CONNECTED & PROTECTED:

THE VULNERABILITIES AND OPPORTUNITIES OF IOT SECURITY

ABIresearch®

TRUSTED INTELLIGENCE SINCE 1990

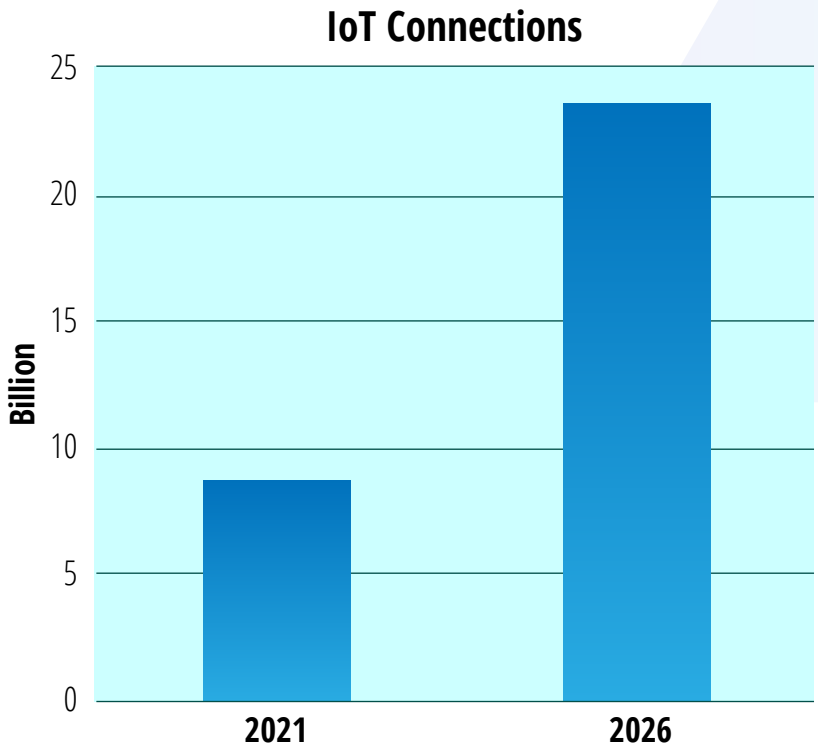
MORE CONNECTIONS, MORE THREATS

Today, there are 8.6 billion IoT connections. By 2026, that number will nearly triple to 23.6 billion, according to ABI Research market data.

This exponential growth will usher in a new era of connectivity and productivity in the years ahead. However, it will also result in new threat vectors and vulnerabilities. In fact, concerns about security in the Internet of Things (IoT) are widespread.

