Expert Guide

FOR INTEGRATORS AND SOLUTION PROVIDERS

Staying on Top of Emerging IT Security Trends

Inside

The security threat landscape is constantly evolving. New technologies open up new targets. Emerging standards may help.

This Expert Guide walks IT solution providers through the latest threat vectors facing SMB customers, the complexity of cloud security, and concerns around 5G. It also includes a look at NIST guidelines for the Internet of Things.

POWERED BY
ChannelPro
WWW.CHANNELPRONETWORK.COM

IoT playbook
WWW.IOTPLAYBOOK.COM

BE AFRAID:

AN EXPERT TOUR OF THE SECURITY THREAT LANDSCAPE

Channel pros need to address the latest threat vectors facing customers, including cloud, IoT, mobile devices, and—gasp—MSPs themselves. By Colleen Frye

FACT: BUSINESSES ARE EXCITED about taking advantage of cloud, the Internet of Things (IoT), and mobility to drive innovation and agility.

Fact: IT departments don't know how to secure those technologies fully.

Fact: Cybercriminals know IT is overwhelmed and are pouncing.

Security veteran Jayson Ferron, CISO at Interactive Security Training, says MSPs must spell out a harsh choice for customers: "You have to decide whether or not you want to be the target, or you want them to move past you."

The rise of new devices and endpoints on networks has only added to IT's already challenging job, leading to poor security hygiene, says Ian Thornton-Trump, head of security at AmTrust Financial. Organizations are "not following their standard procedures for putting something on the network. It's all kind of done quickly, and sometimes without even the involvement of IT."

The Big (Ugly) Picture

To address new threat vectors, it's important to put mitigation strategies in place. Our security experts walk through a few scenarios:

Threat Vector: Cloud

Organizations are rushing to get cloud applications up and running without necessarily thinking about security, Ferron says. As a result, they're not taking advantage of the security controls the cloud providers have in place. "It's not the cloud provider's issue; it's the people setting up the servers who are not doing all the steps," Ferron stresses. "The exact same thing that we've been doing on-prem we should be doing in the cloud." And don't forget to test it, he adds.

For his part, Thornton-Trump says the No. 1 mitigation strategy is to understand what security controls are available. Second, he says, "is really come up with a security control approach that's based on risk."

JAYSON FERRON

If organizations don't have the skill set for cloud security, Thornton-Trump advises bringing in an expert partner or getting a third-party review. "I think that would catch a lot of these problems. But, again, it's whether or not the business is prepared to make that investment."

Threat Vector: Internet of Things

The Internet of Things creates a Catch-22 for security, Ferron says. "Consumers are buying devices and they're not asking the question about security. And the people selling the devices … are not offering additional security. Until the consumer requests it, the manufacturers aren't going to."

Thornton-Trump adds that IoT vendors are "awful at responding to security researchers, who have found vulnerabilities in their products."

Another Catch-22 is that IoT is designed for doing things at scale, "but, when it has a vulnerability, it now is in an ugly situation where its original purpose can be suborned by the bad guys to do something else," Thornton-Trump says.

Credential stuffing is a common attack strategy now, he says, where cybercriminals cycle through passwords that were compromised in a public data breach, or simply pick the top thousand or so worst passwords. "Now you've basically managed to get into a number of accounts for a number of people."

To mitigate risks, Ferron advises organizations to lean on policy and procedures when putting these devices on the network, asking questions like: What does it do? How does it talk? What does it communicate with? What's its security rules? Is there a way to change the default usernames? "Why aren't we doing this for the IoT devices?"

He adds that MSPs need to talk about risk awareness with customers. "Risk awareness really says a couple of things. What is this doing for our organization? How is it going to do [it]? How is it going to help us? What risk does it bring to our organization?"

Threat Vector: Mobility

BYOD is pretty much the modus operandi for businesses now, but that mobility creates another attack vector. For example, mobile phones are subject to phishing attacks via SMS messages, and apps downloaded from storefronts may only have a cursory check for security, Ferron says. "So [marketplaces] could be putting stuff up in the store that they don't even know if [they are] compromising phones and devices."

One simple mitigation step would be to use digital signatures in-house, he says. "If you don't see a digitally signed [signature] from your counterpart or your employee, don't

open it up—and send it to the help desk. That's not a hard thing to do, but it would reduce a percentage of those spear phishing attacks considerably."

