Beyond the IoT Hype: A Primer for Security Dealers

Wicked or wickedly good Internet of Things impacts home security, smart home, appliances.

By Bill Zalud
January 15, 2015

Craving more hype? Then say hello to the Internet of Things (IoT). IoT will be everywhere, will do everything, will touch everyone — and generate trillions of dollars. It will be on every wrist, imprinted into bike shorts and on cans of green beans; it will reside in every home, office, factory, hospital room, school desk, and tent worldwide. The mighty IoT may one day spew out data streams of monoicosebyte proportions, all seemingly in a nanosecond. (Monoicosebytes are 9x exponential steps beyond the terabyte.)

If you’re counting, it will be the fourth industrial revolution — the ultimate tipping point. The paramount of all paradigm shifts. The most disorderly of disruptive technologies.

IDC, a global tech market intelligence firm with an awesome ability to count objects before they exist, claims the installed base of connected things will be 212 billion by the end of 2020. These IDC crystal-ballers say Internet of Things will be “a new construct in the information and communications tech world,” and they peg IoT spending at $8.9 trillion by 2020.

Predictable with any market “ready to explode,” there is even more research to prove the point.

In its “2014 State of the Internet of Things” study, Accenture Interactive, which advises marketing and digital clients worldwide, says that 69 percent of all consumers plan to buy an in-home IoT device in the next five years. By the end of 2015, about 13 percent of consumers will own an IoT device — smart thermostats and Internet-connected security cameras are examples. Currently, only about four percent have even one such device.

Taking into account those who already own such products, Accenture Interactive ticked off connected devices expected to be most popular over the next few years:

- Connected security systems (11 percent expected adoption in the next year; 35 percent in the next five years).
- Smart thermostats (13 percent projected adoption in the next year; 43 percent in the next five years).
- Wearable wellness devices (22 percent expected adoption by 2015; 43 percent adoption in the next five years).
Eagerly sitting at the connected home table or ready to grab a seat, companies from giant-sized Google to pint-sized AAAA Security Services, are salivating over this looming feast. The trouble is there’s no tangible IoT infrastructure; no fully accepted new-and-improved Internet (like next-generation IPv6); no across-the-board standards; not enough living engineers to build the IoT; no sufficient battery life to make little things tick-talk for very long. So hold onto your quad core smartphone: Things aren’t really talking to other things like the IoT “sell” says.

Today and into the near future, the closest IoT nirvana gets is the Internet of Some Things: a smart TV, security video cameras each with an IP address, a smart thermostat, a smart water heater or, maybe, a smart home platform with a smartphone controller. Some things are connected, sometimes to each other; but more often, various devices and applications are not easily interoperable.

The IoT cheerleaders can’t even agree on a moniker for the Internet of Things. For example, Microsoft uses “Internet of Your Things.” On the factory floor it’s “machine-to-machine” or M2M. Cisco and Qualcomm like the “Internet of Everything.” Others prefer the Internet of Objects or Internet of Smart Objects.

It turns out the most-accepted term — Internet of Things — was coined by Procter & Gamble executive Kevin Ashton as an attention grabber to rouse snoozing grey flannels at a Cincinnati supply chain meeting in 1999.

Home security, automation, entertainment systems, home appliances, wearables and healthcare devices, as well as the smart home overall will, in the long run, turn into all things hung from the ubiquitous IoT. And this may possibly be boom or doom for security and smart home dealers and distributors, as well as home appliance manufacturers and their designers.

In some ways, “it’s already here,” comments Adam Justice, vice president of embedded and networking firm Grid Connect and board member of the IP for Smart Objects (IPSO) Alliance. “Connected locks. Connected light bulbs. Connected home energy management systems.” These and other examples are now providing value to consumers. It also lets some companies “get ahead of the competition,” he says.

Taking a measure of consumer interest in smart home applications and the Internet of Things, a survey commissioned by Savant Systems, known for its smart home involvement in the luxury and mid-market, discovered that more than half of consumers in the United States believe home automation will be an everyday feature less than 10 years from now, and nearly one-fourth say that the technology will be an everyday feature in less than five years.

The survey, conducted by GfK Custom Research, further reveals that control/ease of use (69 percent) and convenience (58 percent) are the most important features for consumers when purchasing a new technology. The bottom line is that consumers just want and appreciate things working together, adds Tim McInerney, director of product marketing at Savant. Cost savings (41 percent) and safety and security (35 percent) were cited as the two primary considerations among consumers for the adoption of smart home automation systems.

