Tech Outlook

PROSYS
A PIVOT COMPANY

December 2016

Waging War against Ransomware

Cisco Umbrella, combined with Cisco AMP for Endpoints, can help organizations prevent and contain ransomware attacks.

Ransomware attacks have reached epidemic proportions, and more evasive and destructive threats are on the horizon. In their 2016 Midyear Cybersecurity Report, Cisco's Talos researchers predict that new modular strains of ransomware will be able to self-replicate, spread faster and quickly switch tactics to maximize efficiency. Because traditional security tools are helpless against ransomware, organizations need a new set of weapons to wage war against these attacks.

Most IT professionals understand the basics of a ransomware attack. By clicking on a malicious link, ad, attachment or infected thumb drive, a user launches a malware infection that uses strong encryption to "lock" all the files it can access. Unless detected and stopped, a ransomware attack can spread quickly throughout an organization, encrypting the files on the victim's device and any network- or cloud-connected file shares.

In actuality, ransomware attacks occur in phases. The initial payload of the attack is not the ransomware itself but an exploit kit such as "Angler" or "Zeus." The exploit kit analyzes the environment to determine which ransomware variant will be most effective, then initiates a callback to its command-and-control host to receive the private keys needed to encrypt the data.

"Antivirus software, intrusion prevention systems and other tools that rely upon known attack signatures cannot detect these exploits. In fact, the rise of ransomware is driving a shift away from signature-based solutions," said Michael Hritz, Vendor Alliance Manager, ProSys.

continued on page 2

TECH OUTLOOK

PRSRT STD
U.S. POSTAGE
PAID
Tulsa, OK
Permit No. 2146

continued from page 1

"But by understanding the phases of a ransomware attack, it's possible to greatly reduce the odds that the attack will be successful. The Cisco Umbrella cloud security platform is capable of recognizing malicious domains and blocking those connections. If the exploit does reach the device, Cisco AMP for Endpoints employs continuous analysis, sandboxing and other advanced capabilities to help identify and strop the threat."

Blocking Connections

Cisco Umbrella uses the foundation of the Internet – the domain name system (DNS) – to protect against malware, botnets and phishing campaigns regardless of location or device. After all, hackers generally must rely upon the DNS to execute their attacks. When a user clicks on a malicious link in a phishing email, for example, the browser sends a DNS request to the website hosting the malware. In addition, the exploit kits used in ransomware attacks typically make DNS requests to their command-and-control systems.

> "The rise of ransomware is driving a shift away from signature-based solutions."

Leveraging technology Cisco acquired through its purchase of OpenDNS in 2015, Umbrella uses big data analytics and statistical models to examine more than 80 billion DNS requests each day. Umbrella "learns" to identify Internet activities that point to cyberattacks, making it possible to discover and even predict the domains and IP addresses used by exploit kits and many ransomware variants.

"Umbrella is capable of blocking malicious traffic that travels over any port, protocol or application, including direct-to-IP connections," Hritz said. "If a user clicks on a malicious link or is redirected from a compromised site, Umbrella prevents the browser from connecting to the malicious host and downloading the malware. And infected devices are prevented from phoning home to their command-and-control systems, so exploit kits are unable to launch their malicious tasks.

"Unlike HTTP proxies, which intercept all DNS requests, Umbrella selectively reroutes suspicious domains for further inspection to provide effective protection without impacting performance. And because it is highly effective at stopping command-and-control callbacks, it can stop the execution of a ransomware attack even if devices become infected."

Umbrella Investigate enables security researchers to query Umbrella's indexed and cross-referenced data using sophisticated analytics, real-time cyber intelligence scoring and threat classification. The data can also be integrated with SIEM and threat intelligence tools through a RESTful API.

Preventing Infections

Cisco AMP for Endpoints works in concert with Umbrella to protect against ransomware attacks at the device level. If a user downloads a malicious email attachment or inserts an infected thumb drive, AMP for Endpoints uses reputational and behavioral indicators as well as signatures to detect the exploit kit and prevent it from executing. It can also detect and block many ransomware variants.