It's also a new service opportunity for channel pros, Thornton-Trump says. "It's always good money for the channel when you can build services around something that doesn't cost you a lot to do, but has an impact and reduces the likelihood that you have to do an incident response."

Threat Vector: You!

An emerging threat vector that has been grabbing attention is MSPs. Cybercriminals are using vulnerabilities in the MSP's infrastructure as conduits to attack their clients. For example, Thornton-Trump points to the hacking group APT10 and its Operation Cloud Hopper campaign, which was a global series of sustained attacks against MSPs and their clients starting around 2015. And in another incident in February of this year, cybercriminals successfully encrypted all 2,000 computers managed by at least one MSP impacted by an attack that exploited an outdated version of the ConnectWise ManagedIT Sync plugin for Kaseya's VSA remote monitoring and management system.

"Basically when you get that kind of success when you have done a really great job of compromising MSPs, entrepreneurial cybercriminals are going to look at that and go, 'Hey, here's an attack surface that looks great, that apparently folks can infiltrate fairly easily, and, oh, by the way, when something bad happens to their customers, we can escape any sort of scrutiny at all,'" Thornton-Trump explains.

Ferron notes that MSPs aren't always following basic security rules themselves. "If you're an MSP, you should be the picture of everything that should be done right," he stresses. MSPs, he adds, "have got to think of their infrastructure as a security operations center."

Thornton-Trump says that MSPs who are not following the same practices they recommend for customers are putting their customers—and their business model—at risk. MSPs need to go beyond anti-virus and vulnerability management and "really address foundational, architectural security all the way up to cloud and web applications security, and pretty much everything in between," he says.

If an MSP doesn't have the skill or resources to do so, Thornton-Trump suggests partnering with a managed security services provider or another MSP to fill in the gaps.

Conversations Needed

For MSPs, Thornton-Trump says, security really comes down to understanding what they have to protect. It's "a relationship between you and that customer, and it needs to be something that is defined in your contract for services."

Security also needs to be a continual conversation, both internally at the MSP and externally with customers, according to Ferron. "We have to, you and I, as a partnership, look at what the outside world wants to get from you, and how we can protect it, and how we can secure you. … It's an ongoing discussion."

It's not all scary, bad news, though. "You're not alone in this," Thornton-Trump says. "There are a lot of resources in the channel."

PHOTO: BOWIE15 iSTOCK

READER ROI

CLOUD, IOT, AND MOBILE DEVICES are some of the latest threat vectors MSPs and their customers face.

THE FOUNDATION for many mitigation strategies is good security hygiene and following traditional policies and procedures.

MANAGED SERVICE PROVIDERS, an emerging threat vector, must lock down their own infrastructure and follow the same practices they recommend for customers.

5G Raises Security Concerns

5G, LONG ANTICIPATED and now soon to hit the mainstream, may be a double-edged sword. While the extra speed and bandwidth are welcome, extra security worries will force integrators and IT solution providers to add extra protection.

"IoT devices and 5G are a nightmare for security," says Joe Molick, founder of Molick Enterprises, a small managed services provider in the San Diego area.

One issue is that 5G "requires a lot more base stations, which increases your attack surfaces, and there will be lots more devices added, like Internet of Things nodes," says Todd Kelly, chief security officer for Cradlepoint, a global provider of cloud-delivered LTE and 5G-ready wireless edge solutions.

Carriers are addressing such issues by building in more network protection, he continues, but channel pros need to proactively protect SMB customers implementing 5G anyway. Applications have scattered from the data center to a variety of clouds, so every connection is a new security issue.

Kelly says Cradlepoint is a big fan of Zero Trust Network Access (ZTNA), a technique for allowing application access without network access. "We always tell customers to treat the network as untested because you don't know what you'll connect over," he says.

Channel pros with public sector clients that fall under the "second responder" banner (organizations that support first responders such as utilities, hazardous waste cleanup firms, and first aid services) may be able to take advantage of first responder networks like FirstNet from AT&T and Verizon's private core network for public safety, Kelly adds. They come with end-to-end security and better user authentication.

He also suggests getting a jump on 5G security by adding new 4G network equipment today. "[Band] 14 LTE addresses some 5G security features such as protection against 'bidding down' attacks," says Kelly. In such an attack, a device between the endpoint and the tower tricks the device into downgrading security. "5G will push internet access closer to the edge with mobile edge computing, so pushing security from the data center to the edge will be important," he says.