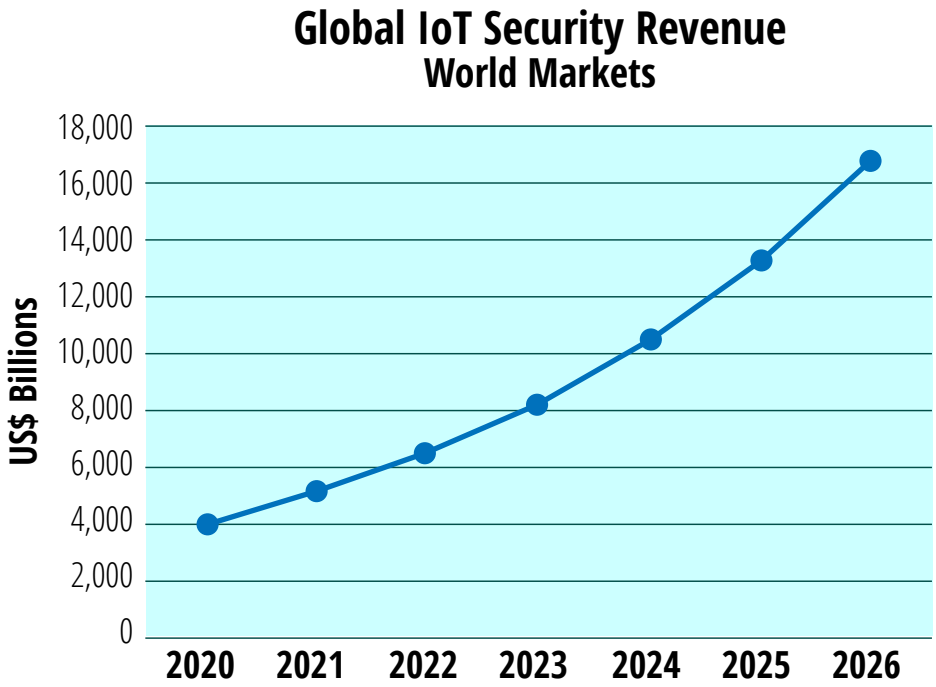
- Some devices are incapable of being secured, as a result of limited resources, processing capabilities, and computing power
- Original Equipment Manufacturers (OEMs) and vendors often choose to accept the risk, rather than remediate it during a Cost-Benefit Analysis (CBA), while many others choose not to do a CBA at all
- Functional safety-type IoT devices prioritize availability and often cannot simultaneously ensure confidentiality
- There are limited IoT security solutions in the market, due in large part to the fragmented nature of the IoT itself

While these security gaps pose a significant challenge for companies and end users, they also represent a tremendous opportunity for players in the IoT space, including IoT service providers, vendors, platform operators, and Information Technology (IT)/Operational Technology (OT) security organizations.



BREAKING DOWN THE US$16.8 BILLION IOT SECURITY MARKET

Much like the number of IoT connections is set to explode, so too is the revenue opportunity in IoT security. ABI Research market data shows that total revenue in the space will reach US$16.8 billion by 2026.



THE THREE MARKET CLUSTERS

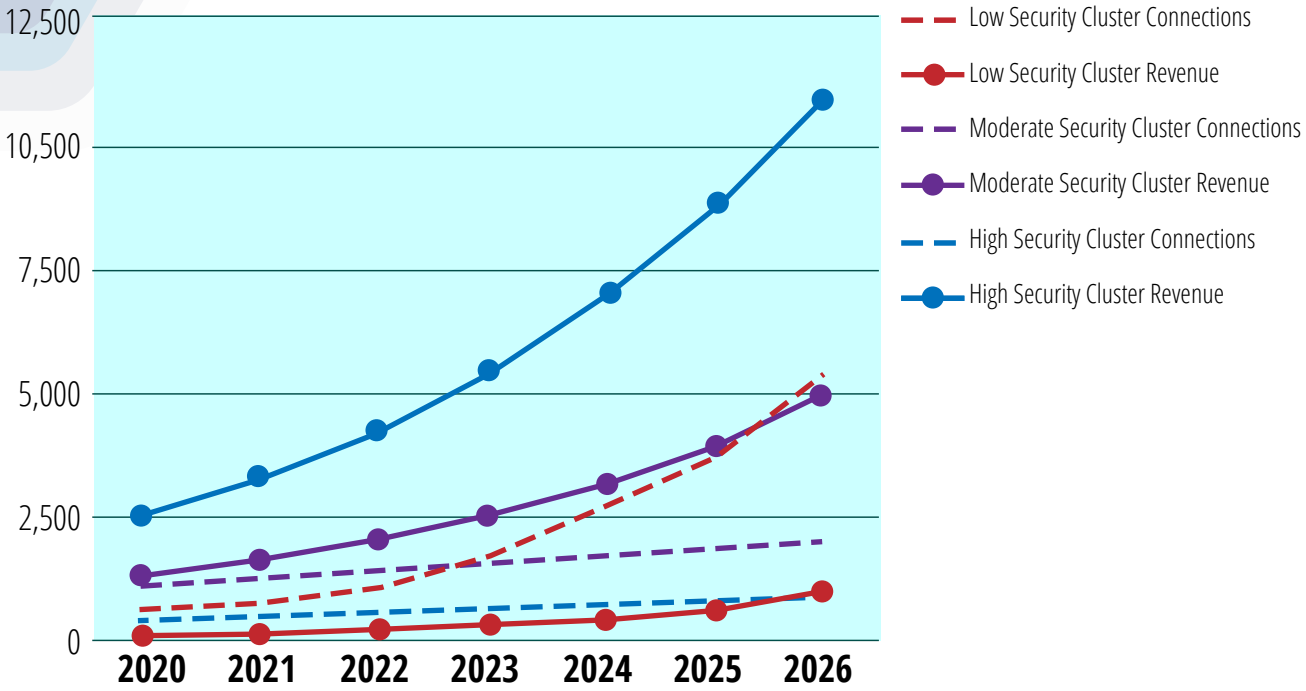
ABI Research classifies all IoT markets into three distinct market clusters based on low, moderate, and high security requirements, as described below:

