Cybersecurity and the Smart Home Industry Snapshot

How the surge in smart homes may open the doors to opportunities and vulnerabilities for consumers and solution providers

November, 2017

FROST & SULLIVAN

Contents

Introduction:
Connected Living and the Smart Home

Understanding Connectivity and Connected Living

What do we mean by a Connected Ecosystem?

Internet of Things (IoT) is a technological revolution aimed at adding a new dimension to the world of information and communication technology by embedding short-range mobile transceivers into gadgets or things used in everyday life. A connected ecosystem is the outcome of the implementation of IoT that enables every individual device to communicate and share information with each other for more effective management and streamlining of processes.

Why do we need a Connected Ecosystem ?

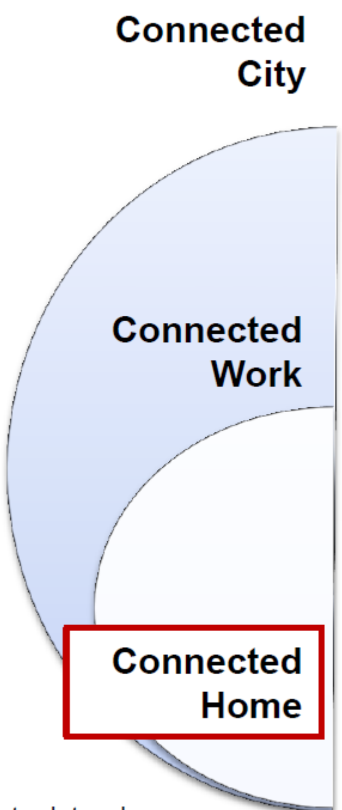
- With the global economic pressure to lower the cost of operations and services and to improve business efficiency to stay competitive in the market, asset management and process efficiency are the key areas of focus among organizations. This can be facilitated by a connected ecosystem within a particular sector.
- Leveraging huge amount of information captured from the connected network, will help in improving the decision making process and enable delivery of advanced functionalities such predictive insights more accurately.
- Until now, the Internet is the only technology, which has been strongly leveraged by enterprises to communicate with the world. However, connecting these discreet sources of information could bring in additional revenue streams for an organization and also help organizations to provide more customized solutions to its customers, thereby improving satisfaction for the clients

Key Benefits of Connected Ecosystems

Source: Frost & Sullivan

Smart Homes form a Basis for Connected Living

Connected living describes a world in which consumers use different devices to experience compelling new applications and services that integrate video, voice, and data services providing users with access and connectivity anytime and anywhere.