For IoT devices, Kelly prefers to go beyond network segmentation. "Add a separate IoT network that doesn't touch the corporate network," he suggests, such as a private network over a carrier network. 5G's ability to handle more end devices than 4G will help.

Be aware, too, that hackers can—and probably will—use inexpensive tools to attack 5G equipment. For instance, the hardware needed to run a bidding down attack costs less than a thousand dollars.

Finally, make sure IoT devices going on 5G networks have security right out of the box, adds Molick. "Don't connect the device until it initiates security." Good advice for both 5G and current networks.—*James E. Gaskin*

CLIMBING PAST CLOUD SECURITY COMPLEXITY

Security is hard. Cloud security is even harder, but with the right strategy and methods it's possible to design more secure systems. By Samuel Greengard

"YOU HAVE TO START FROM A ZERO-TRUST FRAMEWORK AND FOCUS ON THE PRINCIPLE OF LEAST PRIVILEGE."

STEVE RILEY
Senior Director of Research, Gartner

THE COMPLEXITY of cloud security serves as both a challenge and an opportunity for channel pros.

On one hand, the cloud introduces new and sometimes unfamiliar security requirements. Not only does it multiply connection points and overall exposure, it introduces more vendors and additional layers of complexity. Moreover, it's no longer possible to rely solely on web application firewalls, data loss prevention, secure web gateways, and basic authentication tools. On the other hand, channel pros who guide clients through the maze and help them arrive at more secure IT frameworks can boost trust and, ultimately, achieve deeper relationships based on value.

While securing IT systems and locking down data has never been simple, it's grown exponentially more complex in the era of cloud computing and widely dispersed systems. Today, data and information flow across devices, offices, and companies. "It's a borderless world of data," observes John Yeoh, global vice president of research at the Cloud Security Alliance (CSA).

It's safe to say that the old rules of security don't apply in the cloud. MPLS networks with fixed providers have fallen by the wayside. Many on-premises tools and applications don't work well in the cloud, where servers and containers are typically software-based. Names and IP addresses constantly change, and businesses frequently don't have full control over containers, applications, and more.

"You're often subscribing to someone else's application, and there's often a greater degree of abstraction because you don't own the network or the virtual machines," says Steve Riley, senior director of research at IT consulting firm Gartner. Given that lack of control, "it's necessary to move away from the idea of a secure network of systems and enable a network of secure systems. This means hardening the host or container because that's what a subscriber has control over," Riley says.

In the cloud age, therefore, managed service and IT solution providers need to rethink the way they design cybersecurity solutions. "Cloud security requires a different mindset and a different framework—and it is evolving rapidly," says Joe Vadakkan, global head of cloud security at cybersecurity integration firm Optiv. "It increasingly requires highly automated and scalable solutions."

PHOTO: BLACKRED ISTOCK

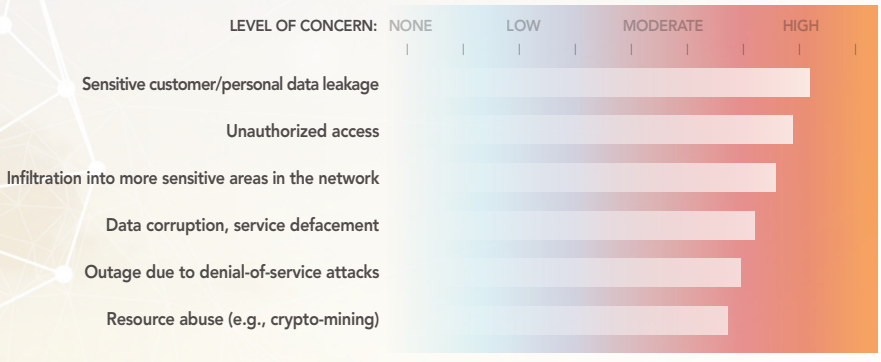
Out of the Haze

The challenges surrounding cloud security are significant. A 2019 study of 700 IT and security professionals conducted by CSA and AlgoSec found that common problems revolve around misconfigurations, visibility into the entire cloud estate, inadequate audit preparation and compliance, holistic management of cloud and on-premises environments, and managing multiple clouds. What's more, human error factored into many problems. In all, 11.4% of respondents reported a cloud security incident in the past year, and 42.5% had a network or application outage. Eighty-one percent of cloud users said they encountered significant security concerns.

