PARKS
ASSOCIATES

Residential Security and Encryption: Setting the Standard, Protecting Consumers

A Parks Associates Whitepaper Developed for Qolsys

Qolsys
QUALITY OF LIFE

Residential Security and Encryption: Setting the Standard, Protecting Consumers

The security industry needs to evolve to meet the challenges of cybersecurity threats. Unencrypted sensors and lack of firewalls and panel security open companies to litigation and expose consumers to danger. Dealers have an obligation to understand the evolving threats from cybersecurity attacks, select partners that have addressed known vulnerabilities, and put mechanisms in place to quickly respond to new threats as they emerge. This whitepaper outlines specific threats to sensors, security panels, and network connections that security dealers need to address.

The Challenge of Cybersecurity

As security and smart home converge, ignoring the cybersecurity threats targeting these systems can cost home security dealers millions and do lasting damage to their brands and the industry as a whole.

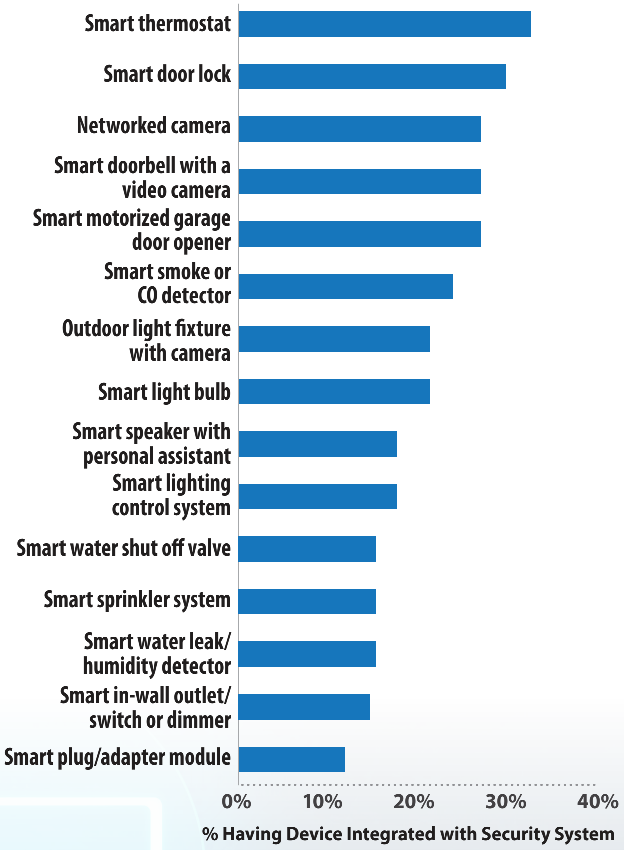
> The ongoing cat-and-mouse game between hackers and cybersecurity experts requires constant vigilance.

Increasingly, security systems and smart home devices are integrated in the connected home.

What is assumed to be secure today is often not, as hackers find new weaknesses and develop tools to exploit them. When implementing a cybersecurity solution, security system providers need to consider all components and connections to the system, from the wireless connection between the sensors and the panel to the panel's connection to the cloud. Every link in the chain must be secure. Both consumers and security dealers expect that security systems are secure, yet the reality is that many of the systems installed today have known vulnerabilities.

Smart Home Devices: Integration with Security System

U.S. Broadband Households that have a Security System with Home Control



© Parks Associates

Dealers have an obligation to understand and address the security shortcomings in the systems they are installing.

The National Institute of Standards and Technology (NIST) has developed a cybersecurity framework that outlines cybersecurity measures that fall under five areas: identify, protect, detect, respond, and recover.[1] It is to "facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks."

This framework describes voluntary standards, but it is only a matter of time before mandatory cybersecurity standards are enacted. For the security industry, the question is whether the industry will wait for regulators to mandate encryption or other cybersecurity standards or move voluntarily. While compliance is still voluntary, security dealers have the opportunity to evaluate the risk versus the cost of installing security systems that address cybersecurity threats.