"Because traditional signature-based solutions do not provide an effective defense against modern malware, organizations have begun layering additional products onto the endpoint to identify and respond to threats. However, this adds operational complexity," said Hritz. "Cisco AMP for Endpoints is an end-to-end solution that provides simpler, more effective endpoint security. It is capable of blocking known and emerging threats in real time through a combination of traditional antivirus scanning, big data analytics, machine learning and other advanced techniques."

Through continuous monitoring, AMP for Endpoints can also detect and rapidly respond to threats that are successful in evading its front-line defenses. It records all file activity to detect malicious behavior, and shares and correlates threat information in real time. Deep visibility and a detailed recorded history of malware behavior reduces detection times to minutes. Built-in sandboxing technology allows organizations to quarantine and analyze unknown files.

AMP for Endpoints also accelerates investigations through a simple cloud-based user interface that enables IT teams to search across all enterprise endpoints for indicators of compromise. Users can systemically respond to attacks across PCs, Macs, Linux and mobile devices, removing malware with just a few clicks.

Ransomware may be the biggest threat organizations face, but new tools are available to help organizations defend their systems. With the ability to disarm an attack at every phase, Cisco Umbrella and AMP for Endpoints are proving effective weapons in the war against ransomware.

News Briefs

Flash Sales Boost Storage Market

The falling price per gigabit of flash storage is giving organizations a bigger bang for their storage buck, according to the latest release of IDC's Worldwide Quarterly Enterprise Storage Systems Tracker. Although worldwide enterprise storage revenue remained flat during the second quarter of 2016, flash-based storage systems experienced solid demand.

Global enterprise storage revenue for Q2 2016 was almost identical to last year at $8.8 billion — a zero percent year-over-year growth rate, according to IDC — although total capacity shipments were up 12.9 percent to 34.7 exabytes during the quarter.

The total all-flash array market generated almost $1.1 billion in revenue during the quarter, up 94.5 percent year over year. The hybrid flash array segment continues to be a significant part of the overall market with $2.3 billion in revenue and 26.1 percent market share.

"Spending on all-flash deployments continues to grow and help drive the market," said Liz Conner, IDC storage research manager. "The decreasing cost of flash media, coupled with increasing use cases, high-density deployments and availability of flash-based storage products, have resulted in rapid adoption throughout the market."

AT&T Tries Broadband over Power Line

AT&T recently announced it is nearing field trials of a new initiative that involves delivering multi-gigabit broadband over power lines. AT&T says "Project AirGig" will be easier to deploy than traditional fiber, will use license-free spectrum and can deliver ultra-fast wireless connectivity to any home or handheld wireless device. The company says field trials will begin in 2017.

Broadband over power lines once was considered a promising concept for transmitting data over utility lines, but it fizzled after it was found to dramatically interfere with local radio waves. AT&T says its new concept will avoid that interference by utilizing unlicensed spectrum and by never making a direct connection to the power line.

Instead, AT&T would use low-cost plastic antennas and devices located along the power lines to transmit modulated radio signals. The company says it has more than 100 different patents governing the implementation of this technology, which could help deliver last-mile broadband access to urban, rural and underserved parts of the world. Because it does not require new fiber to the final destination, AT&T notes that there will be no need to build new towers or bury new cables.

"Project AirGig has tremendous potential to transform Internet access globally — well beyond our current broadband footprint and not just in the United States," said AT&T executive John Donovan.

Tech Outlook

Copyright © 2016 CMS Special Interest Publications. All rights reserved.

Editorial Correspondence:
10221 E. 61st Street
Tulsa, OK 74133
Phone (800) 726-7667
Fax (918) 270-7134

Change of Address: Send corrected address label to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission. Tech Outlook is published monthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

ProSys locations

Atlanta, GA
(Headquarters)
Phone: 678-268-1300
Toll-Free: 888-337-2626
chash@prosysis.com

Atlanta, GA
(Integration Center)
Phone: 678-268-9000
Toll Free: 888-337-2626
twheless@prosysis.com

Austin, TX
Phone: 512-658-5847
Toll Free: 888-337-2626
jwestmoreland@prosysis.com

Birmingham/Montgomery, AL
Phone: 205-314-5746
Toll-Free: 800-863-9778
birminghamsales@prosysis.com