So, no matter hype or helpful, here today or waiting for tomorrow, it makes business sense to know more than a headline or two about IoT and its connections to the smart home.

Basically, the Internet of Things is the interconnection of uniquely identifiable embedded computing-like devices within the Internet infrastructure. It’s expected to offer advanced connectivity of objects, devices, systems and services covering a variety of protocols, domains and applications. Internet-connected objects sense, communicate, compute and potentially actuate as well as have intelligence, multimodal interfaces, physical/virtual identities and attributes.
Beyond these basics, things get dicey quickly.

Which gets us back to the IPSO Alliance, a resource center and thought leader for industries seeking to establish the Internet Protocol as the basis for IoT and M2M applications, according to its stated role. Earlier in 2014, the alliance stepped forward to broaden its Internet of Things standards vision to include education on the proper use of protocols to create end-to-end IoT solutions as well as to promote open standards using current and emerging IP technologies.

“As more standards organizations attempt to lay claim to the IoT, it was important to redefine our vision to ensure we are meeting the needs of our membership and, more importantly, of the design community at large,” says Pete St. Pierre, the alliance president and a member of the product management team for the Internet of Things at Oracle.

Adds Alliance Chairman Geoff Mulligan, a consultant recognized as a key developer of the embedded Internet, “We will publish two documents outlining open standards for interoperability among objects.” The first, he says, defines a simple and extensible set of smart objects that can build communication between devices used in smart energy, home automation and a host of other functions. The second outlines a conceptually simple architecture that can be used to build interoperable machine-to-machine and IoT applications.

“The ultimate goal is to define how to use the existing set of open standards, specifically IP, to build successful IoT products,” adds St. Pierre. “This can be done without creating new and complicated protocols in the future.”

“There’s no need to reinvent the wheel,” agrees Christian Légaré, IPSO member and executive vice president and CTO at Micrium, which makes embedded software components for engineers building microprocessor, microcontroller and digital signal processing-based devices for appliances, among other products. It’s a matter of showing people “how to use the IP protocol and reference architectures,” he says.

In addition to such show and telling, an inherent issue hampering IoT growth is the 40-plus year old IPv4 protocol, the fourth (Really the first; don’t ask.) version for the IP Internet. It routes traffic, among other functions, but limits the number of total address to 4,294,967,296, not nearly enough to handle all of that anticipated IoT traffic.

Enter IPv6, way back in 2006. It solves the address-limit problem and specifies a new packet format to minimize packet header processing by routers. Consider a packet like a letter: The header is the envelope and the data area is whatever is inside the envelope. Because IPv4 and IPv6 packet headers are significantly different, the two protocols are not interoperable; in essence, IPv6 is not backward compatible with IPv4. So network operators implementing IPv6 IoT will need to run a dual stack IPv4/IPv6 network for years to come. Mulligan suggests, “It’s really not hard to run a dual stack, not as difficult as people think. And it will become a critical necessity” when those billions of devices hang on Internet.

In addition, for IPv6 to work, it must be implemented end-to-end: IPv6 has to be enabled by everyone along the way — network hardware vendors, transit providers, access providers, content providers and endpoint hardware makers.

So, for numerous reasons, the shift to IPv6 is moving ahead but with lethargic speed; only by mid-2014 did IPv6 traffic go over four percent of total as compared with IPv4. Not many service providers are change-over activists. Observes Légaré: North America holds about 70 percent or so of worldwide IPv4 addresses and its service providers are “shy about investing in new gear after getting burned in the past.” In North America, Comcast Corporation, the mass media, home automation, broadcasting and cable company, is one of few
carriers to commit to IPv6.

There’s also a power challenge with IoT, “a need for next-generation power delivery that offers low power consumption and that transforms conventional styles of power supply,” advises Oleg Logvinov, director of special assignments in semiconductor firm STMicroelectronics’ Industrial & Power Conversion division. His company is a member of the IPSO Alliance and Logvinov is chair of the IEEE’s Standard for an Architectural Framework for the Internet of Things Working Group, among other IEEE standards group assignments.

One IoT challenge — security and its twin sister privacy — is a harder nut to crack.

