ABIresearch®
TRUSTED INTELLIGENCE SINCE 1990

KEEPING THE IOT SMART & SECURE

ASSESSING THE SECURITY, ANALYTICS & OVERALL ECOSYSTEM OF SMART IOT GATEWAYS

KEEPING THE IOT SMART & SECURE

By the end of 2020, there will be 1.91 billion Internet of Things connections. Securing these connections is becoming an increasingly challenging – and critical – function. That is why key IoT vendors are investing significant dollars and hours into research and development related to Smart IoT gateways.

However, IoT gateways are currently caught amid a greater transformative evolution that shifts focus from the cloud to the edge, reversing the investment priorities of the past decade, causing IoT vendors to revisit their market strategies, further enhancing edge capabilities for gateways.

OTHER KEYS TO KNOW

Hardware and software digital security options in IoT gateways are steadily gaining momentum involving increased support for crypto-processes, Internet Protocol Security (IPsec)/Virtual Private Network (VPN) options, Machine Learning (ML)-empowered anti-malware, firewall and Intrusion Detection and Prevention System (IDPS), secure Root of Trust (RoT), and device bootstrapping, among many others.

Increased level of edge processing and data filtering for IoT gateways may originate at the silicon and chipset level, along with other critical security operations. However, native support with cloud management platforms is still very much part of the equation.

Securing legacy equipment, offering extensive brownfield management services, and providing hardware, software, and platform-agnostic gateway services to ease implementation and increase interoperability and data-driven intelligence. This will streamline the transition of Information Technology (IT) security tools into the Operational Technology (OT) infrastructure at both the gateway and the server levels, providing a much-needed security respite for IoT implementers.

Industrial IoT (IIoT), connected utilities, and smart energy markets will benefit more from the addition of next-gen IoT gateways, allowing a wide range of edge operations and intelligence, but still highly dependent upon overarching cloud services.

7 PRIMARY CHARACTERISTICS OF NEXT-GEN IOT GATEWAYS

With this evolution in mind, next-gen IoT Gateways are being developed with seven core characteristics in mind:

- Digital security
- Extended connectivity support
- Edge processing
- Authentication and management
- Cloud services
- Analytics
- Edge intelligence

DEFINING SMART IOT EDGE GATEWAYS

Smart IoT edge gateways have all the characteristics of router devices, but also encompass a much more extensive range of technological elements, including advanced connectivity support and network management, hardware/embedded and software cybersecurity options, processing power, data analytics, intelligent design, multi-tenancy vendor support, advanced management options, Application Programming Interface (API) design, cloud service integrations, higher levels of modularity, and some level of Artificial Intelligence (AI) support, which, on top of some network services, is also related to some form of security automation and orchestration (as part of a larger suite or managed service), network security, anti-malware, or malicious traffic depending on software elements, Operating System (OS), and Software Development Kits (SDKs).

SOME ORGANIZATIONS BELIEVE THAT SEGMENTING GATEWAY PRODUCTS IS WRONG AND, ULTIMATELY, NOTHING LESS THAN A MARKETING SCHEME

The term "smart IoT edge gateways" is used to reflect the current evolutionary trends and designs needed to bring IoT gateways into the future and address the growing IoT deployment, security, and management requirements. They can be referred to as "smart," "intelligent," or "next-generation" gateways (or routers, depending on the vendor). Still, some vendors use various descriptions as marketing terms, regardless of actual software or hardware capabilities. Note that other organizations believe that segmenting gateway products is wrong and, ultimately, is nothing less than a marketing scheme, but, perhaps quite ironically, they still use terms like "Artificial Intelligence" and "AI" to describe their own solutions, even though they offer no automation on any level, edge analytics and data filtering are severely lacking, and the ML tools involved are just borderline intelligent (e.g., simple linear regression) or incapable of providing any meaningful insights.