In the early 1960s, car manufacturers did not include seat belts in every car, mostly due to the added cost. Seatbelts became mandatory in 1968. Prior to that date, manufacturers weighed the risks and benefits versus the cost of adding this basic safety features to automobiles.

If you are a security dealer today, you should be asking yourself, **"Am I okay selling a car without seatbelts?"**

Security dealers must weigh the costs versus the benefits of compliance with cybersecurity best practices. The costs are clear. Encrypted sensors cost more than unencrypted sensors. Upfront costs for security panels with greater protection against hacking may also be more expensive.

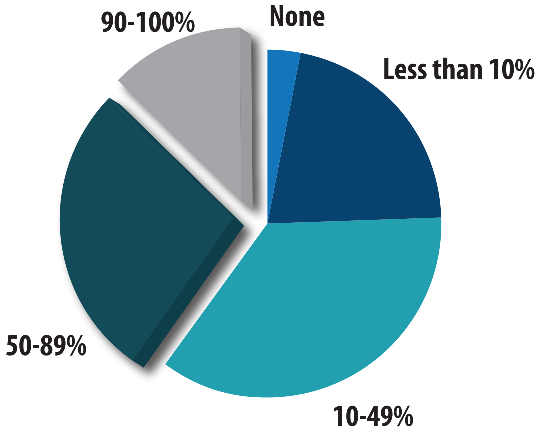
The benefits from the additional costs are less direct. Do residential customers know or understand the difference, and are they willing to pay more for an encrypted solution? Are residential consumers making the assumption that the security system they are buying is already encrypted, when in fact it is not?

Smart Home Installations – Adding Risks to Security Systems

More and more security installations include smart home devices, which are increasingly the target of cyberattacks. In Parks Associates' *Security Dealer Survey*, U.S. dealers estimated that 75% of their security system sales include at least one smart home device.

Residential System Installations Including a Smart Home Device (Q3/17)

Among Security Dealers Selling Systems with Interactive Services



© Parks Associates

SECURITY DEALERSTUDY
Smart Home and DIY Systems

[1] https://www.nist.gov/cyberframework

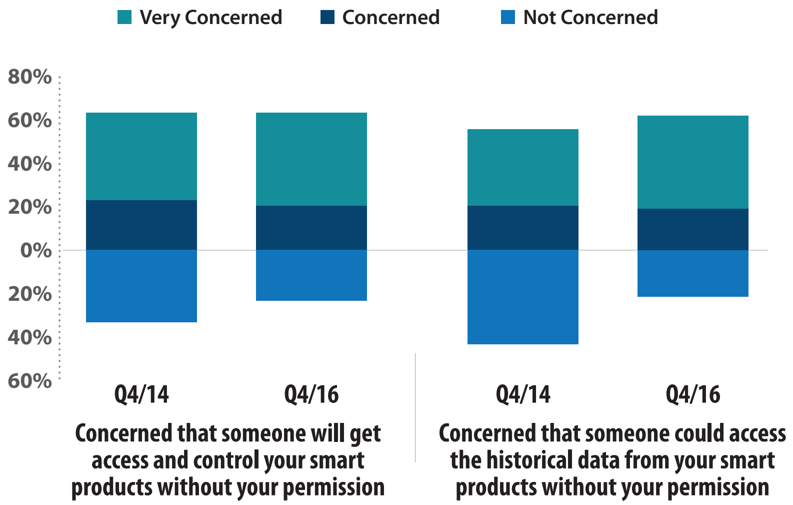
Security Consumers: Attitudes and Beliefs

Consumer concerns about data security are rising, creating an opportunity for security dealers willing to respond accordingly.

- 64% of U.S. broadband households are concerned about security and privacy when using their connected devices.
- Almost half of consumers are "very concerned" about hackers getting control of devices and accessing data.
- In the past two years, the share of "very concerned" has increased, and the share of "not concerned" has decreased by about half.