At a most fundamental level, cloud security incorporates any and all data that touches private, public, and hybrid clouds. The risks and protections are similar to conventional IT systems, but the topography and structure of cloud networks create far more intrusion points and data exposure hazards. APIs make it easier to bypass conventional perimeter-based security protections, and in many cases provide a backdoor into systems that can lead to a takedown. Clouds are also highly dynamic, and threats to the infrastructure are constantly changing.

And while cloud providers—including the likes of AWS, Microsoft, Google, Rackspace, and Oracle—have strong security controls in their data centers and offer security tools in

SECURITY CONCERNS WITH REGARDS TO APPLICATIONS RUNNING IN THE PUBLIC CLOUD



SOURCE: *CLOUD SECURITY COMPLEXITY: CHALLENGES IN MANAGING SECURITY IN NATIVE, HYBRID AND MULTI-CLOUD ENVIRONMENTS*, CLOUD SECURITY ALLIANCE AND ALGOSEC, 2019

applications, default configuration settings can create problems. "Default configurations aren't necessarily safe, and the cloud provider may not notify you that this is the case," Yeoh explains.

Problems often revolve around authentication methods, permissions, whether data is encrypted at rest and in motion, and which cloud services and components are open by default. Not surprisingly, cloud providers often lean toward convenience and ease of use. Often, channel pros and others engineering and designing IT frameworks don't bother to examine how systems are configured and how they interact with each other within the realm of security. "If you're not careful," Yeoh says, "you inadvertently wind up with systems that can expose a lot of sensitive information. If someone has access to cloud components, folders, or files, they can do a tremendous amount of damage."

For MSPs, it's unwise to view cybersecurity as the primary responsibility of cloud service providers. There are simply too many moving parts and bits of data to think that checking settings and connections is sufficient.

"Unless it's specifically called out in a contract, a cloud provider's focal point is availability and uptime … not security," says Kevin Beaver, principal information security consultant at Principal Logic. The problem extends to SOC 2 audits, he continues. These reports "often paint a rosy picture in terms of security … but actual vulnerability and penetration testing that highlights technical flaws is also needed."

A sense of complacency can be fatal, Gartner's Riley adds. "Over the last decade we've gone from, 'I'll never trust cloud computing to be secure' to 'It has to be more secure because AWS, Microsoft, and Google are offering these services.'" However, cloud security failures are more common than ever, he points out. What's more, "They're almost always the fault of the customer for not appreciating that they have the primary responsibility and taking time to ensure that everything is configured properly."

Too often, designers and end users overlook basic settings, such as open file shares, Riley adds. "Although they are supposed to be locked down by default, they are not. A lack of controls allows someone to go in—perhaps a developer—to simplify things. Unfortunately, in the process, they inadvertently share everything with the world."

The upshot? "The cloud is a more secure starting point than your own data center, because instead of the whole stack, you only have to secure certain slices of the stack," Riley explains. "But the attention you have to pay to those slices is much greater than before. You have to start from a zero-trust framework and focus on the principle of least privilege."

A Clearer View

A starting point for improving cloud security is to build a more expansive and nuanced framework that hinges on three key areas: managing security across a diverse array of devices and SaaS services in different locations, including at the edge; establishing security beyond a single data center or location and replicating the security everywhere; and maintaining a complete view of settings and protections across cloud providers and clouds.

A security plan must be flexible enough to scale as an organization adds systems and software, while recognizing that some data is more valuable than other data. This points to the need for a more comprehensive security-by-design framework, centralized visibility and controls, continuous compliance monitoring and reporting, the ability to monitor and track the threat landscape, and a plan for dealing with a breach or other security incident when it occurs.