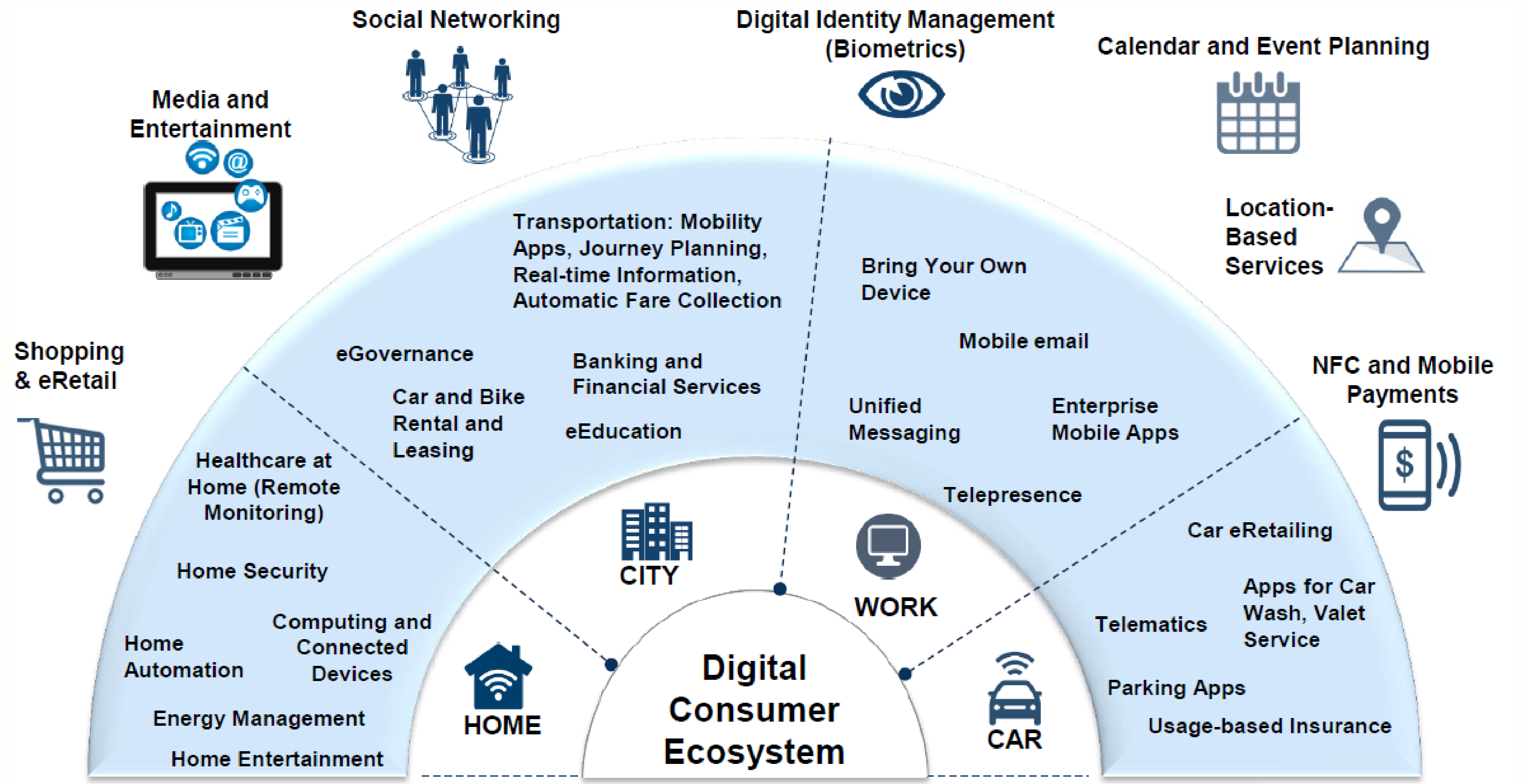
Governance	eServices, eAdministration, and eSecurity
Banking	Mobile payments, kiosk services, online banking, and online stock trading
Transportation	Passenger-car telematics, smart mobility cards, and mobility applications
Communication	Telepresence, unified messaging, remote desktop access, virtual private networks, and audio, video, and Web-conferencing tools
Mobility	Mobile email, enterprise mobile applications, people locator applications, human resource applications, and BYOD
Collaboration	Web-based project collaboration tools, cloud-based file sharing services, desktop sharing, and enterprise social media
Home Automation	Heating, Ventilation, and Air Conditioning (HVAC) controls, lighting control systems, security controls, and entertainment controls (audio and video switchers and processors)
Home Energy	Metering systems (inbuilt or taking input from external smart meters), and energy display systems
Home Entertainment	Video streaming, multi-functional smart devices, and new media value-added services
Home Health	Remote monitoring and control, symptom checks through sensors and surveillance, remote delivery of advice, and telemedicine
Education	Remote education services and virtual tutoring

Relevant sub-trends considered for this study

Source: Frost & Sullivan

The Digital Consumer Ecosystem

Consumer technologies combined with increased home automation open the door to cyber-related vulnerabilities



The next generation of solutions for connected living will be driven by the convergence of technology and suppliers across homes, cities, work, and cars.

Source: Frost & Sullivan

Overview of Key Smart Home Technologies

Features	Products/Services	Technology Used for Communication	Remarks
Safety and Security	• IP Video Surveillance • 24/7 Monitoring Service • Window/Door Sensors • Motion Detection • Smoke/CO Alarm • Water Leak Detection	Wireless protocols (Z-Wave, Zigbee, Wi-Fi, and KNX-RF) Wired protocols (Insteon, DALI, KNX, X10, and UPB)	These 4 features are offered as a comprehensive solution only by some participants in the ICT industry. However, many technology and system providers in the ICT and BT industries are expected to adopt new business models to enter the smart and connected home market and sustain growth in the next 5 to 10 years.
Home Automation	• Remote Access (e.g., lighting, home appliances, and window blinds) • Remote Automatic Locks • Automated Ambient Lighting • Automated Heating and Cooling		
Home Energy Management	• Heating, Ventilation, Air Conditioning (HVAC) • Smart Thermostat Control • Appliance Scheduling • Lighting Controls • Consumption Monitoring • Price Monitoring/Arbitrage (TOU) • Event Notification • Solar Monitoring • Trend Identification • EV/ES Charge/Discharge • Battery Charge/Discharge • Weather and Price Signal Forecasting		
Home Entertainment	• Audio and Video Systems • Home System Integration and Remote Control		

Key: DALI—Digitally Addressable Lighting Interface; UPB—Universal Powerline Bus;

Note: Most solution providers include HVAC control, home entertainment, and safety and security as part of comprehensive home automation solutions