Low-Security Requirements: Agriculture, asset tracking, digital signage, home appliances, home monitoring, home security & automation, inventory management, kiosks, people and pet tracking, smart parking, smart street lighting, wellbeing, wearables, and vending

Moderate-Security Requirements: Aftermarket telematics, commercial building automation, condition-based monitoring, fleet management, gas meters, heavy transportation, smart grid, video surveillance, smart meters, and water meters

High-Security Requirements: Automated Teller Machines (ATMs), healthcare equipment monitoring, intelligent transportation, patient monitoring, OEM telematics, and usage-based insurance

IoT Security Connections and Revenue by Cluster
(Millions and US$ Millions)



The sheer number of new IoT connections over the next 5 years, the increased digitization capabilities of certain IoT markets (e.g., utilities, industrial, infrastructure, and smart cities), and the increase in connected users and assets, along with the increased connectivity needs brought forth by the COVID-19 pandemic, are all fair predictors for digital security overall.

The amount of IoT security revenue, however, does not always correlate with the amount of IoT connections and some markets are expected to experience disproportional 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, life cycle management and predictive maintenance, firmware updates, and device and data integrity.

The high-security market cluster, which includes increased security profile devices like ATMs, Points of Sale (PoSs), healthcare devices, and OEM telematics, is expected to dominate, generating the majority of IoT security revenue and increasing from US$2.4 billion in 2020 to US$10.8 billion in 2026.

ABI Research forecasts that digital security services will enter the Return on Investment (ROI) equation significantly faster in the next 3 years, as both security vendors and IoT players will better understand how to protect the key monetization applications related to their IoT strategies.

FOUR IOT SECURITY SEGMENTS

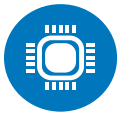
ABI Research classifies IoT security services into four main categories: device security, network and communication security, data security, and application security. Each category contains various technology components and holds different infrastructure requirements, which, in turn, differ greatly in each IoT market, vertical, or application.

Total IoT Security Segmented by Security Technologies
World Markets

Security Technologies	Revenues	2020	2021	2022	2023	2024	2025	2026	CAGR 20-26
Device Security	(US$ Millions)	1,083	1,416	1,834	2,356	3,023	3,832	4,826	28.7%
Network & Communciation Security	(US$ Millions)	1,379	1,710	2,107	2,633	3,357	4,273	5,551	25.7%
Data Security	(US$ Millions)	1,053	1,395	1,831	2,380	3,064	3,883	4,879	29.8%
Application Security	(US$ Millions)	302	409	545	716	931	1,189	1,506	31.6%
Total	**(US$ Millions)**	**3,817**	**4,930**	**6,318**	**8,085**	**10,375**	**13,177**	**16,764**	**28.1%**

WHAT IS DRIVING REVENUE?