The Carolinas
Toll-Free: 888-337-2626
chash@prosysis.com

Indianapolis, IN
Phone: 317-688-1283
Bill.sanders@prosysis.com

Knoxville, TN
Phone: 865-310-8843
Toll-Free: 800-863-9778
info@prosysis.com

Louisville, KY
Phone: 502-719-2101
Toll-Free: 800-863-9778
pmadden@prosysis.com

Mexico City
Phone: +52 (55) 3601 3755
pmadden@prosysis.com

Miami, FL
Phone: 305-256-8382
Toll-Free: 800-891-8123
lspivack@prosysis.com

Mid-Atlantic
Phone: 800-634-2588 ext 2
midatlantic@prosysis.com

Nashville, TN
Phone: 615-301-5200
Toll-Free: 800-863-9778
pmadden@prosysis.com

New England
Toll Free: 800-634-2588 ext 1
newengland@prosysis.com

Seattle, WA
Phone: 425-939-0342
sballantyne@prosysis.com

Tampa, FL
Phone: 813-440-2410
800-891-8123
lspivack@prosysis.com

Security Skills Gap

Studies reveal dearth of cybersecurity talent is creating measurable damage.

Security incidents are increasing in sophistication and frequency, yet industry studies find that an alarming shortage of cybersecurity talent is resulting in direct and measurable damage to companies worldwide. Worse yet, most organizations say they don't believe the skills gap can be closed in the near term.

A study from Intel Security and the Center for Strategic and International Studies (CSIS) finds that 82 percent of survey respondents admit to a shortage of cybersecurity skills, with 71 percent citing this shortage as responsible for damage to organizations by making them more desirable hacking targets.

"A shortage of people with cybersecurity skills results in direct damage to companies, including the loss of proprietary data and IP (intellectual property)," said James A. Lewis, senior vice president and director of the Strategic Technologies Program at CSIS. "This is a global problem; a majority of respondents in all countries surveyed could link their workforce shortage to damage to their organization."

Another study by ISACA and RSA Conference finds that 75 percent of security professionals lack confidence in their team's ability to handle anything more than the most basic security incidents. In addition, 59 percent say that fewer than half of their cybersecurity job candidates could be considered "qualified upon hire."

"The lack of confidence in current cybersecurity skill levels shows that conventional approaches to training are lacking," said Ron Hale, Chief Knowledge Officer of ISACA. "Hands-on, skills-based training is critical to closing the cybersecurity skills gap and effectively developing a strong cyber workforce."

In 2015, 209,000 cybersecurity jobs went unfilled in the U.S. alone, and there are no signs of this workforce shortage abating in the near-term. The Intel / CSIS report estimates an average of 15 percent of cybersecurity positions will go unfilled by 2020.

This shortage is building in an environment where 74 percent of the ISACA respondents say they expect a cyberattack this year and 30 percent say they experience phishing attacks every day. More than half also say they expect attack surfaces to expand and exacerbate risk with the increase in cloud, mobile computing and the Internet of Things, as well as advanced targeted cyberattacks and cyberterrorism across the globe.

The demand for cybersecurity professionals is outpacing the supply of qualified workers, with highly technical skills the most in need across all countries surveyed. In fact, skills such as intrusion detection, secure software development and attack mitigation were found to be far more valued than softer skills such as collaboration, leadership and effective communication.

The Intel / CSIS report identifies the following recommendations for addressing the cybersecurity talent shortage:

Increase Cybersecurity Spending: Unsurprisingly, countries and industry sectors that spend more on cybersecurity are better placed to deal with the workforce shortage. The banking industry has been particularly active in increasing cybersecurity spending, reflecting its prominence as a target. Finance consumes more cybersecurity products and services than any other private sector industry, and thus could help drive best practices for training and hiring cybersecurity talent.

Redefine Education and Training Requirements: About half the companies surveyed prefer a bachelor's degree in a relevant technical subject as a minimum requirement for hiring, but only 23 percent of respondents say education programs are preparing students to enter the industry. Nontraditional methods of practical learning, such as hands-on training, gaming and technology exercises, and hackathons, may be a more effective way to acquire and grow cybersecurity skills. More than half of respondents believe that the cybersecurity skills shortage is worse than talent deficits in other IT professions, placing an emphasis on continuous education and training opportunities.

