Ovum Market Radar: Smart Home Cybersecurity

Making smart homes easier to manage and more secure

Publication Date: 13 Sep 2019 | Product code: CES006-000099

Richard Edwards

Summary

Catalyst

With the increase in consumer Internet of Things (IoT) devices, cybersecurity is becoming a prominent issue for residential customers. However, most consumers do not have the necessary technical know-how to protect their home networks and connected devices, which leads to a heightened level of concern about family security and privacy issues. This, in turn, creates new barriers that prevent increased adoption of smart home technologies and services.

To help protect as well as reassure consumers, all players in the ecosystem including communications service providers (CSPs) need to commit to making smart homes easier to manage and more secure. The starting point for this is the home network: detecting, protecting, and responding to the devices, applications, and technologies that homeowners and family members connect to it.

Ovum view

Vulnerabilities in residential gateways and consumer IoT devices have turned the threat of cyberattacks into a significant issue for consumers, forcing regulators and governments to act. The US Federal Trade Commission (FTC) has stated that it will hold manufacturers and sellers of connected devices to account for failures that expose user data to the risk of compromise, and the British government has published its *Code of Practice for Consumer IoT Security* for manufacturers. It is only a matter of time before the spotlight falls on broadband service providers, so Ovum advocates partnering with a cybersecurity vendor now rather than being forced to do it later under the scrutiny of the regulator.

Key messages

- Thoughts of hackers, scammers, identity theft, privacy violations, and the need to protect children and vulnerable adults are obscuring the benefits of smart home tech.
- Hundreds of thousands of consumer IoT devices are susceptible to malware infestation and subsequent weaponization.
- The residential broadband market is obsessed with speed, when it should be obsessed with the quality of experience, which includes security.
- Broadband service providers must prevent their gateways from being highjacked by malware and offer cybersecurity protections to consumers and their IoT devices.
- The digitally savvy consumer equates cybersecurity with the protection of personal privacy and all their connected devices, especially those within the home.
- Broadband service providers that demonstrate a commitment to cybersecurity can expect reduced customer churn, lower support costs, and new revenue opportunities.
- Broadband service providers need to invest now in advanced Wi-Fi platforms to reduce increasing operational costs. This investment should include a roadmap for delivering advanced cybersecurity capabilities into the home.

- IoT and media devices currently account for a third of home-network connections, representing thousands of device types and hundreds of brands.
- A growing number of cybersecurity products are using artificial intelligence (AI) and machine learning (ML) technologies.

Recommendations

Recommendations for broadband service providers and consumer-device makers

Broadband service providers have traditionally maintained a "hands-off" approach when it comes to customer-device security, but they now need to consider a different approach where IoT is concerned. Device manufacturers, retailers, application developers, and broadband service providers all need to follow industry best practice to make it easier for people to stay secure in a digital world, and partnering with a cybersecurity company is one way of achieving this in an effective, proactive, and adaptable manner.

Broadband service providers should harden their residential gateways to prevent them from being hacked and highjacked and offer stronger cybersecurity protections to consumers and their IoT devices. Failure to act is likely to result in customer losses relating to data, privacy, identity, and money and in service provider losses in terms of brand damage, customer trust, regulatory fines, and connectivity outages. By using cybersecurity technologies, service providers can mitigate cybersecurity risks, explore new revenue streams, reduce churn, and offer residential customers a better smart home experience.

Ovum's *Broadband Gateway Shipment Forecast: 2018–23* indicates that 80% of residential-gateway shipments are through broadband service providers. However, existing residential-gateway, router, and wireless-access-point vendors should not consider consumers and service providers to be captive markets. With global shipments of 230 million units per year, the residential-gateway market presents a tantalizing opportunity for new entrants, especially when services and IoT hardware are taken into account.

Delivering high-quality, high-speed voice, video, and data services to Wi-Fi devices in the home can be challenging, especially in high-density residential areas. Support calls and truck rolls have a significant impact on the operational profitability of service providers, and data shows that rates increase as more devices are connected to the home network. Broadband service providers should investigate mesh, adaptive Wi-Fi technologies, and Wi-Fi software data-analytic platforms that can accommodate IoT growth to keep call-in rates at manageable levels.

Scoping the smart home cybersecurity market

Definition and characteristics

The IoT presents a range of opportunities for consumers and suppliers, but a significant number of devices on the market today have been found to lack basic security capabilities. Users should be able

to benefit from their connected devices safely, confident that adequate security and privacy measures are in place to protect their online activity.