NETWORK AND COMMUNICATION REVENUE DRIVEN BY CLOUD AND WIRELESS SERVICES:



Overall, IoT security services are expected to experience more than a 400% increase within the next 5 years, climbing from US$3.8 billion in 2020 to US$16.8 billion in 2026, marking a 28.1% Compound Annual Growth Rate (CAGR). Network security is expected to absorb the majority of the revenue, driven primarily by cloud security, wireless security, and secure monitoring services. 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 Embedded Subscriber Identity Module (eSIM) management).

INCREASED ATTENTION TO DATA PROTECTION ENDEAVORS BY IOT VENDORS PARTLY DUE TO PREVIOUS IT-BORNE REGULATIONS LIKE THE GDPR, NIST, ISO, AND HIPAA:

Organizations are also starting to place additional emphasis on data protection services due to increased concern for data loss prevention and data integrity endeavors. This is also partly driven by certain standardizations and regulations like the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), the National Institute of Standards and Technology (NIST), and the International Organization for Standardization (ISO) that managed to reach the greater IoT market landscape, especially with key user-focused IoT applications in the automotive market (i.e., aftermarket telematics, OEM telematics, intelligent infrastructure, and heavy transportation). 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.

FIRMWARE SECURITY, SECURE OVER-THE-AIR (OTA), AND PATCH MANAGEMENT TO DRIVE APPLICATION SECURITY:

Finally, application security is expected to be driven mainly by secure Firmware Over-the-Air (FOTA) updates for certain IoT markets (e.g., automotive and telematics), patch management for IoT devices and IoT routers/gateways, and firmware security for certain types of attacks like web attacks, backdoors, zero-days, data exfiltration from web apps or insecure Application Programming Interfaces (APIs), supply chain attacks, rootkits, botnets, and cryptojacking, among others. IoT device vendors are also keen to develop more security-focused Software Development Kits (SDKs); however, DevSecOps endeavors still have a tough roadmap ahead to transition from IT-borne environments to larger threat surfaces and complex IoT environments.

DEVICE VERSUS CLOUD VERSUS ON-PREMISES

The IoT security supply chain originates at the device level during manufacturing, then permeates all provisioning, management, and monetization services up until and including proper device decommissioning, thus ending its life cycle, while keeping the IoT fleet intact from any obsolete, insecure nodes. Cloud, network, and communication security will absorb the brunt of the business-as-usual IoT deployment and management, and setting the operational framework, protocols, and parameters required to manage devices, users, and systems. Data and application security relate to more technical, albeit still crucial, characteristics.

This roadmap, however, is greatly affected by infrastructure, cloud, and network architecture. On-premises and internally-managed deployments versus private or public cloud architecture (Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS)), as well as Managed Security Services (MSS) all have different service options and challenges associated with them. Therefore, there are multiple ways in which IoT security services can be further sliced and categorized based on their point of application to device-centric and edge gateway services, on-premises services, and cloud-based services with MSS options usually following the latter model.

END DEVICES AND GATEWAYS

IoT security services include identity issuance, provisioning, hardware security, and attestation services involving digital certificates, encryption keys, X.509s, or any other form of Identification (ID). On top of standard communication, routing, and Internet Protocol (IP) connectivity functions, IoT gateways and routers take on the device management mantle. Acting as a high-security node, IoT gateways are bridging management services between the edge and organizational servers either on-premises or cloud-based (public, private, or hybrid cloud). This crucial link is further strengthened (or weakened) depending on the overall infrastructure security posture.

CLOUD-BASED SERVICES

The cloud is the dominant option for managing and securing IoT assets. The cloud offers flexible and scaling options for data storage, management of connected assets, and securing said assets, along with providing adaptable services for users, devices, applications, and systems. There is little doubt that public cloud-based security management options will expand their already superior services compared to on-premises services when it comes to the evolution of the entire IoT ecosystem.