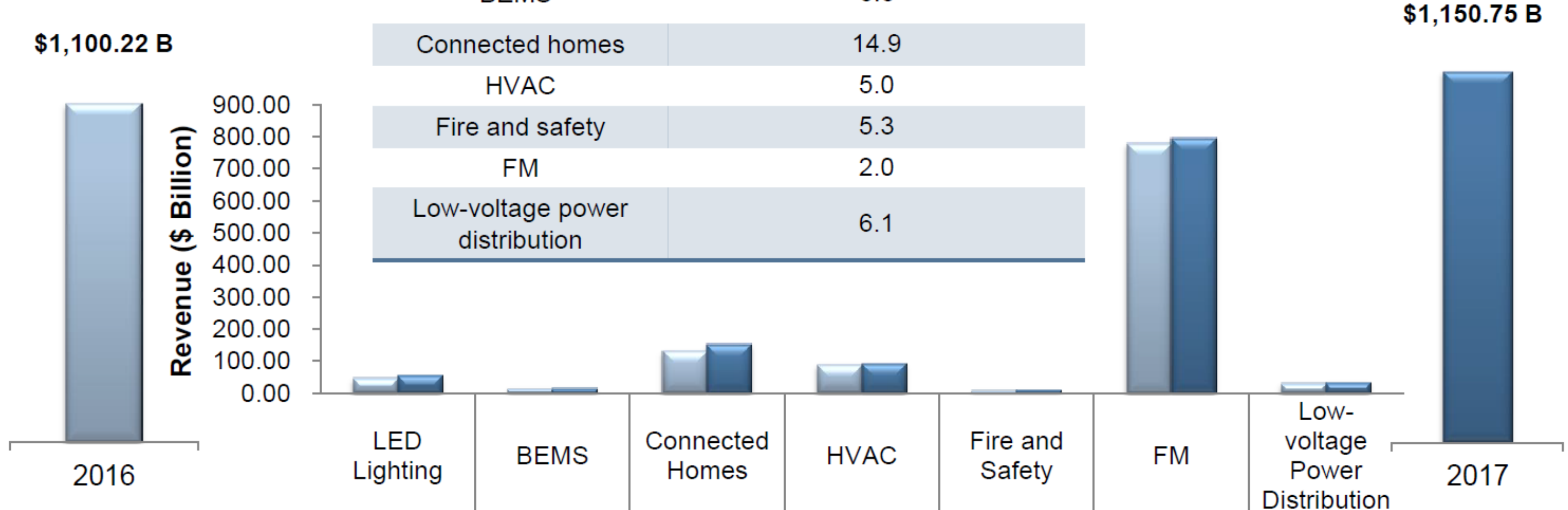
Source: Frost & Sullivan

Smart/Connected Homes See Growth Surge

Smart and connected homes are one of the fastest growing markets within the global Homes & Buildings sector

Total H&B Industry: Revenue by Sector, Global, 2016 and 2017

Sector	Growth Rate (2016–2017) (%)
LED lighting	16.4
BEMS*	6.6
Connected homes	14.9
HVAC	5.0
Fire and safety	5.3
FM	2.0
Low-voltage power distribution	6.1



	LED Lighting	BEMS	Connected Homes	HVAC	Fire and Safety	FM	Low-voltage Power Distribution
2016	47.30	12.88	132.40	88.47	8.57	780.04	30.56
2017	55.07	13.73	152.13	92.88	9.02	795.50	32.42

*BEMS includes the HEMS, BEMS, BAS, and home automation system (HAS) markets

Note: All figures are rounded. The base year is 2016. Source: Frost & Sullivan

Smart Home Cybersecurity and Consumer Perceptions

Smart Home Potential and Implications

Frost & Sullivan research indicates smart home markets are gaining traction in North America

	Strategic Implication
38% of homes in North America have adopted some form of smart home solution.	The proportion of homes that are exposed to cyber risks related to smart home technologies is significant and is expected to grow. Strategies to effectively secure those solutions will be needed.
24% of homes in North America are likely to adopt smart home solutions in the next 12 to 18 months.	
The market penetration of each major type of smart technology (e.g., security, entertainment, is less than 20%.	The categories of devices to be secured is broad; adequate coverage could be challenging. The urgency to work with smart home solution providers to ensure cybersecurity across solution and device types will increase in the next 12 to 18 months.
Each major type of smart technology can penetrate an additional 10% to 20% of the market in the next 12 to 18 months.	
Adoption is motivated by cost efficiency and home security considerations.	There may be an opportunity to leverage overall home security as a motivator for adopting cybersecurity solutions.
Detached houses, apartments, and townhouses provide the larger base of current and potential adopters.	Efforts to promote cybersecurity solutions can prioritize residents of these dwelling types.