However, unlike PCs, tablets, and smartphones, the majority of IoT devices cannot have third-party cybersecurity software installed, so the consumer has to cross their fingers and hope that device manufacturers, IoT service providers, application developers, and retailers of internet-connected products are "doing the right thing" and following industry codes of practice. But what if they are not? This is where broadband service providers can help.

One logical monitoring point for smart home cybersecurity is the home gateway or consumer premises equipment (CPE). Enterprise-security vendors have been offering intrusion prevention, web security, device management, advanced threat protection, vulnerability scanning, and endpoint-protection solutions for several years, and now these technologies are available to consumers (either directly or via their broadband service providers) in the form of hosted, managed, and private cloud-based smart home cybersecurity services.

Key capabilities

IT security professionals talk about adopting a multilayered approach to cybersecurity, and this is also true in the smart home cybersecurity market. Consumers face many of the same threats at home as they do at work, but the solutions presented in this report all focus on individuals and families. Broadband service providers have a choice of solution types based on the vendor approach. Some vendors offer turnkey solutions, which are ideal when time to market is important. Others offer a tailored approach, integrating their solutions with a service provider's business and operational support systems. And there are white-label solutions for when a more holistic brand experience is required.

Capabilities vary in terms of reach and range, but service providers should consider core features such as

- web filtering and threat detection to defend against malicious software
- scam and fraud detection to block phishing and social engineering attacks
- identity protection to preserve privacy and prevent data theft
- network and device protection to block hackers and malware
- parental controls to protect children and vulnerable adults using their devices
- device monitoring and anomaly detection to prevent incidents before they happen
- router hardening and brute-force protection against password attacks
- network segmentation and bandwidth optimization for media devices
- a mobile app for network and device management and security alerts.

It can be useful to think about these features under the categories of protection, detection, response, and remediation. In terms of solution deployment, service providers should consider how and where they intend to run smart home cybersecurity solutions. Some vendors adopt a managed-services approach, while other vendor products can be deployed in the service provider's data center or on public cloud platforms.

Business value and applications

The offerings presented in this Market Radar offer service providers and their consumer customers a new kind of service: security as a service (SECaaS). The SECaaS business model has been around for a while in the world of enterprise IT. The service provider integrates its security services into the customer's IT infrastructure on a subscription basis, doing so better, quicker, and cheaper than an organization would on its own.

Consumers do not want the hassle of installing virus-protection software, spam-filtering software, and other security tools on their computers, smartphones, and tablets; IoT devices do not offer this capability anyway. The conceptual model of smart home cybersecurity consists of a set of cloud services and the home gateway working together, keeping the home network and the devices connected to it secure, protected, and private.

With this model in place, service providers can tackle customer-dissatisfying situations more effectively, thereby reducing support costs while offering a more satisfying service, which will reduce churn. And by shifting the service demarcation line from CPE to the home network and its devices, service providers and their partners can offer families and individuals those all-important delighters and value-added services. With a combination of Wi-Fi 6, Wi-Fi mesh, and AI data-analytics capabilities, service providers can extend features and the value of high-speed broadband services to every corner of the home with less impact from neighboring networks, especially in high-density residential areas.

Market landscape

Market origin and dynamics

The smart home cybersecurity market draws upon a range of products, technologies, and services, but it was the arrival of smart firewalls, mesh Wi-Fi routers, and internet-security devices for home users in 2016–17 that drew attention. Bitdefender, Cujo, Dojo, F-Secure, Plume, and Trend Micro are just some of the vendors that offer consumer hardware-networking products. However, as 80% of home-networking equipment is sourced through broadband service providers, it quickly became clear that partnering with service providers was the way to go, especially considering the subscription element of the products on offer.

Key trends in the smart home cybersecurity market

The smart home cybersecurity market is still maturing, albeit at a quickening pace. Part of the challenge is the refresh cycle of CPE. The firmware running on residential gateways and routers is updated periodically, but as with smartphones, the supply chain determines the speed at which this happens. Third-party software data-analytics platforms can be distributed across existing CPE hardware, but this can still take time to integrate into the service provider's network.

Other aspects of the smart home cybersecurity market have similarities with the smartphone and tablet market, not least of which is the proximity of Apple, Google, and Amazon. Today these vendors are focusing on the control aspect of IoT devices connected to the home network, but Google Wi-Fi

and Amazon's recent acquisition of Eero hint at where future opportunities lie, especially if we consider the integration of the smart speaker and Wi-Fi extender or access point.