CONNECTIVITY & IOT MANAGEMENT PLATFORMS

COMMUNICATION AND PROTOCOL TRANSLATION

Connectivity Support: A standard requirement for all gateway/router products is the extended support for a variety of communication protocols and connectivity modules. Tailoring connectivity options to focus only on communication needs for specific verticals or applications will drive down costs. The difference between the connectivity options for standard and the "smart" IoT gateways is the advanced connectivity support, interoperability options, streamlined cloud-edge communication, protocol translation capabilities, support for legacy systems, and some form of data encryption (which might not always be applicable depending on the target application).

These characteristics are addressed on three different levels:

1) The hardware level with the incorporation of the appropriate connectivity modules that allow communication with each communication protocol;
2) The gateway software level, which enables multi-protocol support, routing, and protocol translation; and
3) In some cases, at the network architecture level proposed by leading communication authorities and industry entities.

PROTOCOL TRANSLATION FOR BOTH LEGACY AND STATE-OF-THE ART PROTOCOLS IS OF CRITICAL IMPORTANCE FOR GATEWAYS OPERATING IN THE IIOT, CRITICAL INFRASTRUCTURE, CONNECTED UTILITIES, SMART ENERGY, AND BUILDING AUTOMATION MARKETS

Protocol Translation, State-of-the-Art Communication, and Interoperability: Next-gen gateways will offer extended support for a wide array of communication protocols coupled with flexible connectivity services. This includes protocol translation for both legacy and state-of-the-art protocols, which is of critical importance for gateways operating in the IIoT, critical infrastructure, connected utilities, smart energy, and building automation markets.

IOT DEVICE MANAGEMENT PLATFORMS

An essential component of next-gen IoT gateways is management services, whether localized (gateway-based), on-premises (network server-based), or platform (cloud-based). This is a quintessential characteristic that distinguishes gateways from their older, traditional role of merely routing data traffic between different devices and servers, into their emerging role of extending secure management services to connected device.

NEXT-GEN IOT GATEWAYS WILL NEED LOCALIZED, ON-PREMISES, OR PLATFORM MANAGEMENT SERVICES

Device management options can be customized according to the implementers' specifications. It can be simple and straightforward, albeit somewhat insecure, ranging from managing simple credentials and device keys, all the way to more secure uses of digital certificates and complex Public Key Infrastructure (PKI) options. Note that digital certificate management can be achieved internally without a Certificate Authority (CA). This is a more cost-efficient option, but not all organizations can handle the internal management of digital certificates if they lack the necessary IT infrastructure or investment in Hardware Security Modules (HSMs) used to generate and manage encryption keys and Key Encryption Keys (KEKs).

HARDWARE SECURITY AND EDGE COMPUTING

CRYPTOGRAPHY AND ENCRYPTION KEY MANAGEMENT

Hardware Security and Ability to Safeguard ID Credentials: Smart IoT edge gateways usually require some embedded hardware security with a secure enclave or isolated environment (e.g., Trusted Platform Module (TPM), Trusted Execution Environment (TEE), and System-on-Chip (SoC)). This allows safe storage or high-value data and applications, as well as encryption keys and digital certificates used in IoT device management. This includes management of the gateway itself, but, in some cases, also management for all adjacent devices, depending on implementer parameters and deployment requirements.

Key Considerations for PKI and Encryption Vendors at the Gateway Level: Making use of PKI in the IoT is quite challenging and must also be addressed at the gateway level. Key considerations include the following:

- The use of embedded hardware security elements, especially TPMs for higher-end devices that can support crypto-functions.
- Assessing the quality and entropy level of those cryptographic elements (i.e., the ability to run certain functions within a tolerant level of entropy).
- Storage and processing requirements so as not to overburden other applications or processing operations (especially crucial in IIoT and IT/OT implementations).
- Ability to integrate with certain brownfield and legacy components, as well as greenfield devices.
- Hardware and software security options that can support key functions depending on targeted IoT applications (e.g., industrial protocol conversion, digital certificate rotation, multi-containerization, IDPS, etc.).
- Ability to obtain a level of quality of service for cloud management platforms.
- Ability to provide interoperable services for said cloud services.
- Provide control for new security operations that extend beyond network segmentation like data exfiltration protection and Data-Loss Prevention (DLP) at the edge.
- Support all standard next-gen gateway options for data analytics (which should accompany DLP options), filter, and aggregation, effectively making the transition from the cloud to the edge.