Source: Frost & Sullivan

Consumers and Cyber Precautions

Frost & Sullivan survey shows even early market adopters often do not employ full protections

	Adopters (n=474)	Potential Adopters (n=307)	Non-Adopters (n=482)
I am aware of identity theft	66%	80%	77%
I follow the password etiquette	55%	66%	57%
I am taking steps to secure my personal information across devices and online accounts	51%	50%	40%
I read privacy agreements	49%	43%	35%
I ask service/ technology providers about how their personal information across devices and online accounts are being secured	31%	13%	7%
I encountered an incident in the past one year that relates to loss of personal information/ identity theft	25%	10%	8%

Q24. Which of the following apply to your own practice or experience?

Source: Frost & Sullivan

Consumers and Cyber Precautions

Yet concerns about cybersecurity run high across all segments of smart home adopters

The majority of adopters and potential adopters have cybersecurity concerns

Top 2 box -very high and high concern	Adopters *(n=474)*	Potential Adopters *(n=307)*	Non-Adopters *(n=482)*
High initial setup costs	66%	74%	62%
The costs (time, money, effort, risks) outweigh the benefits	58%	67%	58%
Potential access to personal information from the home network	65%	62%	52%
Security breaches on the smart home network	63%	62%	52%
High management/ maintenance costs	61%	62%	52%
Risk of loss of privacy and personal integrity	65%	60%	49%
Security breaches of smart home cloud services	63%	61%	50%
Effect of electrical or power systems failure on the system	62%	54%	51%
Effect of system failure on the ability to manage the home	59%	56%	44%
Insecure smart home apps	61%	52%	43%
More likely to fail than manual systems (due to greater complexity)	56%	52%	46%

Q10. Thinking about smart home solutions, to what extent are the following a concern regarding their possible use in the home?

Source: Frost & Sullivan

Challenges in Cybersecurity Adoption

Homes, buildings, businesses and solution providers are often ill-prepared for cyber threats

Lack of Security Standards	Due to the need for an open architecture of IoT, security is a major concern hindering wide scale adoption of the concept. Standardization could act as a major facilitator for the adoption of connected ecosystem for secured effective communication and interoperability. However, the present standards are mostly developed focusing a specific region or a specific application sector. There is still a lack of unified standardization activities that could help in realizing the connected world concept. The industry requires collaboration across the globe from various industries for effective communication and seamless interoperability of devices and objects.
Lack of Comprehensive Security Solution	Apart from standardization activities, many organizations also lack the understanding of the security loopholes in their operating environment. Deploying a security solution for the enterprise database is not adequate enough to protect the ecosystem. It warrants protection of the unique communication channels based on use cases, protection of the devices connected to the enterprise network, management of devices and also continuous monitoring of the connected systems. The connected ecosystem demands for a comprehensive security strategy at multiple levels of the connected network. Technology innovation plays a vital role in many steps of this strategy.
Lack of Cross Platform Security Technology	Identity and access management solutions acts as key elements for device and system protection. However, with gradual shift of enterprise systems into the cloud, traditional IAM solutions fail to protect the cloud infrastructure. Biometric authentication is also an important aspect, which requires compactness in design to fit the modern day devices such as smartphones and wearables. New monitoring platforms with user friendly visualization is also the need of the hour for business users to continuously monitor their network from remote locations through mobile devices. Advanced analytics are required to be available in mobile for remote real-time insights.

Source: Frost & Sullivan

Cybersecurity and Physical Security

Smart Home Solutions

Safety and Security are top entry points for cybersecurity attacks, though systems across a smart home may be vulnerable

Home Automation: Remote monitoring and centralised control of lighting, window blinds, and home appliances

Home Energy Management: Automatic synchronisation of energy consumption data for minimised future energy use (on the basis of usage patterns and exterior conditions)

Home Entertainment: Personalised entertainment through open platforms from various broadcasters and Internet providers

Virtual Education: Virtual tutoring through technology-enhanced Web-based services and high-speed Internet

Safety and Security: Remote surveillance of entire home and occupants through smartphones and tablets

- Video Surveillance
- 24/7 Monitoring Service
- Window/Door Sensors
- Motion Detection
- Smoke/CO Alarm
- Water Leak Detection