“Security, particularly for critical infrastructure, is a key concern for end users owing to the number of attack points and potential magnitude of impact,” says Frost & Sullivan Industrial Automation and Process Control Senior Research Analyst Rahul Vijayaraghavan. “As the IoT market moves towards semi- and fully-autonomous control networks, end users will have limited awareness and control in the event of targeted attacks, heightening the risk of sudden disruptions.”

In June 2014, for instance, HP (Hewlett-Packard) released results of a study revealing that 70 percent of the most commonly used IoT devices contain vulnerabilities, including password security, encryption and general lack of granular user access permissions.

“While the Internet of Things will connect and unify countless objects and systems, it also presents a significant challenge in fending off the adversary given the expanded attack surface,” says Mike Armistead, vice president and general manager, Fortify, Enterprise Security Products, HP. “With the continued adoption of connected devices, it is more important than ever to build security into these products from the beginning to disrupt the adversary and avoid exposing consumers to serious threats.” Headlines already warn that some connected baby monitors and home security video cameras are being exploited. (To see results of SDM’s poll on this topic, visit http://www.sdmmag.com/polls/30/results.)

According to Vijayaraghavan, security is one of the “four pillars essential to facilitating a smooth transition into the IoT era. The others: communication, data management and networking.

So, without security, the IoT likely will not be widely adopted, contends Bill Boldt, senior marketing manager of security products at Atmel, which is a founding company of the Open Interconnect Consortium, with an aim to improve interoperability and define connectivity requirements for IoT devices across multiple vertical markets. Any IoT product requires the highest level of security possible, says Boldt. It is not just the data the IoT application generates that needs to be protected; some applications also store personal information, identities and log-in details for service providers that would certainly be a target for hackers.

Likewise, being able to access an IoT application that is controlling other appliances such as home security, life safety, heating and air conditioning systems would compromise system integrity and potentially have dire consequences. Also, manufacturers need to protect their IoT devices from being cloned and sold as counterfeit products in order to protect brand equity and preserve potential revenue streams, so security needs to have a layered approach.

To achieve this level of security, for example, Atmel has a range of hardware authentication and encryption devices containing methods of protecting secret keys that not only restrict access, but also provide key generation and management. Boldt points out that, “when securing secret keys, hardware key storage is stronger than software-only storage every time.” With cryptography engineering being built-in to IoT, developers and dealers do not need to be cryptography experts. Also, hardware countermeasures are employed on the devices to further protect security. These include a metal shield over the whole crypto-authentication device, no probe/test points and tamper detection algorithms.
A total approach can be Trusted Platform Module (TPM), which can be thought of as a microcontroller that can take a punch, and come back for more, Boldt contends. The TPM is a small integrated circuit with an on-board microcontroller, secure hardware-based private key generation and storage and other cryptographic functions (digital signatures, key exchange, etc.), and is a solid way to secure IoT end points, edge devices, email and Web access while protecting local data.

Privacy is yet another kettle of Internet of Things fish. Take fitness bracelets and wristwatches, which collect personal health information and store it in the cloud, as one example.

Perhaps most striking is Americans’ lack of confidence that they have control over their personal information, according to a report by the Pew Research Center’s Internet Project. That pervasive concern applies to everyday communications channels and to the collectors of their information, both in the government and in corporations, observes Mary Madden, the Pew report’s senior researcher. For example:

- 91 percent of adults in the survey “agree” or “strongly agree” that consumers have lost control over how personal information is collected and used by companies.
- 88 percent of adults “agree” or “strongly agree” that it would be very difficult to remove inaccurate information about them online.
- 80 percent of those who use social networking sites say they are concerned about third parties like advertisers or businesses accessing the data they share on these sites.
- 70 percent of social networking site users say that they are at least somewhat concerned about the government accessing some of the information they share on social networking sites without their knowledge.
- Yet, even as Americans express concern about government access to their data, they feel as though government could do more to regulate what others do with their personal information:
  - 80 percent of adults “agree” or “strongly agree” that Americans should be concerned about the government’s monitoring of phone calls and Internet communications. Just 18 percent “disagree” or “strongly disagree” with that notion.
  - 64 percent believe the government should do more to regulate advertisers, compared with 34 percent who think the government should not get more involved.
  - Only 36 percent “agree” or “strongly agree” with the statement: “It is a good thing for society if people believe that someone is keeping an eye on the things that they do online.”

Still another IoT obstacle is more perception than reality.