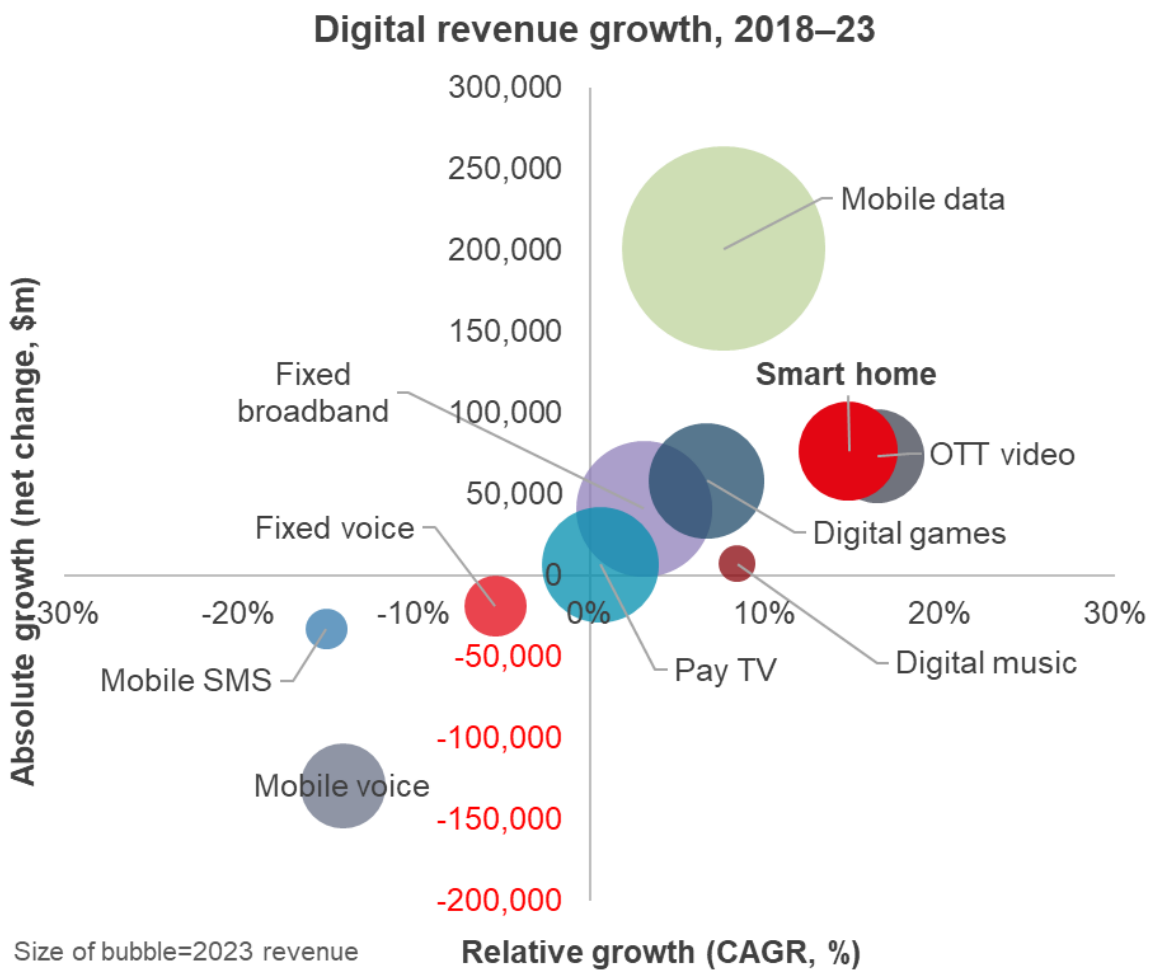
AI and ML feature in all the offerings presented in this Market Radar. This points to the enormous challenge of staying one step ahead of cybercriminals, state-sponsored hackers, and companies that overstep the line when it comes to gathering personal data.

Future market development

Early adopters of consumer IoT products are moving on from discrete device control and simple "do-this-then-that" routines. Integration, optimization, and automation are the next phase of smart home development, uniting multiple different technologies and systems and the thousands of devices that are in use. Smart home automation platforms enable the design of rules and offer time- and event-based triggers, scripts, actions, and notifications. And let us not forget voice control, which puts the vendors mentioned above in a strong position because of their prominence in millions of homes.