Diversify the Workforce: Industry studies show that women and minorities are underrepresented in the cybersecurity field. Workforce enhancement efforts should aim to create a broader pool of cybersecurity talent. Another barrier to expanding the cybersecurity workforce is a stigma that lingers with job candidates who have a history of hacking. Employers should develop a more flexible attitude toward hiring people who have hacked.

Improve Incentives: While salary is unsurprisingly the top motivating factor in recruitment, other incentives are important in recruiting and retaining top talent, such as training, growth opportunities and reputation of the employer's IT department. Almost half of respondents cite lack of training or qualification sponsorship as common reasons for talent departure.

Encourage Government Action: More than three-quarters (76 percent) of respondents say their governments are not investing enough in building cybersecurity talent. This shortage has become a prominent political issue as heads of state in the U.S., U.K., Israel and Australia have called for increased support for the cybersecurity workforce in the last year.

"The security industry has talked at length about how to address the storm of hacks and breaches, but government and the private sector haven't brought enough urgency to solving the cybersecurity talent shortage," said Chris Young, senior vice president and general manager of Intel Security Group. "To address this workforce crisis, we need to foster new education models, accelerate the availability of training opportunities, and we need to deliver deeper automation so that talent is put to its best use on the front line."

The Agile, Open and Secure Data Center

Cisco Application Centric Infrastructure (ACI) helps you create an automated IT environment that is fast, flexible, and responsive to the needs of your business. It accomplishes this using a business-relevant software defined networking (SDN) policy model across networks, servers, storage, security and services.

ACI effectively turns the traditional IT model upside down. Network complexity is eliminated, so it no longer dictates application deployment or operation. Instead, application needs dictate IT deployment and operation.

Contact ProSys to learn more about ACI and software-defined networking.

PROSYS
A PIVOT COMPANY

www.prosysis.com
888-337-2626

© 2016 Cisco Systems, Inc. All rights reserved. CIS-125

Implementing the Internet of Things

Despite the enormous potential value, organizations are struggling to overcome IT and business challenges.

The story goes that the term "Internet of Things" began life as the title of a presentation in 1999. Kevin Ashton, who went on to become cofounder and director of the Auto-ID Center at the Massachusetts Institute of Technology, was talking to Proctor & Gamble executives about radio frequency identification (RFID). His larger message was much more interesting.

He noted that, up until that time, data was mostly generated by some human action — typing, scanning, pressing a button. RFID enabled "things" to become data generators, and if you could connect those things to the Internet, they could deliver their data anywhere. Broaden the concept to include sensors, industrial equipment and a host of other connected objects, and the Internet of Things (IoT) is born.

The possibilities are limitless. Vending machines that tell you which products need to be replenished. Trucks that communicate directly with fleet maintenance software. And of course consumer products that let you use your smartphone to lock your doors, control your thermostat and peek inside your refrigerator.

According to new data from Juniper Research, there were 13.4 billion IoT devices in 2015, and that number will reach 38.5 billion in 2020 — a rise of more than 285 percent. IoT "smart home" applications grab media headlines, but the industrial and public services sectors will form the majority of the device base. The IoT is transforming industries as diverse as retail and agriculture, and turning buildings, utilities and entire cities into highly automated systems.

Although the IoT is already vast, it's still in its infancy. Most enterprises are trying to figure out how to connect and secure their IoT devices. Once that hurdle is overcome, organizations face the problem of collecting, storing and analyzing all the data being generated.

"We're still at an early stage for IoT," said Steffen Sorrell, author of the Juniper Research study. "Knowing what information to gather, and how to integrate that into back-office systems, remains a huge challenge."

Mind-Boggling Complexity

The IoT has a profound impact on an organization's network infrastructure. Devices must not only connect to the Internet but share information with diverse applications and management platforms. Organizations must be able to integrate and manage a wide range of fixed, mobile, wired and wireless data sources with tremendous variances in media types, connection speeds and communication protocols.

According to data from Machina Research, 71 percent of IoT connections use short-range technology such as Wi-Fi, Zigbee and in-building power-line communication (PLC) networks. That's because consumer electronics and building security and automation systems currently dominate the IoT. However, cellular connections are growing rapidly, largely due to "connected car" applications. And by 2025, 11 percent of connections will use a low-power technology such as Sigfox or LoRa.