Concerns About Hacking of Smart Products

U.S. Broadband Households

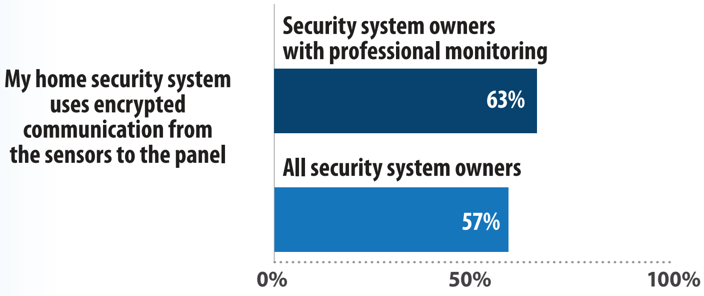


© Parks Associates

It is clear that consumers do understand and expect connected products to address cybersecurity threats.*

> While most consumers do not know whether their sensors are secure, **63% of professionally monitored subscribers** believe these signals are encrypted already and would be surprised to find that they are not.
>
> © Parks Associates

Owner Beliefs/Expectations for Cybersecurity of their Security Systems: Communication



© Parks Associates

The cost of allowing these customers to remain vulnerable to potential cyberattacks can be tremendously high even if the systems are not hacked. A major security firm recently settled a multimillion-dollar lawsuit regarding claims its network was secure while its sensor communications were not encrypted. Dealers have to weigh the cost of cybersecurity measures against potential legal ramifications of installing systems with known vulnerabilities.

* Parks Associates conducted an online survey of U.S. security system owners in 1Q 2018 to gauge their beliefs on the cybersecurity settings and status of their system. The survey included 312 security system owners, with 259 that have professional monitoring, and the security consumer charts on pages 4, 8, and 12 are derived from this survey.

Dealers can focus on three key areas – **the sensors, the panels, and the network** – to ensure they are aware and address the potential vulnerabilities in a security system.

Sensor Security

In the 1980s ITI developed a one-way protocol for communication with wireless sensors that has proliferated throughout the security industry. When initially developed, this technology was costly and complex. The radio protocols were proprietary, and attempting to interfere or copy their signals was not only illegal but required expensive signal interception technology.

Today's security dealer might be surprised to find that the signaling technology utilized today hasn't changed. As each sensor transmits its information, it provides notification of the sensor function; battery status, which defines the sensor battery state; sensor supervisory to communicate the sensor status; and tamper. While different security panel manufacturers use different frequencies, most still use this one-way communication scheme from the sensor to the panel that was invented in the 1980s.

Keychain remotes using legacy technology are vulnerable to a replay attack.

The wireless transmissions are the same every time a door sensor is activated or a key fob disarms the system, and the communication is not encrypted, so this system of communication is vulnerable to a replay attack. In a replay attack, someone simply records the wireless communication signals and later plays the signals back using signal interception technology that today has become accessible and affordable, and become the subject of multiple articles with news sources such as Wired, Forbes, and Good Morning America.

Anyone can easily purchase these "software-defined radios" on the internet and research the technology and methodology for this attack on different websites. When one of these devices replays a sensor's signal, the security system will respond as if the signals came from the actual sensor in the home. **To protect against these threats, wireless sensor communication must be encrypted so that each signal received by the system is protected.**

Leveraging Military Grade Security Technologies

Israel-based manufacturer Visonic, purchased by Tyco in 2011, leverages military-grade electronic security technology in its PowerG two-way communicating sensors that include 128-bit AES encryption. Two-way communication allows the sensors and the panel to exchange keys for encryption. PowerG has military grade, frequency-hopping technology with vastly superior range over the legacy protocols, including intelligent signaling auto adjustment to reduce battery strain in less challenging installations. While this encryption capability has been in market for a number of years and has been widely used in commercial applications, most panels and sensors used in residential applications do not utilize encrypted sensor technology.

Economics and an inherent resistance to change have been the primary drivers behind the decision to stay with one-way, unencrypted sensors.

Residential dealers want a low-cost sensor with wireless encryption and excellent battery life. One-way sensors have a single radio and therefore consume less power than sensors with two-way communication, while sensors with two-way communication and frequency hopping are more costly than traditional sensors.

