

iotega is ... safer, smarter living



Until quite recently, the concept of the connected home was the stuff of novels and TV shows, reaching the public as part of a vision of a futuristic world in which people have control over virtually all aspects of their home life by speaking or pushing a button. However extraordinary the idea may once have been, it has in recent years taken flesh, becoming something not only possible but probable — a technological inevitability.

It is quintessentially human to want to make life at home easier. And it is not a modern human desire either. Stories of the ancient Romans, with their innovations in building materials and plumbing, attest that, even millennia ago, one of the marks of an evolving society was in the time and energy it invested in its home innovations.

Before the emergence of the Internet of Things, a homeowner was ahead of the curve if they had a home security system in place. Bonus points went to those who had any combination of (a) lighting set to a timer, (b) a remote-operated garage door, and (c) the Clapper.

Gradually, as technology became more affordable, companies began developing home automation



products. Product popularity resulted in more investment, which in turn resulted in even cheaper and more efficient products. With 2020 on the horizon, the connected home has reached the point where people barely notice it anymore. It is now possible for consumers to control their heating and cooling, lighting, TVs, alarms, and doors from controllers and smartphones.

Concept on the rise

One prominent market research report¹ predicts the global home

automation system market to leap from a value of USD 39.93 billion in 2016 to USD 79.57 billion by 2022. This ties in with what Cisco predicted in its 2013 paper “The Internet of Everything: Global Private Sector Economic Analysis²” that:

...\$14.4 trillion of value will be ‘at stake’ over the next decade [2013 to 2022], driven by ‘connecting the unconnected’ (people-to-people, people-to-machines, machines-to-machines, etc.) via the Internet of Everything.

Value at Stake is the potential bottom-line value that can be created, or that will migrate among private-sector companies and industries, based on their ability to harness the Internet

SECURITY: iotega features robust, cyber secure PowerG technology with end-to-end 128-bit AES encryption, which ensures a hack-proof security system.

WIRELESS COMMUNICATION: iotega supports Wi-Fi, Z-Wave Plus, and Ethernet, together with optional 3G and LTE* communicators which work with a preferred offering of security and home automation devices.



“ The idea that you can control such “home factors” as temperature and lighting from a handheld device would have been difficult to conceive of even a generation ago.

of Everything over the next decade. Cisco predicts that this Value at Stake will be \$14.4 trillion for companies and industries worldwide over the next 10 years.

More specifically, over the next 10 years, the Value at Stake represents an opportunity to increase global aggregate corporate profits by about 21 percent.

In other words, from 2013 through 2022, \$14.4 trillion of value (net profit) will be ‘up

for grabs’ for private-sector businesses globally — driven by the Internet of Everything (IoE).

This just-beginning boom comes as no surprise considering the ubiquity of smartphones and the widespread use of other “always connected” digital devices such as tablets. It is natural that people should go from asking if their device can connect them to their friends, colleagues and media to asking if it could connect them to the place where they spend most of their time.

The smart home of the future

All but the most stubborn Luddite would agree that smart homes make people’s lives better, or at least easier to manage and more convenient. The idea that you can control such “home factors” as temperature and lighting from a

handheld device would have been difficult to conceive of even a generation ago.

But smart homes are not just “cool.” Set up the right way, they can provide excellent security, whether that security is in the form of a standard burglar or fire alarm, auto-door locking and unlocking, auto-calling of police and fire services, and smart lighting.

As a concept, the smart home is coming into its own. At a time of now widespread broadband connectivity, and the proliferation in the home of devices such as smartphones, tablets, and smart TVs — many of which can control home appliances such as cameras, sensors, smart meters, lighting, and HVAC — it is now technologically possible to activate a connected home.

Barriers to adoption

Projections for the smart homes market speak to a bright future.

Here are a few statistics:

- The smart homes market will be worth USD 58.68 billion by 2020³
- The market will be worth USD 121.73 billion by 2022⁴
- The market will grow from USD 15.6 billion in 2016 to USD 43 billion in 2020⁵
- Consumer spend on smart home automation will hit \$100 billion by 2020⁶

While there is “play” in these numbers in the precise details, the conclusion is invariably the same: that the smart home market is bursting at the seams and ready to explode. Nevertheless, there are many challenges facing the industry, and many psychological hurdles prevent-

ing consumers from committing en masse to smart home technology. Among these challenges:

- **Concerns around security:** Consumers, both those who have smart homes and those who are considering establishing one, have never been more concerned about security in general and the security of their connected devices in particular. Consumers who are on the fence want to avoid exposing themselves and their families to risk.
- **Dollars and cents:** There is a feeling among consumers that smart home technology, being quite new, will go obsolete quickly. Consumers will often stack this fact against a product’s price and think, perhaps not unreasonably, that it is too expensive.

- **Technological fragmentation:**

So many networks, standards, and devices in smart homes gives rise to interoperability issues and confusion on the part of consumers, who must set up and use (or fear they must set up and use) multiple devices.

iotega security

In the Wikileaks age, security is never far from the mind of homeowners considering a connected home system. The iotega wireless security system answers this gigantic question with robust PowerG technology⁷ and end-to-end 128-bit AES encryption.

