worry that the rise of digital may mean, at some point, the beginning of physical smart card dematerialization.

KEY ACTION POINT

Despite the clear trend towards digitization, smart card and secure IC vendors need to be mindful before pulling the plug on physical card solutions or diverting significant investments away from the physical in favor of the digital and embedded. In many instances the primary identity or token is bound to the physical and then digitized to the digital, creating a scenario whereby the digital is a companion to the physical. This is especially true for the identity and payments markets and for this reason a market-by-market assessment is required before executing on possible physical market exit strategies, with the physical remaining a strong market element for many years to come.

TREND TO WATCH:
THE IMPACT OF A REMOTE WORKFORCE

The pandemic changed the way businesses operate, with remote working continuing in many regions and across sectors. While there is a gradual return to work, it is clear that many will not return to the same working norm that dominated pre-pandemic. Investments and acceleration in digital transformation strategies have made businesses more flexible from this perspective. Distributed working environments affect both workers and assets (IT, OT, and the IoT). Secure connectivity and identity management have become key priorities in disparate and heterogenous networks. All these elements are driving demand for hardware security.

KEY ACTION POINT

OEMs in particular will need to adapt email and network security tools that were targeted for on-premise use in server rooms and data centers so that they can be leveraged in remote desktops settings of home workers. From a cost perspective, security software alternatives will be used instead of actual appliances. But in the case of regulated or safety-critical sites, then smaller form factors will be required (modem-sized appliances or USB-type form factors). For semiconductors specifically, they will need to determine the demand for secure hardware by closely following application demand; e.g. secure key storage for identities or secure execution environments for crypto acceleration, etc.

TREND TO WATCH:
THE CHIP SHORTAGE FALLOUT

On top of accelerating digitization is the chip shortage impact, which is a continuing theme, and an impactful challenge across all security hardware component markets, as it relates to the manufacture, supply, allocation processes, and significant increases to chip ASPs. Although a relatively new challenge and one considered a by-product of the COVID-19 pandemic, the timeline to a "business as usual" scenario is not clear cut, and all ecosystem players are looking extremely closely at the chip shortage and how strategies can be put in place to help minimize operational impacts.

KEY ACTION POINT

This fallout means that strategies which reduces reliance on single IC vendors and/or foundry are of paramount importance and the striking of new supply deals, adopting a multi-sourcing policy a must. Although this may take months, if not years to implement, it will help mitigate any future supply problems, help with future buying power, and help bring ASPs back to nominal levels more quickly.

In order to minimize shorter term market disruption, communication between chip and smart card suppliers and their end customers need to be proactive, rather than reactive. Communication efforts between secure IC, smart card and their customer bases should be externed and enhanced, and regular and transparent conversations related to required demand vs what is available clearly communicated.

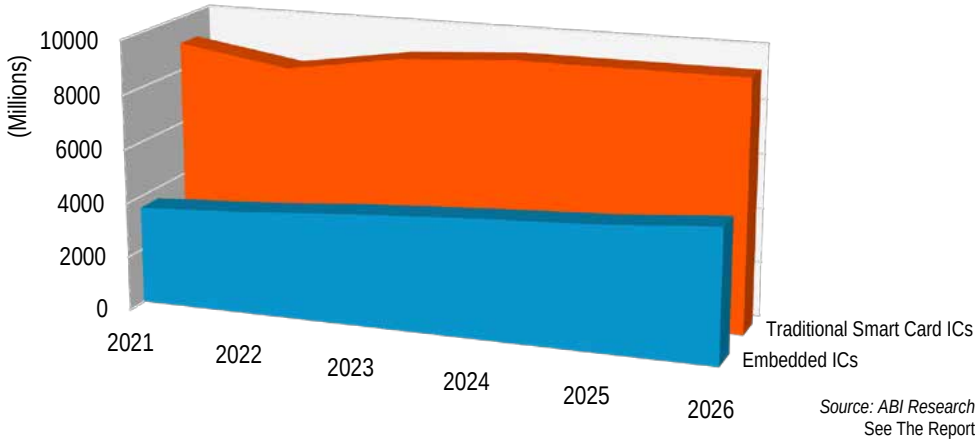
TREND TO WATCH:
A MIXED BAG FOR BIOMETRIC TECHNOLOGIES

The pandemic had a detrimental effect on the market for contact-based biometric technologies, accelerating the transition toward contactless solutions. This fast-tracked the adoption of face recognition technologies across enterprise and commercial applications, pushing developers to sharpen their algorithms and greatly increase their accuracy. However, fingerprint-based recognition remains the standard across government, border control, and law enforcement, all of which are bolstered by the expansion of Automated Biometric Identification Systems (ABIS), biometric databases, and registries.