Consumer IoT and the smart home is a recognizable market, but we cannot separate it from the world of smartphones and mobile devices, wearables, smart speakers and media entertainment devices, AI assistants, residential security products, and assisted-living solutions. Ovum's current view is that the smart home represents a new growth area for broadband service providers and the broader ecosystem, with 15% CAGR ($76bn of new revenue) representing a total of $153bn by 2023 worldwide (see Figure 1).

Figure 1: Smart home represents one of the quickest-growing revenue opportunities in the consumer market



Source: Ovum

To date, broadband service providers have primarily relied on download speeds to differentiate their products. However, as all broadband service providers move toward high-bandwidth fiber and DOCSIS 3.1 connections, marketing strategies will need to shift from speed measured at the CPE to speed and quality of connection within the home. However, above all, providers will also have to demonstrate their commitment to making smart homes easier to manage and more secure.

Vendor landscape

The smart home cybersecurity landscape consists of startups, established vendors, and companies that are extending their product portfolios simultaneously in commercial and consumer markets. SAM Seamless Network is the youngest vendor presented in this Ovum Market Radar. The company was founded in 2016 by former cyberspecialists in the Israeli Defense Forces. Meanwhile, McAfee, F-Secure, and Trend Micro have been providing IT security solutions to organizations and individuals for 30 years.

Allot Communications, F-Secure, and Trend Micro are public companies, employing some 8,800 staff between them. However, McAfee is the industry heavyweight, having somewhere in the region of

9,500 employees globally. Four of the vendors in this report are headquartered in California, two in Israel, and one each in Romania, Finland, and Japan.

The only hint of market consolidation is the acquisition of Dojo-Labs by BullGuard in 2016. McAfee was founded in 1987, and the company was acquired by Intel in 2010. The company was spun out again in 2017. Recent venture capital investments are an estimated $66.2m: Cujo AI ($8.5m, Series B), Plume Design ($42.2m, Series C), and SAM Seamless Network ($15.5m, Series A). Investors include KPN Ventures, Samsung Ventures, Liberty Global Ventures, Jackson Square Ventures, Presidio Ventures, Shaw Ventures, Comcast, Deutsche Invest Venture Capital (DIVC), and Intel Capital.

Table 1: Ovum Market Radar: smart home cybersecurity vendors

Vendor	CSP offering	Headquarters	Founded	Employees	Status
Allot Communications	Allot HomeSecure	Israel	1966	600	Public
Bitdefender	Bitdefender IoT Security Platform	Romania	2001	1,600	Private
Cujo AI	Cujo AI Platform	US	2015	200	Private
Dojo-Labs (BullGuard)	Dojo Intelligent IoT Security Platform	US	2002	40	Private
F-Secure	F-Secure SENSE	Finland	1988	1,700	Public
McAfee	McAfee Secure Home Platform	US	1987	9,500	Private
Plume Design	Plume Platform	US	2014	200	Private
SAM Seamless Network	SAM	Israel	2016	40	Private
Trend Micro	Trend Micro Consumer Connect	Japan	1988	6,500	Public

Source: Ovum

Market Radar vendors: smart home cybersecurity

On the Radar: Bitdefender IoT Security Platform

Ovum view

Bitdefender's broad portfolio of products and services can help broadband service providers adopt a more active role in the smart home market and its nascent economy, especially in the US and Europe.

Key messages

- Manufacturers and sellers of connected devices should be aware that the FTC will hold them to account for failures that expose user data to the risk of compromise.
- Bitdefender's modular IoT security technologies address the cybersecurity challenges associated with residential gateways, smart home devices, and traditional endpoints.
- Bitdefender IoT Security Platform is a customizable, flexible, modular offering for CSPs, router manufacturers, and smart home hubs.
- Bitdefender IoT Security Platform addresses the cybersecurity challenges of CSPs, networking-hardware manufacturers, and home-security providers.

Why put Bitdefender IoT Security Platform on your radar?

Underpinned by cheap hardware, industry network effects, big data, cloud analytics, and API-first service models, the IoT is impacting every sector. In the residential sector, opportunities related to home security, energy management, and assisted living are driving early market adoption. However, consumers are also looking for assistance and reassurance. CSPs are well placed to step in and help, but to do so requires a partnership with a company such as Bitdefender.