ADVANCED EDGE CAPABILITIES

Processing, Data Filtering, Bandwidth Capacity, Real-Time Operations, and the Cross-Vertical Value Proposition: Next-gen hardware capabilities must also include advanced edge processing power. Edge processing is not solely used to expand computing power and hasten software operations. It also extends into several key applications that deal with high-volume and potentially high-quality data traffic. The smart gateway transition into advanced edge processing serves various purposes, with the primary being decreased bandwidth capacity, intelligence efficiency, real-time operations, and cross-vertical implementations.

THE SMART GATEWAY TRANSITION INTO ADVANCED EDGE PROCESSING OFFERS DECREASED BANDWIDTH CAPACITY, INTELLIGENCE EFFICIENCY, REAL-TIME OPERATIONS, AND CROSS-VERTICAL IMPLEMENTATIONS

Increasing Efficiency of IoT Intelligence and Analytics: Because most data harnessed at the edge is not particularly useful for implementers, it makes little sense to spend additional resources and upload every piece of data only to be discarded again by implementers or cloud operators. Data filtering and data aggregation at the edge can help sort, manage, discard, and aggregate only the high-value data required according to implementers' specifications, thus boosting intelligence efficiency.

DATA FILTERING AND DATA AGGREGATION AT THE EDGE CAN HELP SORT, MANAGE, DISCARD, AND AGGREGATE ONLY THE HIGH-VALUE DATA REQUIRED ACCORDING TO IMPLEMENTERS' SPECIFICATIONS

Streamlining Real-Time Operations: Increased processing power at the edge, coupled with fewer bandwidth restrictions, data aggregation, and intelligence efficiency enables real-time operations to run more effectively. Streamlined real-time analytics and intelligence open an entirely new world for the IoT, allowing for precise management of critical or high-value applications, while also boasting a new value proposition for IoT security operations.

SOFTWARE SECURITY AND VIRTUALIZATION

MODULAR OSS AND SECURITY OPTIONS

THE LINUX-BASED OS HAS BECOME QUITE COMMON AND ITS MERIT AS A FLEXIBLE AND CUSTOMIZABLE SOFTWARE TOOLSET IS ALMOST UNMATCHED

Modular OSs and SDKs: A key element in any smart IoT edge gateway is the presence of a secure and customizable OS to work as a stable platform, allowing communication between end devices and cloud services, and the protected use of applications. The use of a flexible SDK from gateway vendors is always a welcome sight for implementers. While the use of open-source software tools is not always the best choice security-wise, the Linux-based OS has become quite common. Its merit as a flexible and customizable software toolset is almost unmatched, prompting many gateway software developers to base their products on Linux kernels. This is especially true for monolithic Linux kernels, which come with already added device drivers, direct hardware communication, and application multitasking. Although security might be somewhat lacking in monolithic kernels, they are designed for devices with a higher digital footprint.

Advanced Security Options: Smart IIoT edge gateways are also expected to have a greatly expanded security arsenal at their disposal. These options are highly dependent on the target application and should not be part of the gateways' mandatory design because that would increase the cost considerably.

Firmware Updates - Security Capabilities Depend on the Connectivity Options On Which They Are Built: The network architecture and communication requirements for IoT deployments may very well be the deciding factor in any IoT implementation because analytics, management, and security capabilities depend on said application's connectivity options. Firmware updates, cryptographic processes, managed security services, device life cycle management, and many cybersecurity endeavors must be enabled on top of the communication options on which they are built and the vertical or application at hand. One of the most crucial security operations for smart IoT edge gateways is the ability to perform firmware updates in a timely, secure, and reliable manner, which, in turn, frames many further options related to connectivity and security.