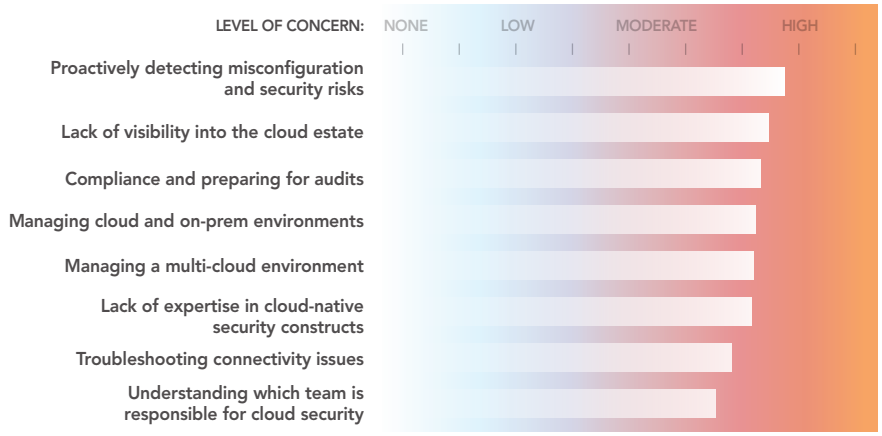
More security, Optiv's Vadakkan says, isn't necessarily *better* security. "You have to think about security less as a stopgap measure and more as a framework that has to be woven into private, public, and hybrid clouds. There's a need for smarter systems and greater automation."

Understanding the value of data and conducting a thorough cost-benefit analysis shines a light on the process. "The key is to bring all the various components and pieces under the umbrella of an information security program," Beaver explains. All of this, in turn, helps cloud security designers better understand the nuances of web applications, data flow, network designs, cloud infrastructure, and improved data governance. "Beyond that, just as with traditional networks, it's all about visibility and control," he adds.

Eye on Tools

While cloud providers offer a growing array of security tools—often at no additional charge—control frameworks such as the Cloud Controls Matrix offered by CSA and activity monitors that fall into the cloud access security broker (CASB) category are essential. These solutions, among other things, introduce trust ratings, trust levels, digital

LEVEL OF CONCERN POSED BY ITEMS WHEN MANAGING SECURITY IN THE PUBLIC CLOUD



SOURCE: *CLOUD SECURITY COMPLEXITY: CHALLENGES IN MANAGING SECURITY IN NATIVE, HYBRID AND MULTI-CLOUD ENVIRONMENTS*, CLOUD SECURITY ALLIANCE AND ALGOSEC, 2019

watermarks, behavioral analysis, permissions and automated API detection, and encryption support. Many CASBs also monitor SaaS applications as well as other applications running in Java Virtual Machines.

Data encryption at rest and in motion are critical too, Riley says. This includes hardware-based encryption that a cloud provider offers. "There's a misconception that encryption slows performance. This simply isn't the case," Riley says. And while some businesses may balk at spending more time and money to encrypt everything, the dollars saved can easily backfire. "If you selectively encrypt data, you're basically saying that you can get 100% of your classifications right, and if something goes wrong, you can stand in front of an auditor or regulator and explain the problem away."

Multifactor authentication (MFA) can also be used to protect accounts, containers, folders, and more. Vadakkan notes that only about 7% of companies with clouds use the technology consistently, and that the resulting lack of protection frequently leads to gaping holes in security. What's more, if an attacker steals someone's credentials, no amount of protection—including encryption—will impede this individual. By incorporating the principle of least privilege into applications and systems, controlling permissions carefully, and using physical and virtual tokens to authenticate through MFA, Riley says, an enterprise can dramatically reduce unauthorized access to data along with its overall risk profile.

Yet, even with the most robust cloud security in place, you must plan for the worst. If a distributed denial-of-service attack occurs or ransomware seizes systems and data, your customers can sidestep much of the pain if there is a backup and data recovery solution in place. Having failover capabilities mapped out before a breach or breakdown occurs is critical too. This, among other things, requires your customers to reassess current availability resources as well as the service infrastructure used for e-commerce, internal business operations, and other important tasks—areas in which you can guide them.

Beyond the Clouds

Cloud security is continuing to evolve, Vadakkan says, so it's wise to keep an eye on emerging auto-remediation tools, which automate cybersecurity tasks such as scanning for vulnerabilities and fixing flawed configuration settings. In most cases, these applications can be integrated with other security applications and tools offered by the cloud service or a third-party security provider.

Cloud security posture management (CSPM) is another tool that's gaining traction. Riley advises organizations to resist "duplicating their on-premises stacks and instead look for ways to be as cloud-native as possible." However, he adds, "It's impossible using only native controls to have consistent security policies across multiple clouds." CSPM offers key advantages: It abstracts the security pane from cloud deployments, which makes it easier to manage policies and systems; and it frees developers from waiting for others to provision servers and test security settings. "CSPMs provide valuable guardrails for operating within security policies," he says.