ON-PREMISES SERVICES

On-premises security services involve having the organizations themselves handling the majority of system management and security internally. On-premises security services are not a fit for every organization's profile, and there are several pros and cons to consider. On the plus side, on-premises security services allow organizations to have additional control over their infrastructure, with limited public cloud assistance, but potentially a higher dependence on the private cloud. However, on-premises deployments only work for specific IoT market verticals related to OT environments in critical infrastructure, energy, industrial, and healthcare.

STRATEGIC RECOMMENDATIONS FOR COMPANIES AND END USERS

ABI Research recommends implementing security services as a means to strengthen the IoT device identity and connectivity value chain, ensure ROI over existing IoT investments, prepare the infrastructure for scaling needs, and understand which types of services (cloud, on-premises, server, gateway, or device) are aimed at three different options. These include:

Core operations that must be protected at all costs

Value-added services for revenue generation

Useful, albeit secondary and can be revisited or reduced if needed

The first option is mandatory for protecting all vital system functions. The second one will secure a stable ROI over time. The third one can be applied at a custom level, or decreased if the organization is attempting a more cost-effective option and the associated threat vectors do not affect key operations. Many security vendors offer consulting services related precisely to understanding these unique needs for each organization based on their infrastructure, strategy, and IoT deployment needs.

Organizations still looking for a more cost-effective solution and still wishing to boost and secure their core operations versus the secondary ones, but that still struggle to implement security options, are advised to hone their ROI analysis skills in order to separate IoT management from IoT security. Ideally, security should obviously be part of the management equation of any IoT fleet, so for these companies, it is important to see the difference between the two.

MANAGEMENT VERSUS SECURITY:

Are management and security one in the same, or distinct responsibilities and functions? It depends on who you ask. Based on multiple interviews, it is clear that some vendors count it as being an integral part of regular operations, while others classify it as an additional endeavor.

From an organizational standpoint, there are two reasons to separate management services from security services:

ROI can be properly attributed to all respective components, allowing IT to clearly separate security options from all the standard operations, including those offered by prospective partners. However, this can be quite challenging depending on the organizational needs (e.g., cloud, on-premises, and hybrid options).

By knowing which communications, devices, and servers are properly managed and secured, organizations can place additional focus on their most vulnerable entry points (e.g., remote industrial communications), reduce the threat surface in their more Internet Protocol (IP)-heavy interactions (i.e., the more cloud-driven, Internet-heavy aspects), have a more precise understanding of what security tools are expected to do, and determine what security vendors offer and what cloud providers cannot offer.

STRATEGIC RECOMMENDATIONS FOR VENDORS AND PROVIDERS

DEVICE SECURITY SERVICES PROVIDERS

Digital Certificates, Public Key Infrastructure (PKI), and Internal Certificate Management Services: The primary security service comes in the form of managing device identity through digital certificates. This can be achieved both through PKI or internally-managed certificates. Digital certificates are primarily related to asymmetric-based encrypted communication between two or more entities by using PKI, Transport Layer Security (TLS)/Secure Sockets Layer (SSL), and other cryptographic methods. The legitimate third party is called a Certificate Authority (CA), which offers another set of security services, providing a secure and confidential audit trail with an inherent level of non-repudiation that can be extended across most cloud services.

Other than involving the role of a CA, certificate issuance can also be performed internally in an organization. Also referred to as "private" issuance, this involves an organization issuing its own digital certificates to accompany the encryption process of its devices, software, websites, and users. CAs and other security vendors can also provide assistance in this process by helping organizations issue their own certificates without actually being involved in the overarching process. Implementers should expect that there are certain issues concerning the application of digital certificates in the IoT, and additional infrastructure challenges for private/internal ways to identity issuance and management using Hardware Security Modules (HSMs), the use of secure hardware in edge devices, and many other factors related to the transition from enterprise to a larger IoT business strategy.

PaaS/IaaS-Based Security Services:

According to multiple interviews, there is a serious problem with third-party manufacturing facilities in certain countries, and primarily in Asia-Pacific, where manufacturing players steal intellectual property and company secrets from their partners. For many, there is an expectation that the hardware design, software, apps, or any related programming or design architecture will, in some way or another, be copied by their own manufacturing partners.