The security challenges of the IoT are only beginning to be understood. According to a study by HP Security Research, 70 percent of IoT devices have significant vulnerabilities — an average of 25 per device. PricewaterhouseCoopers found that 70 percent of connected devices lack even basic security capabilities.

The security and privacy of IoT data must be maintained while it's in flight across the network, at rest in storage or in use by an application. However, the vast number of devices and the enormous volume of data they generate makes security particularly difficult. Compounding the problem is the rush to implementation. Many organizations launched IoT initiatives without considering security implications from the beginning, and have been forced to reactively patch vulnerabilities.

On top of all that, the IoT is largely unexplored territory. Concerns about costs and return on investment; along with liability, privacy, security and other regulatory matters, are some of the major inhibitors to IoT adoption.

"The complexity of IoT projects is beyond what many companies can handle," said Seth Robinson, senior director of technology analysis for IT industry association CompTIA.

Turning Data into Information

Juniper Research defines the IoT as "the combination of devices and software systems, connected via the Internet, that produce, receive and analyze data. These systems must have the aim of transcending traditional siloed ecosystems of electronic information in order to improve quality of life, efficiency, create value and reduce cost."

The research notes that the IoT, therefore, is only as effective as the sum of its parts. Mere connections create data, but this does not become information until it is gathered, analyzed and understood. The analytics back-end systems of the IoT will therefore form the backbone of its long-term success.

Depending upon the use case, the timeframe for data collection and analysis could be months or milliseconds. For deep analysis of large data sets, traditional compute resources in the data center or cloud may be sufficient. But as demand inevitably increases for both depth and immediacy in analytics, compute resources will have to move to the network edge, closer to the devices themselves, to reduce latency and preserve bandwidth. Very few organizations have implemented edge computing technology.

Nevertheless, a recent Gartner survey suggests that the IoT is moving toward mainstream adoption for many industries. Only 29 percent of organizations are currently using the IoT, but an additional 14 percent are planning to implement it in the coming 12 months, with another 21 percent planning to implement it after that. It's important to note, however, that 28 percent have no plans to implement IoT and 9 percent see no relevance whatsoever in the technology.

"2016 will be a very big year for IoT adoption. We are starting to see a wide range of IoT use cases across virtually all industries," said Chet Geschickter, research director at Gartner. "But the big challenge now is demonstrating return on investment. Executives need to validate the contribution that IoT can make in order to justify large-scale rollouts."

Network Access Policies Must Be Updated for the IoT, Gartner Says

Hackers are already using Internet of Things (IoT) devices — many with weak or nonexistent security controls — to create botnets and infiltrate corporate networks. As the IoT continues to explode, Gartner says organizations must update their network access policies to effectively manage network traffic and address the very real threat of these attacks.