With 212 billion connected things — burglar alarms, smart thermostats, televisions, refrigerators, smart watches — all talking at once, will the future bode monster Internet break-downs? “Right now, only 16 percent of traffic is consumer goods,” points out Légaré. In emerging IoT, much of the traffic will be very short spurts of information — an alarm, temperature, pressure or humidity, for example — made up of short and frequent packets, he points out.

With IoT at a crossroads, it’s understandable that IPSO is sharpening its vision, spurred by the over-hype, carrier reluctance, market confusion and tech complications of such a mighty transition. Muddling the scene, some say, is the recent, sudden eruption of a packet-load of self-proclaimed framers of the IoT constitution, heavy-hitter groups driving particular tastes in architecture and — you can’t blame them — furthering their individual bottom line goals. For example:

**Thread** — Recognizing what it says is the need for a new, better way to connect products in the home, seven companies joined forces to form the Thread Group and develop Thread, an IP-based wireless networking protocol aimed at product developers. Founding members are Yale Security, Silicon Labs, Samsung Electronics, Google’s Nest Labs, Freescale Semiconductor, Big Ass Fans and ARM. The group will create
certification based on third-party testing to verify IoT product “quality, security and interoperability.”
Certified products will bear the Thread logo. Designed specifically for the home, its self-healing mesh
network model uses open standards and IPv6 technology with 6LoWPAN (IPv6 over Low power Wireless
Personal Area Networks) as a foundation and requires, according to the group, “just a software enhancement
for today’s 802.15.4 products.”

While Google itself is not a founding member (Nest Labs is), some industry observers suggest it’s behind the
wizard’s curtain. At the time of the writing of this article, the president of Thread, Chris Boross, is technical
product marketing manager at Nest and Google has made its home systems interest well known with the Nest
acquisition. Thread is quick to point out that Nest Labs joined the group before Google gobbled it up, however.

Open Interconnect Consortium — Technology firms Atmel Corporation, Broadcom Corporation, Dell, Intel
Corporation, Samsung Electronics and Wind River formed this group to improve interoperability and define
connectivity requirements for IoT devices across multiple vertical markets. Hinting at future certification
plans, OIC focuses, it says, on defining a common communications framework based on industry standard
technologies to wirelessly connect and intelligently manage the flow of information among personal
computing and emerging IoT devices, regardless of form factor, operating system or service provider. About
competing groups and efforts, OIC, in its Web site FAQ, states that “currently, we don’t see one single effort
that addresses all the necessary requirements.”

OIC specifications will use both existing and emerging standards such as Wi-Fi, Bluetooth, Wi-Fi Direct,
ZigBee, Z-Wave and Ant+, the latter an interoperability function added to base ANT (Advanced Network
Tools) protocol, an open access multicast wireless sensor net technology found in sport, wellness, home care
and remote control devices. OIC-branded devices will connect using many different operating systems,
including iOS, Android, Linux, Tizen, RTOS (real time operating systems) and others.

Influential semiconductor chipmaker Intel seems a natural at the OIC helm with Samsung Electronics
hedging its bets with representation here and in Thread. Both companies have been active lately. Samsung
Electronics entered into an agreement to acquire SmartThings, an open platform for the smart home and the
consumer Internet of Things. SmartThings supports an open and growing ecosystem of developers, who are
producing new types of connected devices and unique apps in the cloud. Then in mid-2014, Intel rolled out
what it calls the “world’s smallest standalone 3G modem” as part of its increasing investment in IoT for
connected home appliances, security devices, industrial systems and wearables. The chipset, just 300mm
squared, combines transmit and receive functionality with a fully integrated power amplifier and power
management, according to the company.

In October 2014, an OIC founder, Broadcom, exited the consortium. It is expected that, going forward, a
number of companies in this and other IoT standards organizations will shift their allegiance. Specific to
Broadcom, it reportedly left due to a disagreement over intellectual property.