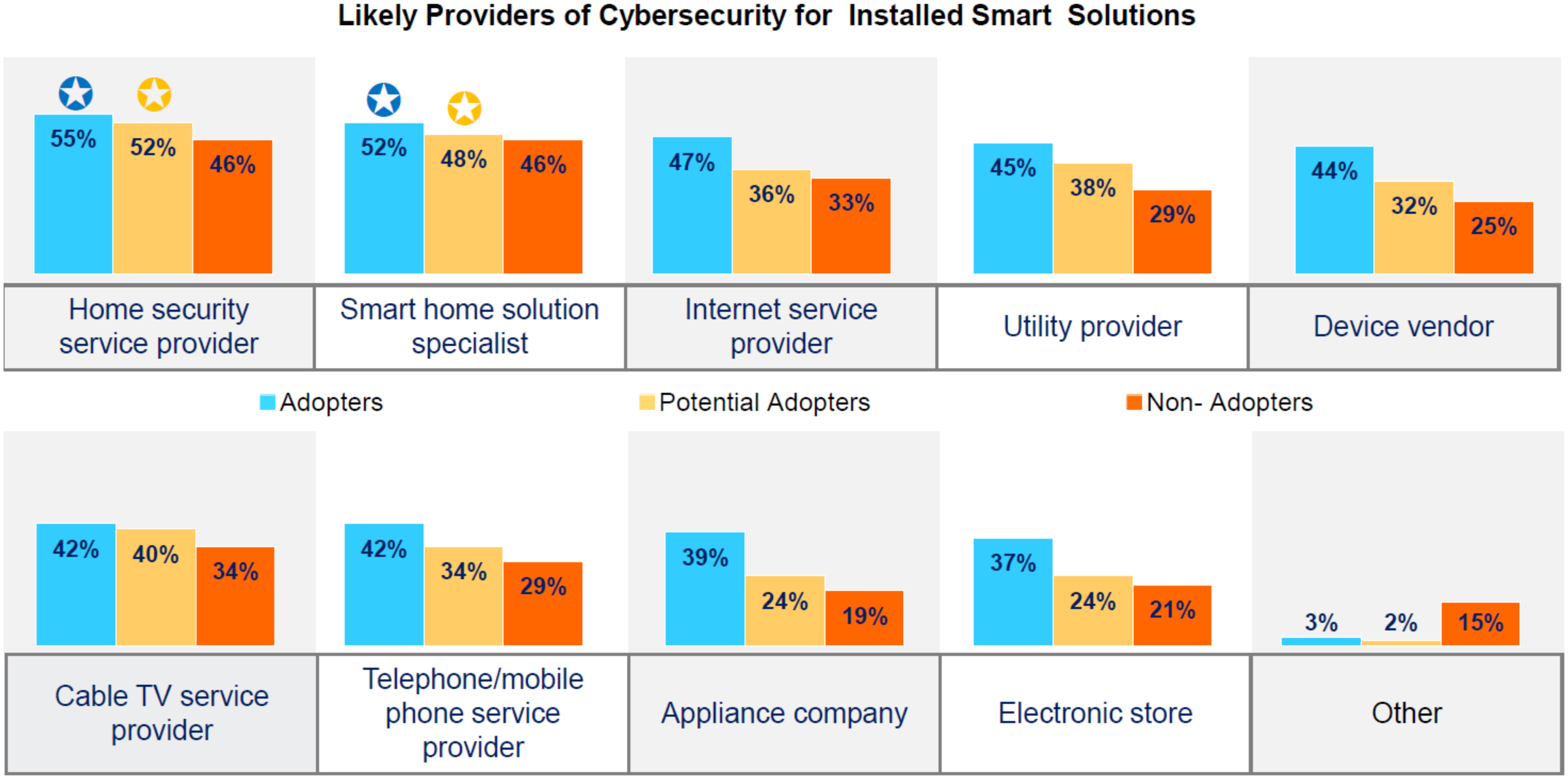
Health and Wellness: Continuous monitoring and evaluation of the general fitness and well-being of occupants

Note: Some solution providers include HVAC, home entertainment, and safety and security as part of their comprehensive home automation solutions.

Source: Frost & Sullivan

Cybersecurity and Smart Homes

Home security companies and solution specialists are viewed as the most likely players for installing cybersecurity systems in homes