Further, with millions of security sensors already installed, transitioning to encrypted sensors will not happen overnight. Dealers moving to encrypted technology will need to support the legacy standards while evolving to secure encrypted sensor technology. This will require security panel manufacturers to enable backwards compatibility for legacy sensors while providing the latest in sensor encryption technology.

While these constraints have challenged this industry for years, the technology is becoming more accessible and affordable as software and hardware engineers focus on bringing new solutions to market.

Qolsys
QUALITY OF LIFE

Silicon Valley-based security and smart home manufacturer Qolsys has developed a good/better/best solution. The IQ Panel 2, an all-in-one 7" touchscreen with built in panel camera supports:

Good: Backward compatibility for legacy sensor protocols (319.5 MHz, 345 MHz, 433 MHz,)

Better: S-Line (Secure line) Encrypted 319.5 released in 2016 concurrent with the release of its IQ Panel 2

Best: PowerG sensor portfolio with industry best range and 2-way encrypted communication

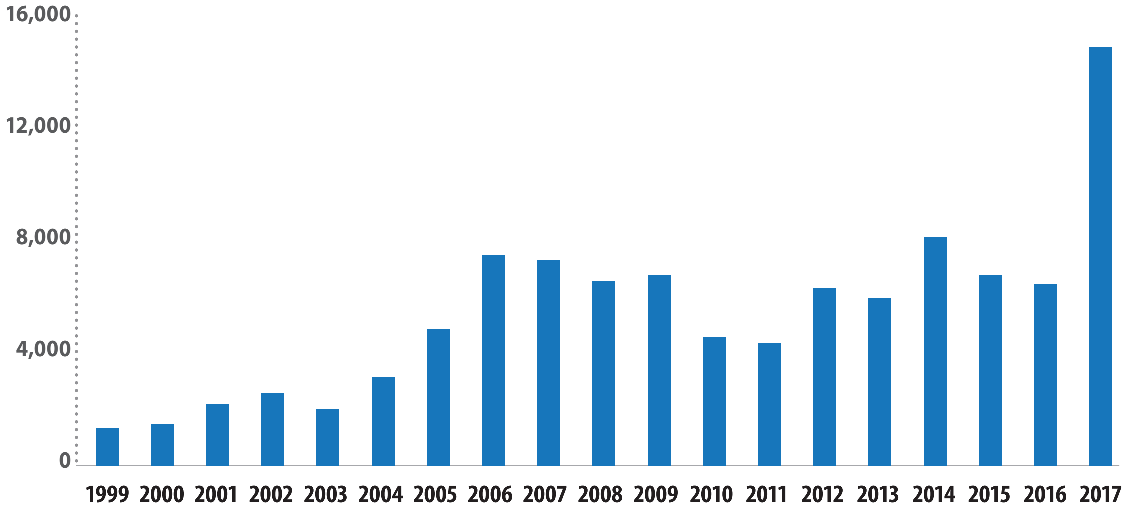
Panel Security

Security dealers trying to establish their place in the market are working to leverage the convergence of IoT and security. IoT solutions add new value to a security system but also open it to more cybersecurity threats. The security panels that allow dealers to leverage these newer technologies must be protected from cyberattacks.

The National Institute of Standards and Technology has developed a vulnerability scoring system that takes into account the attack vector (source of attack), the attack complexity, the privileges required, user interaction required, and impact on confidentiality, integrity, and availability. Based on this system, cybersecurity experts are discovering and addressing security vulnerabilities in increasing numbers.

> Many security control panels use a Linux-based operating system, and in 2017, nearly 15,000 vulnerabilities were identified in Linux.[2]

Linux Security Vulnerabilities



Source: www.cvedetails.com © Parks Associates

Once someone gains access utilizing one of these security vulnerabilities, they plant code that can be activated at a later date. This is called an advance persistent threat (APT). Today, hackers plant code in millions of devices and then sell distributed-denial-of-service (DDoS) attacks via marketplaces on the Clearnet and Darknet. A small DDoS attack is available on the dark web for $90/day. The vendors offering DDoS attacks simply send commands to millions of unsecure devices that were previously hacked to execute the attack.