KEY ACTION POINT

Biometrics players in pursuit of new governmental projects should be aware that budgetary restrictions may appear as an immovable force that hinders negotiations - especially between system integrators and governments. However, legacy considerations and system obsolescence in governmental and law enforcement biometric platforms is a serious concern for intelligence and security agencies that drives investment. Biometric vendors need to be aware of governments objectives which operates in a multi-vendor environment and consider avoiding vendor lock-in through the adoption of open architecture standards for ABIS, developing scalable and interoperable solutions, reducing platform TCO and lowering yearly maintenance costs without sacrificing system reliability, server migration between different biometric platform vendors and enabling inter-agency collaboration.

GLOBAL EMBEDDED IC VERSUS SMART CARD IC SHIPMENTS



Source: ABI Research
See The Report

ABI Research's Trusted Device Solutions coverage focuses on the critical and foundational hardware components that shape the security landscape, cutting across traditional smart card applications, alongside emerging embedded hardware solutions.

FEATURED FORECAST

Driven by recovering economies, as well as the continued upward trajectory of hyper-connectivity and subsequent requirement for computing power, the demand for chips exceeded all expectations in 2021 and demand could not be fully met, with the industry sector bracing itself for 2022 and possibly beyond, as the critical year for the chip shortage hits.

The leading foundries and secure IC vendors are reacting. Arguably, the chip industry has been under-invested in historically, but this is set to change with the majority announcing significant investment plans to help increase capacity. The fact remains that this will be a mid- to longer-term solution, with the benefits of additional capacity likely to not be realized for another 12 to 24 months, with a significant amount of time required to upgrade and expand infrastructure and facilities.

Forecasts for the traditional smart card market stand at 9.0 billion for 2021 and 8.3 billion in 2022 as manufacturing and supply constraints continue, also reflecting overarching foundry and secure IC vendor strategies that, whenever possible, are shifting their respective supply and allocation priorities toward higher margin products.

As it relates to higher-margin solutions, the chip shortage is benefiting the embedded security market. The shift toward higher-margin chip solutions, paired with increased demand for computing devices, has meant that demand for embedded security solutions, including eSIM, secure elements, authentication ICs, and TPMs, has increased significantly. In 2021 and despite the chip shortage, shipments of embedded security chipsets increased 11% Year-over-Year (YoY) and expectations are that the market will continue on a similar growth trajectory, nearing 5 billion unit shipments by 2026.

RELATED RESEARCH

Digital Authentication and Embedded Security Market Data

Alternative Solutions for Sustainability in the Payments Market

Secure Smart Card and Embedded Security IC Technologies

CYBER & DIGITAL SECURITY

ABI Research helps organizations understand the evolving and increasingly connected cyber and digital security ecosystem. Along with exclusive research and extensive market data, we also provide expert guidance to our clients, helping them identify their challenges, understand their markets, and optimize technology investments and strategies.

Our seven Cyber & Digital Security research services offer a deep dive well beyond the device level, examining security applications enabled by a trusted foundation to protect data, networks, infrastructure, and services.

To learn more about any of our Cyber & Digital Security services, or to discuss your specific needs and challenges with our experts, contact us today.

CONTACT US

- Citizen Digital Identity
- Cybersecurity Applications
- Digital Payment Technologies
- Industrial Cybersecurity
- IoT Cybersecurity
- Telco Cybersecurity
- Trusted Device Solutions

ABIresearch
THE TECH INTELLIGENCE EXPERTS℠

Published May, 2022

157 Columbus Avenue
New York, NY 10023
Tel: +1 516-624-2500
www.abiresearch.com

ABOUT ABI RESEARCH

ABI Research is a global technology intelligence firm delivering actionable research and strategic guidance to technology leaders, innovators, and decision makers around the world. Our research focuses on the transformative technologies that are dramatically reshaping industries, economies, and workforces today.

ABI Research's global team of analysts publish groundbreaking studies often years ahead of other technology advisory firms, empowering our clients to stay ahead of their markets and their competitors.