AllSeen Alliance -- This group plans to drive widespread adoption of products, systems and services that
enable IoT, built upon an open, universal development framework. Premier members are Electrolux, Haier,
LG, Microsoft, Panasonic, Qualcomm, Sharp, Silicon Image, Technicolor and TP-Link. As of mid-August
2014, there were more than 60 members; so-called community members include AT&T Digital Life, Bosch,
Cisco, Cloud of Things, HTC, iControl Networks and Revolv, to name a few. Recently, Revolv has been
purchased by Nest and Revolv’s home automation hub will no longer be for sale and development has
stopped. The Linux Foundation-charged alliance now manages the AllJoyn (by Qualcomm) open source
project with software code using open standards. It also has “Designed for AllSeen” branding, its initial phase
certification program for validating products that implement AllJoyn properly, according to the alliance. At a
later time, it plans to introduce a more fully featured certification program with interoperability testing.
In mid-October 2014, Qualcomm said UK-based CSR will be acquired by Qualcomm Global Trading Pte. Ltd, an indirect wholly owned subsidiary of Qualcomm Incorporated. “The acquisition complements Qualcomm’s current offerings by adding products, channels, and customers in the important growth categories of Internet of Everything,” according to a company statement.

“The addition of CSR’s technology in Bluetooth, Bluetooth Smart1 and audio processing will strengthen Qualcomm’s position in providing critical solutions that drive the rapid growth of the IoT, including business areas such as portable audio, automotive and wearable devices,” says Steve Mollenkopf, chief executive officer of Qualcomm.

While Qualcomm knows its Allseen involvement will juice up AllJoyn and its CSR acquisition will broaden an anticipated Bluetooth with mesh offering, another of the Allseen group’s more recently onboard premier players, Microsoft, may see its own participation as a doorway into the smart home and office, thanks to the Microsoft Azure cloud platform, Windows devices and Xbox game console. On the official Microsoft Blog and posted in July 2014, Kevin Dallas, the company’s general manager, Internet of Things, wrote, “We believe the promise of IoT lies in making new and existing devices smarter by connecting them to services in the cloud.”

Another indicator: In mid-2014, Microsoft and American Family Insurance launched a business accelerator for startups focused on home automation. The accelerator will help next generation startups create advancements which lead to safer and smarter homes. “Home automation is ripe for startup innovation,” says Steve Guggenheimer, corporate vice president, developer experience and evangelism for Microsoft.

With more special interest groups than can fit in a Congressional committee room, will Thread, OIC and AllSeen and their muscle members be combatants or will they play nicely by working complementary slices of the total IoT pie?

Sorry, but togetherness may be a day late and a trillion dollars short. Battle lines are already drawn as consumer product makers roll out sky-rocketing numbers of Internet-connected burglar alarms, televisions, refrigerators, smart watches and slow cookers with myriad IoT-like solutions. It’s valuable to ask if history will repeat itself: Remember the infamous 1970s videotape format war with its consumer-bloodied Betamax versus VHS rumble? Four decades later, many smart home products on today’s market or near launch are incompatible with each other or different control platforms.

Always in fighting shape, “Google and Intel are competing; underlining protocols are all IP but they are competing now to some degree,” observes Légaré. Microsoft and Google also seem after the same things when it comes to IoT.

IPSO’s Mulligan is hopeful, however. “Frankly, we see ourselves as ‘big tent;’ we will embrace (others) as long as they talk open standards and don’t cause confusion. We are not saying we are the one and only way.” He sees more harmony than harm among alliances and consortia. His vision of the puzzle pieces fitting together: “View Thread as handling the lower level mesh layer underneath IP. View OIC as commissioning and providing security. And AllSeen as originally looking at a higher layer protocol space sitting on top of the Internet Protocol and using OIC for commissioning and security.”

Clearly, such groups influence IoT developments and help determine the role, product choices, installation needs, appliance designs and bottom lines of dealers, distributors, residential systems integrators, appliance designers, and product manufacturers as well as what finally is purchased, installed and used by consumers, businesses and government agencies.

If such efforts manage to “deliver the right set of platforms and services to realize the IoT opportunity,” as
Microsoft’s Dallas suggests, then some of the hyped excitement will turn into helpful reality. That may already be kind-of happening —that Internet of Some Things.

“Consumers don’t care what the standards are just so things work together and easily,” points out Justice, who adds that the aim of providers is to “deliver the best experience to end users.” He is testing that formula in a recent retail relationship with Amazon.com, where his firm sells ConnectSense, a platform of DIY cloud-based Wi-Fi 802.11b/g wireless sensors that monitors changes in a user’s environment and then sends notifications via phone call, email, text or Tweet. Various sensors monitor temperature, humidity, water, motion, security and lights.