FIGURE 1:
ADVANCED SECURITY OPTIONS FOR IOT GATEWAYS

CONTAINERS	Use of containers to protect software operations and increase device reliability (the use of dockers is quite popular)
RoT AND BOOTSTAP	Secure RoT and protected bootstrapping options
FIREWALLS AND IDPS	Next-generation firewalls and IDPS
SECURE APIs AND API MANAGEMENT	Multi-purpose secure APIs for secure cloud integrations
ANTI-DDoS	Protection versus network attacks, Man-in-the-Middle (MITM) attacks and, most importantly, Distributed Denial of Service (DDoS) attacks
CRYPTOGRAPHY	Network encryption, Virtual Private Networks (VPNs) and IPsec (data packet encryption, communication protocol encryption (mandatory support for Transport Layer Security [TSL])
INTELLIGENCE	Intelligence and anti-malware tools for both known and unknown threats through ML and Deep Learning (DL) software tools, potentially including some lightweight edge version of User and Entity Behavioral Analystics (UEBA) or a software agent communication with the organizations' data center
NETWORK MANAGEMENT	Network segmentation and quarantine (must coincide with network protection and traffic monitoring), additional quarantine security options can extend beyond network and address applications (e.g., rogue third-party apps with unauthorized admin access to devices or platforms)
IoT IAM	IoT device Identity and Access Management (IAM) linked with cloud device and gateway management platforms
TRAFFIC MONITORING	Options for device, network, and data traffic monitoring services (which is particularly important for industrial control systems)
MANAGED SECURITY	For vendors that can afford a bigger overhead investment, edge gateways are a key component in managed security operations through System Information and Event Management (SIEM), Security Operations Centers (SOCs), and expanded cyber-forensics options

(Source: ABI Research)

BREAKING DOWN THE MARKET

Aided by the influx of new Internet Protocol (IP) devices and the upheaval of new IoT integrations across all market spectrums, IoT gateways are set to experience significant growth over the next 5 years. As shown in Table 1, IoT gateway shipments are expected to increase from 102 million in 2020 to 169.2 million in 2025, at a 70% increase. Smart IoT gateway shipments will increase from 8.5 million in 2020 by a factor of 3.5 to 21.4 million in 2025, with an impressive 20% Compound Annual Growth Rate (CAGR).

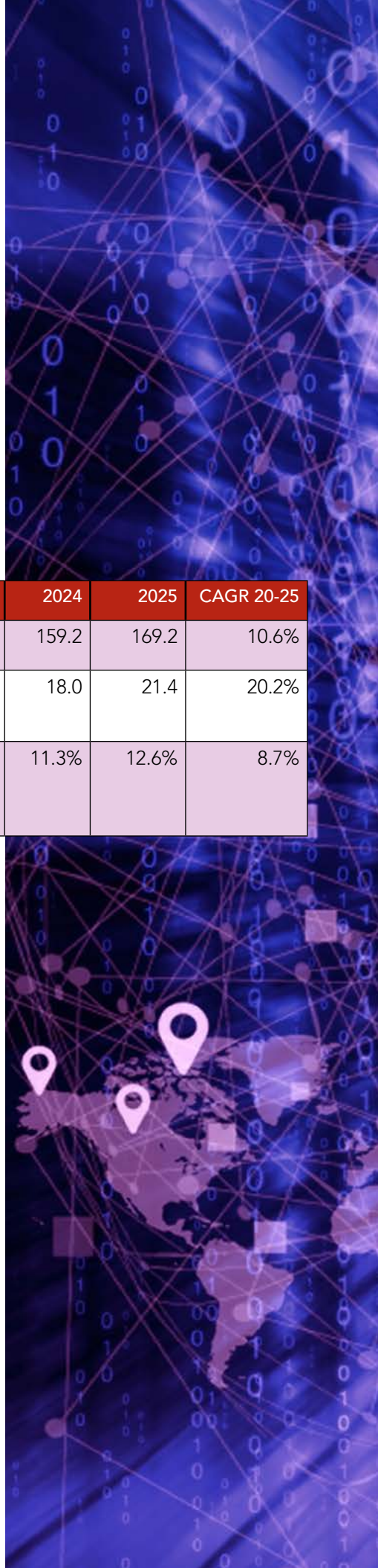
TABLE 1:
IOT GATEWAY SHIPMENTS VERSUS SMART IOT GATEWAY SHIPMENTS, WORLD MARKETS, FORECAST: 2018 TO 2025