On average it takes 205 days for companies to discover these advanced, persistent threats. In the extreme, it took one company eight years to discover the issue.[3] Over 90% of the DDoS issues are discovered and reported by a third party, not the company responsible for the products.[4]

[2] www.cvedetails.com

[3] https://www.infosecurity-magazine.com/news/hackers-spend-over-200-days-inside/

[4] https://www.csoonline.com/article/2131881/critical-infrastructure/advanced-persistent-threats-can-be-beaten--says-expert.html, M-Trends Report, FireEye

The security industry, like every industry, has to move aggressively to assure that as vulnerabilities are identified, the security patches are installed as soon as they are available and on the entire installed base of products, not just new systems.

Preventive layers, such as firewalls and systems that require every process to be authorized and have a token to operate, must be in place to mitigate the risk of infection.

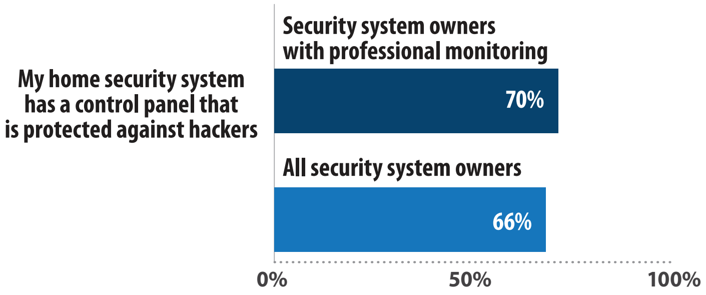
Identifying and containing attacks that get through defensive strategies is also essential. Identification and containment require companies to have visibility into the applications and interactions and precise control over security policy. Visibility and precise control strategies are essential to identify suspicious activity and stop it immediately.

The security industry also has unique attack vectors that have to be addressed. For example, flooding the panel with millions of sensor signals, or “jamming,” is a form of denial of service attack on the security panel itself. Instead of shutting down, or attempting to process the influx of events, the panel must identify the jamming activity and treat it as an attack, notifying the central station.

In addition, the security industry must manage user credentials and provide tools to simplify authentication, providing both a seamless and highly secure user experience. Employing measures such as video verification of an arm or disarm event adds a layer of security onto existing authentication methods. Similarly, managing access codes for door locks through the security panel provides an additional layer of security, ensuring that only active codes are being used.

> Consumers expect that the industry is addressing all of cybersecurity threats impacting control panels—**70% of professionally monitored security subscribers** believe that their control panel is protected from hackers.
>
> © Parks Associates

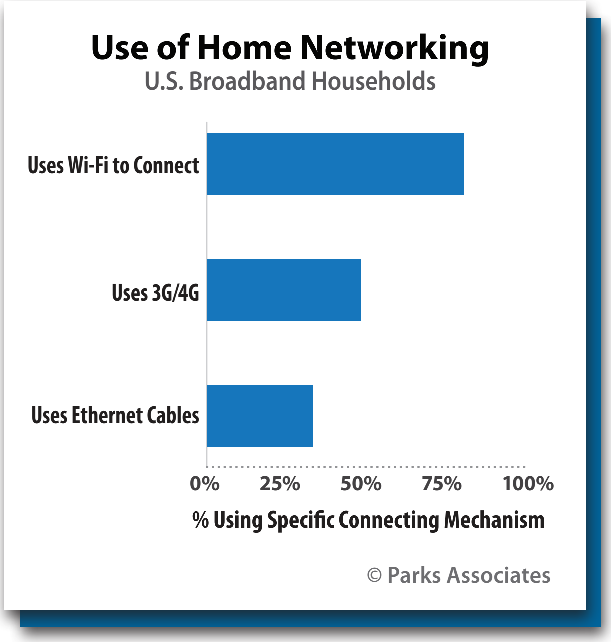
Owner Beliefs/Expectations for Cybersecurity of their Security Systems: Hacker Protections



© Parks Associates

Network Security

The network connection to the security panel is a third area of concern. The wireless network that connects the panel to the interactive service provider and central station is vulnerable to passive monitoring and unauthorized access attacks.[5]



Passive monitoring is a key vulnerability of wireless networks.