In the end, it's crucial for channel pros to recognize that every advance in technology introduces new and sometimes more sophisticated ways for attackers to infiltrate systems and damage or steal data. As the volume of data swells, APIs proliferate, and connection points grow in numbers and complexity, MSPs must remain vigilant and adopt cloud security protections that foster agility and flexibility while reducing risk for their customers.

"The cloud represents a huge disruptive shift in terms of both architecture and security," Yeoh says. "It redraws boundaries. There's a perception that the cloud complicates security, but if security is done right, it can actually improve protection and simplify things."

> "YOU HAVE TO THINK ABOUT SECURITY LESS AS A STOPGAP MEASURE AND **MORE AS A FRAMEWORK** THAT HAS TO BE WOVEN INTO PRIVATE, PUBLIC, AND HYBRID CLOUDS."
>
> JOE VADAKKAN
> **Global Head of Cloud Security, Optiv**

READER ROI

- **THE CLOUD** makes security exponentially more complex, and the old rules and standard tools for securing the network don't apply.
- **CLOUD PROVIDERS** offer strong native security and tools, but integration with legacy IT systems and lack of control over cloud applications introduce greater risks.
- **MSPS NEED TO RETHINK SECURITY** as a framework woven into private, public, and hybrid clouds, and utilize newer cloud tools, implement MFA technology, and have a BDR plan.
- **SOME NEWER CLOUD TOOLS** include cloud access security brokers and cloud security posture management tools.
- **CLOUD SECURITY IS DYNAMIC,** so MSPs must remain vigilant and continue to adopt cloud security protections that foster agility and flexibility.

IoTPLAYBOOK

NIST for IoT

New NIST guidelines for Internet of Things environments are helping to drive acceptance of security recommendations. **By James E. Gaskin**

PHOTO: SHUTTER2U / ISTOCK

THE NIST SECURITY FRAMEWORK is rapidly becoming the gold standard for designing complete layered defense strategies. Now NIST guidelines are available specifically for IoT environments in the form of the recently published NISTIR 8228 document, titled "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks."

"NIST 8228 includes a strong set of recommendations for companies implementing IoT," says Jeff Wilbur, technical director of the Online Trust Alliance (OTA), part of the Internet Society.

NIST 8228 directly applies to integrators and technicians building and managing IoT networks. In the introduction, the document identifies three high-level considerations:

1. Many IoT devices interact with the physical world in ways conventional IT devices usually do not.
2. Many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can.
3. The availability, efficiency, and effectiveness of cybersecurity and privacy capabilities are often different for IoT devices than conventional IT devices.

In addition, NIST 8228 lists three major "risk mitigation goals." First, protect device security and stop devices from being used to launch attacks. Second, protect data security by keeping all data collected or processed by the device confidential. Finally, protect all personally identifiable information the device encounters. These goals are on page 11, and most of the remaining pages of the 44-page document go into detail on ways to achieve these three goals.

AUSTIN JUSTICE

According to Wilbur, NIST 8228 is chiefly targeted at federal users. "It outlines a spectrum of risks in IoT for implementers, and they can choose where on that spectrum they feel comfortable," he says.

Wilbur adds that a separate set of guidelines intended for the manufacturing industry, NIST 8259, has entered the comment stage, and references the 8228 implementation framework extensively.

Forging Ahead

Implementers like Austin Justice, vice president of Justice IT Consulting, an MSP in the Dallas/Fort Worth area, are already making use of 8228. "We started with NIST because we work with government contractors," says Justice. "Most of our customers are manufacturers, and many of them make parts for a major Department of Defense aviation manufacturer, Lockheed [Martin], on the west side of Fort Worth."

Justice finds NIST 8228's best practices helpful, especially compared with the legally binding requirements in HIPAA. "NIST was done by professionals rather than Congress," he explains. "About 90% of NIST is good cybersecurity guidelines in a framework people should be following."

Acceptance is building for NIST 8228 in the security community, which is generally happy with the guidelines. "Everyone had an opportunity to give input to NIST, so those with problems had a chance to speak up," Wilbur explains. "There's lots of momentum building around a common core of security principals for integrators and manufacturers. We hope to see major progress on the vendor side in the next year or so."

For Justice's part, NIST 8228 is a way to capitalize on a growing opportunity. "We didn't start out focusing on IoT," he says, "but our customers have security cameras, parts vending machines, [and] IoT monitoring on all their big equipment all the way down to time clocks."

JAMES E. GASKIN *is a* ChannelPro *contributing editor and former reseller in the Dallas area.*