GATEWAYS	SHIPMENTS	2018	2019	2020	2021	2022	2023	2024	2025	CAGR 20-25
IoT Gateways	(Millions)	72.3	85.6	102.0	114.9	136.6	153.8	159.2	169.2	10.6%
Smart IoT Gateways	(Millions)	5.8	7.0	8.5	10.3	12.9	15.7	18.0	21.4	20.2%
Penetration Rate of Smart IoT Gateways	(%)	8.0%	8.1%	8.3%	8.9%	9.4%	10.2%	11.3%	12.6%	8.7%

(Source: ABI Research)

Examining the Penetration Rate for the "Smarter" Components: The penetration rate of the IoT gateways featuring the more advanced "smart components" is expected to increase from 8.3% in 2020 to 12.6% in 2025. While this percentage may appear relatively small, it is a quite potent predictor for the future evolution of the IoT in its entirety because almost every vital piece of technological evolution that concerns the IoT (from embedded security to software and cloud security, cellular protection, and intelligence operations) has some aspect reflected on the gateway device itself (using of native cloud support, encryption, device management, OS, SDK, etc.).

What Do the Data Suggest? From the perspective of IoT connectivity and, perhaps more importantly, from the perspective of digital security, the data suggest that IoT players can at least expect some level of sophistication and intelligence operations at the edge aided by IoT gateways. Unfortunately, the industry has certainly not reached the threshold required for truly secure, massive IoT integrations. With the fervent increase of IoT connections, which ABI Research forecasts will reach 20 billion by 2025, a mere 169.2 million IoT gateways (not to mention only the fraction of 21.4 million of their "smarter" versions) is not nearly enough to safeguard future IoT ecosystems through edge-based security.



TAKE A DEEPER DIVE INTO DIGITAL SECURITY

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.

ABI Research's Digital Security service offers end-to-end coverage of the digital security ecosystem – from information and communication technologies to the operational control process. This research is particularly salient to enterprises facing the growing proliferation of cyber threats, while also becoming increasingly connected, as in the convergence of IT and OT.

IN THE POST-COVID-19 LANDSCAPE, HAVING ACCESS TO THE RIGHT INFORMATION AND STRATEGIC GUIDANCE IS MORE CRITICAL THAN EVER. ABI RESEARCH CAN DELIVER IT.

TO LEARN MORE, CONTACT US TODAY.

Published August, 2020

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

About ABI Research

ABI Research provides strategic guidance for visionaries needing market foresight on the most compelling transformative technologies, which reshape workforces, identify holes in a market, create new business models and drive new revenue streams. ABI's own research visionaries take stances early on those technologies, publishing groundbreaking studies often years ahead of other technology advisory firms. ABI analysts deliver their conclusions and recommendations in easily and quickly absorbed formats to ensure proper context. Our analysts strategically guide visionaries to take action now and inspire their business to realize a bigger picture. For more information about subscribing to ABI's Research Services as well as Industrial and Custom Solutions, visionaries can contact us at +1.516.624.2500 in the Americas, +44.203.326.0140 in Europe, +65.6592.0290 in Asia-Pacific or visit www.abiresearch.com.