Bad actors near the physical location can listen in to the conversation by using packet sniffers. Encryption defends against passive monitoring, but encryption technology is constantly evolving. Wired Equivalent Privacy (WEP) was the standard in the early days of Wi-Fi until security vulnerabilities were discovered and the industry shifted to Wi-Fi Protected Access (WPA). Weaknesses in WPA led to the introduction of Advanced Encryption Standard (AES), which is part of WPA2.

Recently a team of researchers exposed weaknesses in WPA2, which is the predominant encryption method protecting Wi-Fi networks today. An attacker within range of a network can exploit these weaknesses using key reinstallation attacks (KRACKs) to read information that was previously assumed to be safely encrypted.

Unauthorized access attacks can be accomplished by looking for network backdoors. Bad actors conduct a TCP scan to look for open, unsecured ports. When found, those open ports may allow direct access to sensitive information or enable them to lower the defense by disabling or reconfiguring network security settings. It is essential for products to lock down all ports except those that connect to legitimate destinations and services.

While closing ports and limiting communication to and from legitimate sources is essential, it is by no means sufficient. Man-in-the-middle attacks impersonate legitimate connections such as those of the service provider.

Encryption, like operating system software, must be upgradable to address not just today's threats but tomorrow's as well.

By exploiting the Address Resolution Protocol (ARP), which translates IP addresses into MAC addresses, a "man in the middle" can falsely claim that they have the MAC address of the interactive service provider, enabling the bad actor to gain access to the panel. Authentication is a must to defend against this type of attack.

Passwords, certificates, and an authentication service are required to assure that apparently legitimate connections are in fact legitimate.

[5] Wireless LAN Implications, Problems, and Solutions, Jim Geier, 2015

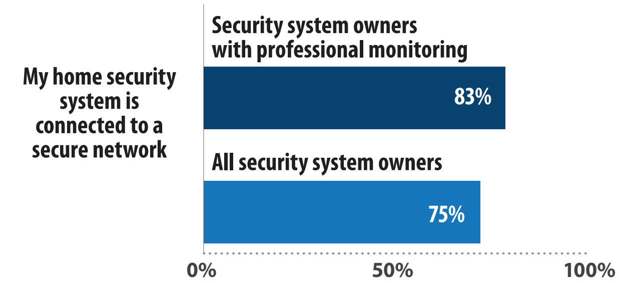
Role of the Dealer in Network Security

The dealer also has a role to play in preventive network security actions. Measures such as network firewalls and network passwords can be added as a prevention layer, and the dealer, as an authority in the security industry, is well positioned to offer advice and additional services. ADT recently announced a preventive network service in conjunction with Symantec's Norton Core. Branded as a cybersecurity service, this solution addresses the preventive measures associated with network security.

Just as the case with sensor encryption and panel security, consumers expect that the industry is addressing all of the network cybersecurity threats.

> **83% of professionally monitored security subscribers** believe that their residential security system is connected to a secure network.
>
> © Parks Associates

Owner Beliefs/Expectations for Cybersecurity of their Security Systems: Network Security



© Parks Associates

Evaluating Cybersecurity of Vendors

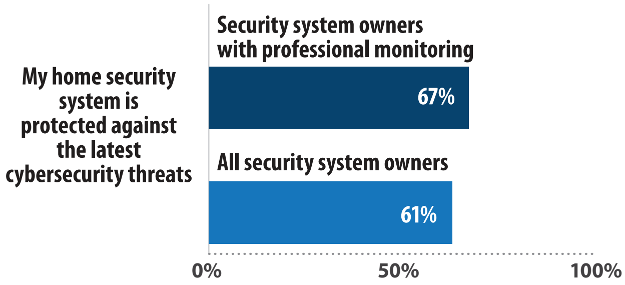
By evaluating the cybersecurity capabilities of vendors, dealers can protect themselves and their customers against cybersecurity threats.