Bitdefender IoT Security Platform presents a range of capabilities to CSPs, CPE manufacturers, and physical home-security providers. For CSPs, Bitdefender offers increased customer retention, decreased support costs, and network-equipment protection. For CPE manufactures, Bitdefender provides next-generation cybersecurity features and smart home device-management controls. Also, for home-security providers, Bitdefender presents complementary digital-security opportunities, equipment protection, and remote management of physical products.

Highlights

Background

Founded in 2001 by CEO Florin Talpes, Bitdefender is a private company. Headquartered in Bucharest, Romania, Bitdefender is a global security-technology company with offices in North America, EMEA, and Asia-Pacific. Bitdefender provides cybersecurity solutions and advanced threat-protection services that protect more than 500 million users in more than 150 countries, from private individuals to employees of the world's largest corporations. Bitdefender acquired RedSocks, a behavioral and network-security analytics company, in October 2018.

Current position

Bitdefender works with government organizations, large enterprises, SMEs, and individuals across more than 150 countries. Employing 1,600 staff and a team of 800+ engineers, Bitdefender was an early provider of IoT and smart home security with the Bitdefender BOX, a hardware-based solution designed to protect all devices connected to the home network including those that cannot be protected by traditional security software.

Bitdefender IoT Security Platform is designed to keep pace with the fast take-up of smart home devices. A self-improving platform, Bitdefender utilizes AI and ML technology to enable device identification and anomaly detection. Other features include device detection and management, vulnerability assessment, and brute-force protection. Through these capabilities, Bitdefender offers three distinct packages for CSPs and companies looking to grow their business with IoT security: Cloud Essentials, IoT Advanced, and IoT Full Stack.

Cloud Essentials addresses endpoint protection and web protection and category filtering at the gateway. IoT Advanced adds DDoS detection and protection at the gateway and brings device detection, identification, and management to the smart home. The customizable IoT Full Stack introduces anomaly detection, brute-force protection, exploit prevention, and sensitive-data protection.

The acquisition of Netherlands-based RedSocks added nonintrusive real-time breach-detection functionality and incident-response services to Bitdefender's portfolio, extending the company's reach beyond its endpoint-protection business. Bitdefender's position in this market is bolstered by 7,000 qualified reseller partners and its technology alliances with Citrix, VMware, Nutanix, the Linux Foundation, Microsoft, and Netgear. The company now needs to develop relationships with major operators, CPE manufacturers, and the movers and shakers of the smart home IoT market.

In July 2019, the FTC stated that it would hold manufacturers and sellers of connected devices to account for failures that expose user data to the risk of compromise. The FTC's advice to consumers is to "secure your router" and "secure your computer." However, what about smart home IoT devices? Bitdefender is not alone in the smart home cybersecurity market, but its trusted status among proactive consumers and enthusiasts gives the company an important edge.

Looking forward, Bitdefender's 20+ original equipment manufacturer (OEM) solutions and software development kits (SDKs) provide evidence of the company's commitment to partners, and its channel credentials are also highly regarded. Partnerships and alliances are going to play a defining role in the smart home market, and this would certainly seem to play to one of Bitdefender's strengths.

Datasheet

Table 3: Datasheet: Bitdefender

Product name	Bitdefender IoT Security Platform	**Product classification**	Smart home IoT security, endpoint protection, gateway services
Version number	N/A	**Release date**	2017
Industries covered	ISPs, broadband service providers, MSPs, equipment manufacturers, and systems integrators	**Geographies covered**	North America, EMEA, and Asia-Pacific
Relevant company sizes	Medium to large	**Licensing options**	Partners: revenue share and/or technology-access fee End users: SaaS
URL	www.bitdefender.com/iot/	**Routes to market**	Direct, partner resellers, and direct to consumer plus co-branding.
Company headquarters	Bucharest, Romania	**Number of employees**	~1,600

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

Broadband Gateway Shipment Forecast Report: 2018–23, CES006-000078 (July 2019)

Driving New Revenue Out of the Connected Home, CES006-000082 (August 2019)

The Road to 2023: Smart Home, CES006-000086 (August 2019)

The Road to 2023: The Ultra-Fast Connected Home, CES006-000089 (August 2019)

"Key trends from the smart home market," CES006-000090 (August 2019)

"Smart home cybersecurity is a must for greater consumer IoT adoption," CES006-000083 (July 2019)

Author

Richard Edwards, Ovum Associate Analyst

Michael Philpott, Senior Practice Leader, Consumer Services

michael.philpott@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Boston
Chicago
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
Paris
San Francisco
Sao Paulo
Shanghai
Singapore
Sydney
Tokyo