An interesting Amazon twist, while the online retailer sells diverse IoT devices ranging from security and life safety to smart home and wellness wearables, the rationale for Amazon to get into smart home wouldn’t have anything to do with trying to create a line of smart home hardware —that’s small potatoes, contends Michael Wolf of NextMarket and NextMarket Insights. “Instead, I believe the company would basically look to create a ‘point of sale’ touch point in nearly every part of the house. Basically, wherever they could stuff a sensor and some intelligence that could connect to a person’s Amazon account.”

Still, a sure bet for the approaching IoT: There will be winners and losers.

- In that fantastic future, with everything IoT-enabled working in a standardized, open environment, there will be less need for custom design and installation for many projects except for the biggest, most complex or projects serving clients who need personal handholding.
- Future off-the-shelf purchasing may mean more buying off a retailer’s shelf or through the Web and not from a traditional distributor’s warehouse or a dealer’s menu of choices. DIY —through Best Buy, Lowe’s, Staples, Amazon and myriad brick/mortar and online stores —will gain considerably as the realized IoT dampens consumer frustrations and fears. “DIY is increasingly a growing market. Convergence permits the same platform for multiple applications,” says Logvinov.
- Products, which often differentiate themselves as to their proprietary setting beyond features and aesthetics, will now be on a more level playing field where pricing will be a much higher priority.
- As more things hop effortlessly onto the Internet and smartphones and tablets evolve into interactive Internet-based application displays and controllers, all without much end user fuss, professionally monitored alarms and security video may to some degree give way to self-monitoring consumers who can call police and emergency medical help directly —the ultimate in verified alarm.
- Product and system maintenance —that extra revenue under contract or purchased warrantees —will reconfigure with fees tumbling or disappearing with the advent of remote, automated diagnostics, repair and updating bundled in. The maintenance of things, devices and appliances, no matter their complexity, will look more like one giant monthly Microsoft Update.
- With everything truly IoT-enabled and pricing pressured downward, mass marketing becomes more attractive and more easily accessible, especially for the widest reaching security companies and broadband providers – with both able to bundle.

According to Blake Kozak, senior analyst for security and building technologies at research firm IHS Inc., “The words ‘smart home’ continue to be kicked around, but what does it truly mean for home security? The answer: Change. For years, consumers have depended on the services of traditional monitoring stations and alarm companies. Equipment was simple and easy to use and did what it needed to do. Then in 2007, came the first iPhone from Apple, one of the first cell phones to deploy a multi-touch interface and in 2008 the release of Android, an open-source platform. Two releases that have changed the way in which consumers interact, not only with each other but other devices.”

He adds, “Fast forward to 2014, the alarm industry is now in a period of change. On the back of smartphone deployments, alarm companies are now offering consumers the ability to interact with the equipment in their
home. With new technology, comes new entrants and security companies now face stiff competition from other suppliers wanting to make a play in the home. With so much change and choice, where does the consumer turn?”

Kozak identified three models that consumers can chose from when rolling out a “smart” security system.

The first security deployment type is what he calls point security, defined as hardware that does not link to other devices in order to generate automation, with each device having its own application. “For example, many of the Z-Wave and Wi-Fi garage door modules used today are often independent of a total solution. Additionally, all-in-one devices such as Piper (owned by iControl Networks) are defined as point security products even though there are capabilities to integrate more pieces of hardware.”

The second type is connected security, which is a traditional burglar alarm system. All devices are connected to a panel, either hardwired or wireless with limited automation in place.

Lastly, smart security is defined as devices that are linked together through one central point and one application can manage all devices.

Says Kozak, to date, globally, connected security has gained the largest traction on the back of traditional monitoring companies. However, more recently, the market has seen a shift and a movement towards smart security and point security (mostly across North America) as more DIY vendors appear in the market and end users demand a seamlessly integrated home.

As this trend to “smart” takes place, the IHS analyst expects point security to benefit and grow because many of these products are used individually prior to being deployed in a single integrated solution. As a result, Kozak anticipates that point security could be a gateway to more “smart” systems.

Overall, these three deployment types are important because they could help shape the future structure of the industry. For example, point security could be a gateway to bigger solutions and more integration within the home as end users become accustomed to these devices.

Alternatively, connected security has the longest track record, yet has failed to increase in overall penetration rate. As a result, the combination of point security, which often involves startups and little to no brand recognition, with connected security, which often involves long-standing and proven brands, will likely lead to a new market of smart security.

*Bill is the Editor Emeritus of Security Magazine, and he can be reached at (773) 929-6859.*