Panel vendors have the obligation to inform dealers how they address each of the cybersecurity threats identified in this paper:

1. Sensor security, protection from a playback attack, encryption
2. Panel operating system security, system for timely patching of security threats
3. Preventive and containment panel security measures
4. Systems for addressing security industry specific threats such as jamming
5. Systems for safeguarding, enhancing, and protecting end-user credentials
6. Network security measures including locking down ports and authentication services

> **67% of professionally monitored security subscribers** believe that their security system is protected against the latest security threats.
>
> © Parks Associates

Owner Beliefs/Expectations for Cybersecurity of their Security Systems: Control Panel



© Parks Associates

Although dealers are not legally compelled to take measures to assure that the security systems they install address known security vulnerabilities, **the cost of not doing so is increasing.** New products are available that address these cybersecurity threats.

Now is the time to study the options, protect your business, and ensure that your customers remain secure.

About Qolsys

Qolsys is a Silicon Valley based security and smart home manufacturer providing state of the art residential and small business solutions to security and home automation dealers across North America. Its flagship product, the IQ Panel 2, features a 7-inch HD touchscreen, a built in 5MP Camera, and the Qualcomm Snapdragon SOC with multiple radios in an ultra-thin form factor. The IQ Panel 2 features several security specific features, including the ability to utilize both S-Line and PowerG encrypted sensor technology, a built in firewall, cloud token authentication to protect the only 2 open ports on the system, visual verification via the built in 5 megapixel panel camera, Bluetooth Touchless Disarming for up to 5 smartphones, eliminating the need for vulnerable keyfobs, and several industry firsts, including a 7" high-definition capacitive touchscreen with an intuitive graphical swipe-based user interface, Dual Path and cloud connectivity over LTE and Wi-Fi for intelligent redundancy, reliability and speed. It also features Z-Wave Plus support for home automation devices; two-way voice, standard 24-hour lithium-ion battery, UL-rated siren, a built-in Glass Break Detector, the ability to view live video cameras on the screen, powerful system health diagnostics and over the air software updates. The IQ Panel 2 is the most powerful security and smart home solution you can buy. The IQ Panel 2 was named a Top 30 Award Winner by SSI for 2017 and previously earned the prestigious 2016 TechVision Challenge award, a form of "Best in Show" at the Electronic Security Expo (ESX).

Qolsys IQ Panel platforms are powered by Android and are tightly integrated with Alarm.com's market-leading connected home services platform, supporting interactive security, video monitoring, energy management and home automation, resulting in increased conversion, end-user satisfaction, fewer dealer truck rolls, improved customer support and decreased total cost of ownership. Learn more at http://qolsys.com.

Parks Associates is an internationally recognized market research and consulting company specializing in emerging consumer technology products and services.

Parks Associates is an internationally recognized market research and consulting company specializing in emerging consumer technology products and services.

The company's expertise includes the Internet of Things (IoT), digital media and platforms, entertainment and gaming, home networks, Internet and television services, digital health, mobile applications and services, support services, consumer apps, advanced advertising, consumer electronics, energy management, and home control systems and security.

For more information, visit **parksassociates.com** or contact us at **972.490.1113** / **info@parksassociates.com**

About The Author

Tom Kerber, *Director, IoT Strategy,* Parks Associates

Tom leads Parks Associates research in the areas of home controls, energy management, and home networks. Tom authors numerous reports on energy management and home controls covering the evolution of technology, partnership opportunities, and new business models. Tom's work at Parks Associates includes managing consumer surveys that track trends and market opportunities and enable insightful evidence-based forecasting for energy, security, and home controls. Tom speaks frequently at key industry events, and his views are sought out by national press organizations and publications.

INDUSTRY EXPERTISE: Residential Security, Smart Home Products and Services, Home Network Technology, Software Systems, Electric Utilities, AMI, Home Energy Management, Demand Response

Twitter ID: @TomAKerber

ATTRIBUTION—**Authored by Tom Kerber.** Published by Parks Associates. © Parks Associates, Addison, Texas 75001. All rights reserved. No part of this book may be reproduced, in any form or by any means, without permission in writing from the publisher. Printed in the United States of America.

DISCLAIMER—*Parks Associates has made every reasonable effort to ensure that all information in this report is correct. We assume no responsibility for any inadvertent errors.*