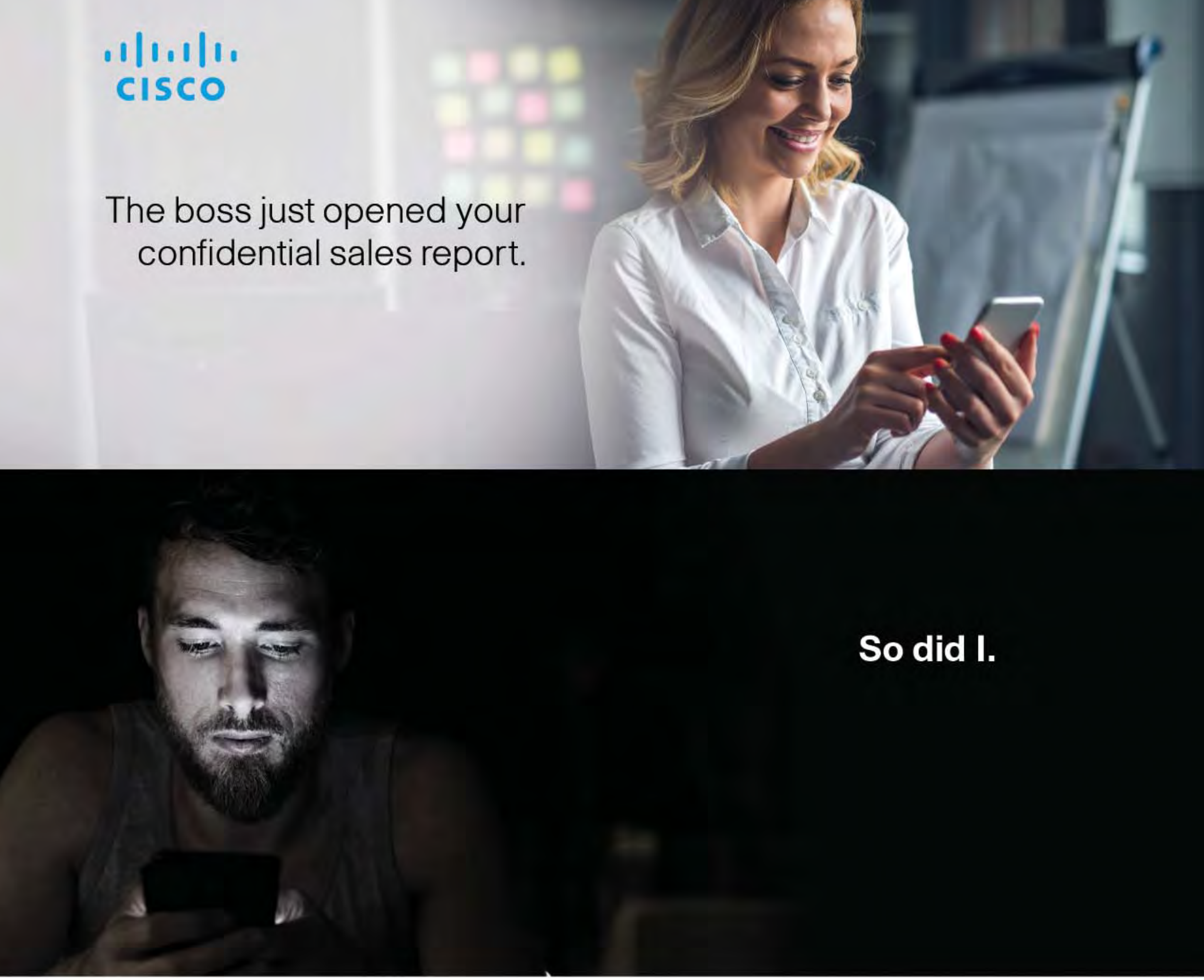
"Whether a video surveillance camera for a parking lot, a motion detector in a conference room or the HVAC for the entire building, the ability to identify, secure and isolate all IoT devices" is critical, said Tim Zimmerman, research vice president at Gartner. Zimmerman notes that so-called "headless" devices — the embedded systems that make up the majority of the IoT ecosystem — are particularly difficult to manage and secure.

"Many IoT devices will use the established bandwidth of the enterprise network provided by the IT organization. However, it is important that the IT organization work directly with facilities management and business units to identify all devices connected to the enterprise infrastructure and attaching to the network," he said.

Once all of the devices attached to the network are identified, the IT organization should determine if and how the devices will be connected, and what role they will be assigned to govern their access. The network access policy should then be created or modified accordingly.

In order to monitor and control the access of IoT devices, organizations may need to consider additional enterprise network best practices. For example, spectrum planning may be needed to prevent interference created by IoT devices that use the 2.4GH frequency band but don't connect via an 802.11 protocol such as Bluetooth, ZigBee or Z-Wave. Packet sniffers can be used to identify devices that may do something undesirable on the network.

Virtual network segments can be used to separate all IoT assets from other network traffic, allowing administrators to prioritize enterprise applications and latency-sensitive IoT systems. For example, video surveillance traffic could be given a higher priority than LED lighting.



Protecting sensitive information is a significant challenge for increasingly distributed and mobile businesses. With Cisco AMP for Endpoints, you can dramatically improve your ability to thwart even the most advanced threats to data security. This cloud-based, software-as-a-service endpoint security solution will not only prevent breaches and block malware at the point of entry, but it will also rapidly detect, contain, and remediate advanced threats if they evade front-line defenses and get inside the network. **Contact your ProSys representative to learn more.**

PROSYS
A PIVOT COMPANY

www.prosysis.com 888-337-2626

© 2016 Cisco. All rights reserved. CIS-130