“ There are many challenges facing the industry, and many psychological hurdles preventing consumers from committing en masse to smart home technology.



In a 2008 paper⁸ about encryption, data storage company Seagate concluded that:

- 128-bit encryption is sufficient to address all commercial and non-top secret government applications;
- the vulnerabilities for data leakage are not due to encryption key size when 128-bit keys are deployed, but to software, key storage and authentication vulnerabilities; and
- when all issues and vulnerabilities around software, key storage and authentication are addressed, the data protection solution that deploys 128-bit AES encryption provides comprehensive security for virtually every need.

Seagate put an exclamation point on the point that 128-bit is sufficient by setting up the following scenario:

- Every person on earth (seven billion) with 10 computers
- Each computer capable of testing 1 billion key combinations per second
- On average, a key can be cracked after testing 50 per cent of all possibilities

The conclusion is powerful: that the earth's population would be able to crack one encryption key every 77 septillion (77,000,000,000,000,000,000,000,000) years.

Many consumers take a do-it-yourself approach to connecting and securing their home and business, purchasing devices online and trying them out — adding to their network one piece at a time, on an as-needed basis. They will often start with remote monitoring and security, and from there move on to such elements as lighting, voice assistants, entertainment systems. However, the reality is that many consumers, especially home consumers, lack the knowledge, time and/or patience to set up off-the-shelf devices.

A connected home solution like iotega, which is easy to install and lets users range from a security-only setup to a full security and home automation solution, is one that anticipates the future and an ever-expanding Internet of Things¹⁰.

iotega simplicity and scalability

The smart home has arrived. Gartner predicts⁹ that the average

family home could contain more than 500 smart devices by 2022 — that's less than five years away.

References

- ¹ <http://www.marketsandmarkets.com/Market-Reports/home-automation-control-systems-market-469.html>
 - ² http://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-economy-faq.pdf
 - ³ <https://www.statista.com/statistics/420755/global-smart-homes-market-value/>
 - ⁴ http://www.marketsandmarkets.com/Market-Reports/smart-homes-and-assisted-living-advanced-technologie-and-global-market-121.html?gclid=EAlaIQobChMzl-tpYiJ1QIVxksNCh0KzgYCEAAAYASAAEgKkfd_BwE
 - ⁵ <https://www.forbes.com/sites/phillipkeys/2016/09/01/who-will-win-in-the-broken-connected-home-market/#35ddd9e8102b>
 - ⁶ [https://www.juniperresearch.com/press/press-releases/smart-home-revenues-to-reach-\\$100-billion-by-2020](https://www.juniperresearch.com/press/press-releases/smart-home-revenues-to-reach-$100-billion-by-2020)
 - ⁷ <http://site.geoarm.com/pdfs/DSC/Neo/dsc-powerg-wireless-technology-brochure-english.pdf>
 - ⁸ <http://www.axantum.com/AxCrypt/etc/seagate128vs256.pdf>
 - ⁹ <http://www.gartner.com/newsroom/id/2839717>
 - ¹⁰ <https://www.ericsson.com/en/mobility-report/internet-of-things-forecast>
- * Only available in the US

About Tyco

Tyco and its portfolio of brands form one of the largest security portfolios in the world. Engineers specializing in video security, access control, location-based security, and intrusion security give Tyco a competitive advantage when it comes to system integration. The company's focus is on turning data from sensors and systems into sharp insights and services that can solve those challenges and improve its customers' operations and performance. With more than a billion sensors and devices already in place across the globe, Tyco is in a unique position to deliver that future and make the Internet of Things work for its customers. Visit www.tycosecurityproducts.com to find out more.

About Johnson Controls

Johnson Controls is a global diversified technology and multi industrial leader serving a wide range of customers in more than 150 countries. Our 120,000 employees create intelligent buildings, efficient energy solutions, integrated infrastructure and next generation transportation systems that work seamlessly together to deliver on the promise of smart cities and communities. Our commitment to sustainability dates to our roots in 1885, with the invention of the first electric room thermostat. We are committed to helping our customers win and creating greater value for all our stakeholders through strategic focus on our buildings and energy growth platforms. For additional information, please visit johnsoncontrols.com or follow us @johnsoncontrols on Twitter.

About Johnson Controls' Building Technologies and Solutions

Johnson Controls' Building Technologies & Solutions is making the world safer, smarter and more sustainable – one building at a time. Our technology portfolio integrates every aspect of a building — whether security systems, energy management, fire suppression or HVACR — to ensure that we exceed customer expectations at all times. We operate in more than 150 countries through our unmatched network of branches and distribution channels, helping building owners, operators, engineers and contractors enhance the full lifecycle of any facility. Our arsenal of brands includes some of the most trusted names in the industry, such as Tyco®, YORK®, Metasys®, Ruskin®, Titus®, Frick®, PENN®, Sabroe®, Simplex® and Grinnell®. For more information, visit johnsoncontrols.com or follow @JCI_Buildings on Twitter.

Copyright © 2017 Tyco Security Products. All Rights Reserved. TYCO, TYCO SECURITY PRODUCTS, IOTEGA and the product names listed in this document are marks and/or registered marks. Unauthorized use is strictly prohibited.