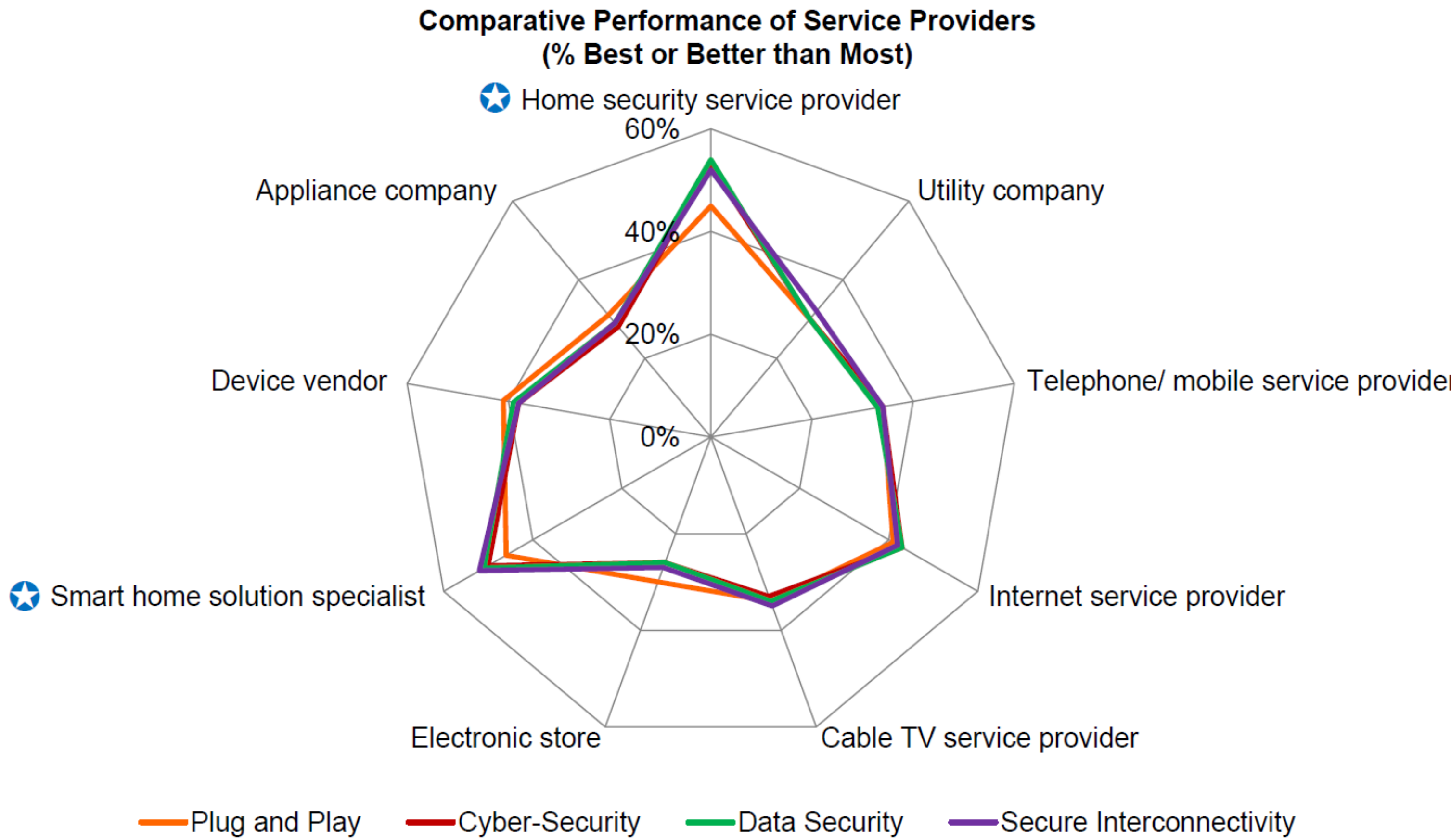


Base: Adopters (n=474)/ Potential adopter (n=307) / Non-Adopters (n=482)
Q13a. Which of the following would be your likely source(s) for providing cybersecurity for your installed smart solutions?

Source: Frost & Sullivan

Cybersecurity and Smart Homes

Home security companies and solution specialists also considered to have wider expertise and capabilities than other home solution providers, such as utilities or cable service providers



Base: All respondents.
Q33. Which of the following service providers would you consider the best, better than most, average, worse than most and worst when providing the following?
(Top 2 Box Scores – Best/ Better than Most)

Source: Frost & Sullivan

Cybersecurity and Smart Homes

Security systems are among the most common currently installed smart home solution for homes in North America

Overall *(n=1,263)*

Secure and monitor your home	17%
Home entertainment/ media streaming management	17%
Energy consumption management	16%
Heating and cooling management	16%
Home lighting management	15%
Health monitoring	11%
Water consumption management	10%
Whole home management	10%
Appliance management	9%
Retail/ Inventory management	7%
None	62%

Q2. Which of the following smart technologies/ capabilities are already available in your home?