Secure manufacturing services can be offered as PaaS or IaaS using virtualized hardware in industrial and OT environments. Industrial players can also benefit from virtual data centers using IaaS, allowing them some flexibility over the constant needs of scaling infrastructure going the "pay as you go" way, especially because many Industrial IoT (IIoT) players are deeply concerned (or should be) regarding their legacy, long-life industrial equipment. The IaaS approach can provide this on-demand flexibility through virtualized hardware, which, in turn, can also be retrofitted with additional secure manufacturing and firmware installation security services.

NETWORK AND COMMUNICATIONS SECURITY SERVICES PROVIDERS

The Future of IoT Security Rests on Autonomous Remediation and Intelligent Cloud and Network Security:

Research interviews and market insights gathered from security organizations like the European Union's (EU) European Union Agency for Cybersecurity (ENISA) and the IoT Security Foundation, as well as leading firms like Intel, Microsoft, Thales, and Qualcomm, ascertain that the multiplicity and sophistication of cyberthreats are steadily forcing a chokehold on IoT implementations, unless IoT security is tackled uniformly across the entire value chain, instead of simply focusing on a specific component.

This grim assessment is supported by multiple security-focused vendors like Cisco, Symantec, Entrust, Palo Alto, and McAfee, as well as IoT gateway vendors like Cradlepoint, Eurotech, and Kerlink. The advent of 5G cellular connectivity will also greatly increase the IoT threat surface and Distributed Denial of Service (DDoS) attacks are expected to become even more powerful over time.

While different organizations are obviously set to support the section of the value chain they operate in (i.e., hardware, software, platform), the truth of the matter is that cloud, network, and communication security is becoming more important than ever, even with the recent move toward edge processing and edge security services. Successfully migrating IT security to OT environments, increasing device visibility, securing OTA updates and management operations, investing in cloud-based security options, adjusting encryption processes to favor asset monitoring, network traffic monitoring, and persistent threat hunting should be among the top priorities for IoT players.

While MSS are a lot easier to implement in IT-focused environments, they are also quite hard to migrate to most IoT markets due to their specific application needs and complexity. However, cyberthreats continue to mount and have even been exacerbated by the COVID-19 pandemic. Additionally, most IoT markets lack the knowledge, resources, and sometimes even the capital to invest in security services, which is also partly due to organizational misalignment.

Therefore, some form of intelligent and autonomous network security, threat monitoring, and remediation, at even the most basic level, should be part of the IT security budget for any new IoT application. This endeavor does not have to span multi-cloud platforms or high-budget Security Operation Centers (SOCs) to monitor each and every entry point or connected asset. Rather, equipping specific high-value organizational applications with some form of intelligent and autonomous (or semi-autonomous) cloud or network protection will greatly assist IT operations.

DATA SECURITY SERVICES PROVIDERS

SIMPLY ASCERTAINING DATA ENCRYPTION BY ITSELF MIGHT BE A MEANINGLESS STATISTIC:

Encrypting data only partly equates to overall data security. Verifying the integrity of the device, user, or platform, along with the data stream, applying identity and access management, and restricting privileges for all server and cloud administrators, along with system availability, should all be considered equally. Similarly, firewall security is a necessary, albeit intelligent-dependent component, requiring that different analytics and intelligence operations be custom-fitted for each specific IoT market, rather than a one-way contingency consideration.

This is based on three key findings from interviews conducted across multiple research projects with cloud providers, digital identity providers, and connectivity and security vendors:

Data encryption capabilities are vastly misunderstood for the entire IoT ecosystem with some companies positing that only 15% of IoT communications are encrypted, while others believe that amount is significantly lower and below 5%. On the other hand, IoT players (especially in industrial and smart cities applications) believe that data encryption will not only severely affect operational latency, but data security, in general, will not justify the added cost

Data Loss Prevention (DLP) tools and firewalls do not always protect all fraudulent traffic or provide 100% protection for related DLP practices. Vendors offered different estimates ranging from 15% to 35% of cyberattacks bypassing firewalls. This percentage is expected to increase significantly for certain IoT markets with less-than-optimal digital security capabilities (e.g., building automation)

The risk of **Advanced Persistent Threats (APTs)** has increased considerably over the last 3 years. Security vendor interviewees estimated that in IT environments, APTs can lie undetected, siphoning data from compromised systems in stealth for a period ranging from 3 to 6.5 months in most cases. This percentage is at least 50% higher than just 2 years ago based on similar research conducted by ABI Research. When applied to the larger IoT ecosystem, this range can increase considerably by an additional 2.5 months, and varies greatly depending on geographical location and the IoT vertical in question, which, in turn, affects other key factors like legacy equipment and security infrastructure, IP and communication protocols dependencies, threat surface, and perimeter defense.

APPLICATION SECURITY SERVICES PROVIDERS

ON-PREMISES COST-EFFICIENCY VERSUS PRODUCT SUPPORT AND MANAGED SERVICES:

Application security is highly dependent on the choice of product support or at least the breadth of resources available to in-house talent. Choosing to work using open-source Operating Systems (Oss), Integrated Development Environments (IDEs), or any IoT framework is a popular cost-cutting measure for application development. However, always keep in mind that immediate partners and service providers are also aligned with this vision and that customers are well informed about any potential challenges or shortcomings.

This is a fine line to walk, because companies are not expected to bluntly mention to their clients that their choice of a free Real-Time Operating System (RTOS), Linux OS environment, SDK is lacking security playbook options, or a Raspberry Pi hardware-based IoT gateway will require additional in-house talent, resources, and manpower to support over time. In many cases, this might force in-house developers to scour different free frameworks, GitHub databases, and open resource libraries in order to find a solution for various service-breaking problems that might arise from said free resources.

This is not to say that free IoT resources do not have their place in the development of the IoT ecosystem. Rather, this suggests that certain companies might feel more secure using a proprietary platform with stable time-tested applications, rather than embark on an implementation journey where certain security service hurdles are to be expected.

DO NOT UNDERESTIMATE THE VALUE OF APIs:

APIs are the unsung heroes of IoT implementations. Poorly designed APIs can severely hinder cross-vertical implementations, not to mention overburden IT departments when it comes to device authentication, software-based authentication, and security alert streamlining.

For example, good API design can make the difference between effective web-based identity provisioning for beacons, Password (PW) devices, and a chaotic mash-up of device IDs struggling to find their way to the cloud. Always keep in mind that IT should have a clear picture of which resources APIs have access to, especially when third-party entities are involved.

DIVE DEEPER INTO IOT AND DIGITAL SECURITY

The connections—and threats—inherent in the growing IoT presents critical challenges for businesses, as well as ripe opportunities for vendors and key players within these ecosystems. Since 1990, ABI Research has partnered with hundreds of leading technology brands, cutting-edge companies, forward-thinking government agencies, and innovative trade groups around the world. ABI Research's leading-edge research and worldwide team of analysts deliver actionable insights and strategic guidance on the transformative technologies that are reshaping industries, economies, and workforces today.

To learn more about ABI Research's **Digital Security** and M2M, IoT, and IoE Research Services, contact us today.

ABIresearch
TRUSTED INTELLIGENCE SINCE 1990

Published April 2021
249 South Street
Oyster Bay, New York
11771 USA
Tel: +1 516-624-2500
www.abiresearch.com

About ABI Research

ABI Research helps organizations–and visionaries within those organizations–successfully conquer digital transformation. Since 1990, we have partnered with hundreds of leading technology brands, cutting-edge companies, forward-thinking government agencies, and innovative trade groups around the globe. Through our leading-edge research and worldwide team of analysts, we deliver actionable insight and strategic guidance on the transformative technologies that are reshaping industries, economies, and workforces today.