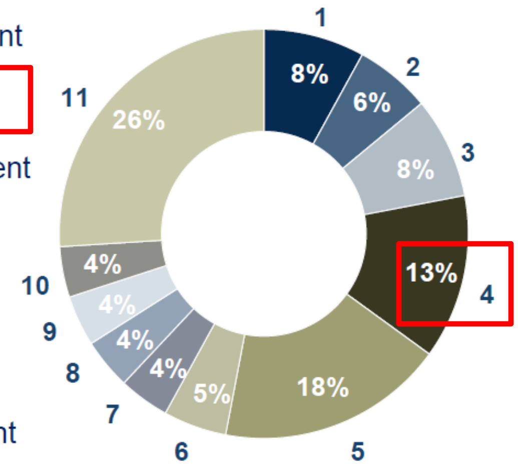
Cybersecurity and Smart Homes

However, security systems are also among the most vulnerable to cybersecurity breaches, according to consumer perceptions, second only to media systems

Adopters' Perceptions

In your opinion, which of your existing connected home systems is MOST vulnerable?

- 1. Energy consumption management
- 2. Home lighting management
- 3. Heating and cooling management
- 4. Secure and monitor your home
- 5. Media entertainment management
- 6. Health monitoring
- 7. Appliance management
- 8. Retail/ Inventory management
- 9. Water consumption management
- 10 Integrated home management
- 11. None (all home systems are secure)

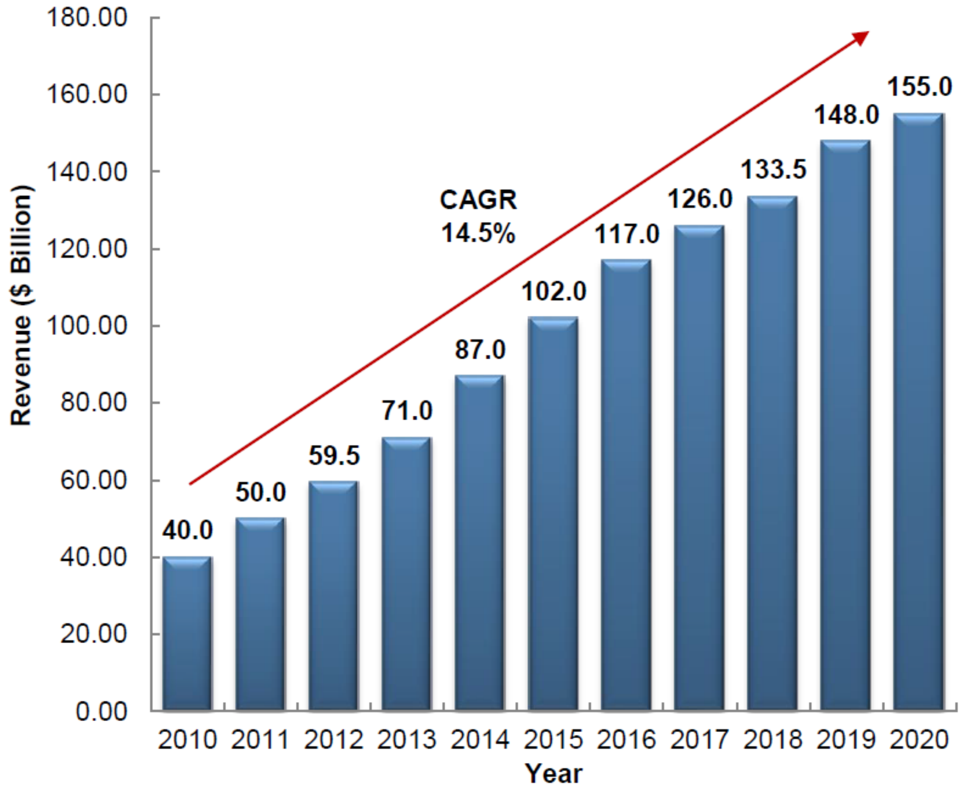


Q29a. In your opinion, which of your existing connected home systems is MOST vulnerable?

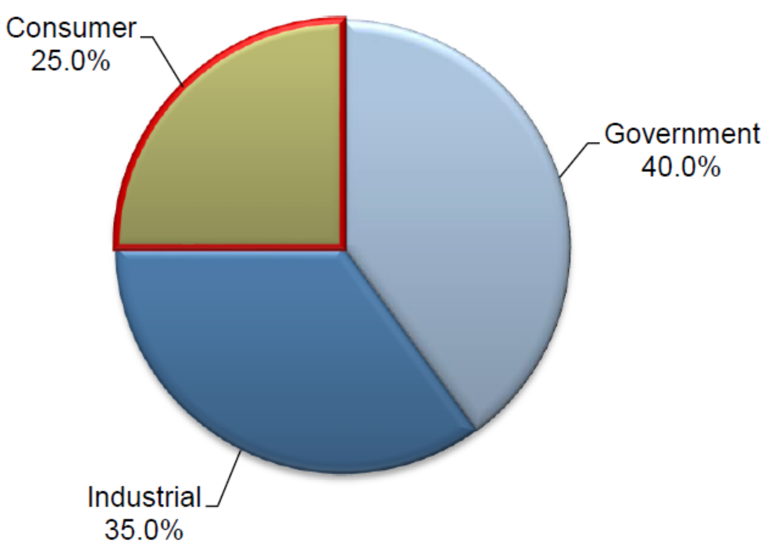
Connected Security Market and Trends

Before significant growth can be seen in the connected homes market, cybersecurity concerns need to be overcome before consumers will be comfortable opening their homes to cloud-based solutions. This is expected to drive investment in cybersecurity at the consumer end, accounting for approximately 25% of the cybersecurity market

Total Cybersecurity Market: Revenue Forecast, Global, 2010–2020



Total Cybersecurity Market: Estimated Per Cent Sales Breakdown, Global, 2016



Note: All figures are rounded. The base year is 2016. Source: Frost & Sullivan

Strategic Conclusions

Strategic Conclusions

Conclusions

Connectivity, connected living and smart homes are all rapidly growing and intertwined trends that will continue to dominate the homes and buildings industry discussion for years to come

As smart and connected homes increase, and consumers continue to blur the lines between devices and the home, the number of potential entry points for cyber threats in the home increase

Despite the risk across multiple devices and entry points, consumers still associate physical security – and physical security providers – as among the leading suppliers of cybersecurity solutions for the home

Opportunities abound for other types of service providers to gain mind share in "cyber-securing" the home. In particular, consumers view media/entertainment as a key potential entry point for threats, yet these providers are not high on the list for suppliers to homeowners in this space

Source: Frost & Sullivan

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Our customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for customers' internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, write to:

Frost & Sullivan

3211 Scott Blvd, Suite 203

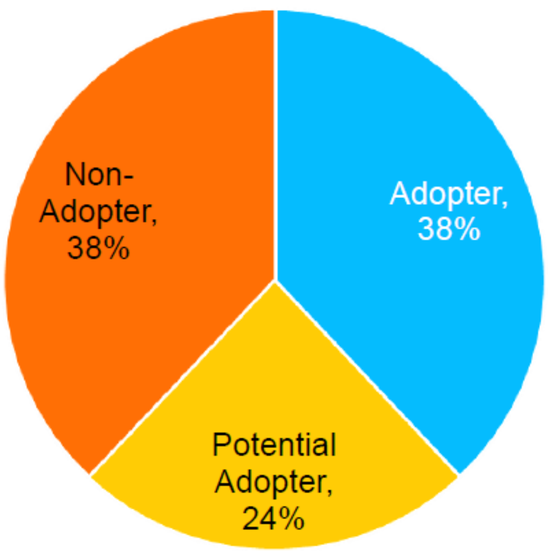
Santa Clara, CA 95054

Appendix

Methodology for Consumer Survey Presented in this Study

A Web-based survey was completed by 1,263 respondents in the United States and Canada. Respondents included adopters, potential adopters, and non-adopters (no intent to adopt). Respondents represented households in urban, suburban, and rural areas.

Adoption of Smart Home Technology

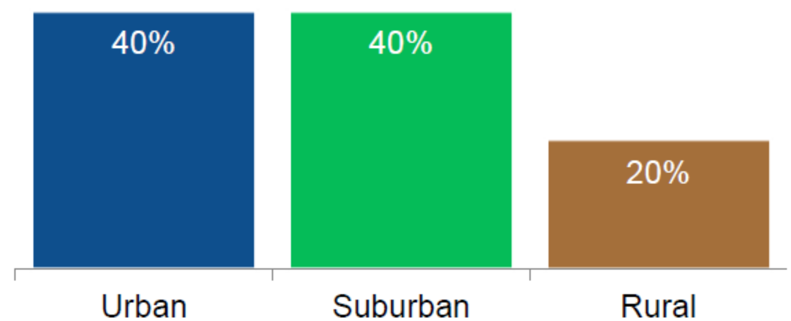


Country

US *(n=1,057)* = 84%

Canada *(n=206)* = 16%

What type of area do you live in?



Note: Due to rounding, percent values in some of the exhibits in this study may not sum to 100.

Source: Frost & Sullivan

The Frost & Sullivan Story

Frost & Sullivan Brings a Global Perspective