September 2015

PROSYS
A PIVOT COMPANY

Delivering Success

The ProSys Integration Center streamlines IT deployments and provides key operational and financial advantages.

Organizations of all sizes face significant obstacles when it comes to technology deployments. In today's highly complex IT environment, many IT teams lack the specific expertise needed to successfully implement new technology solutions, and integrate those solutions with existing systems. With reduced IT headcounts, few IT managers have the luxury of dedicating resources to new initiatives. Meanwhile the pace of business change continues to accelerate, placing demands on IT to complete implementations on rapidly shrinking timelines.
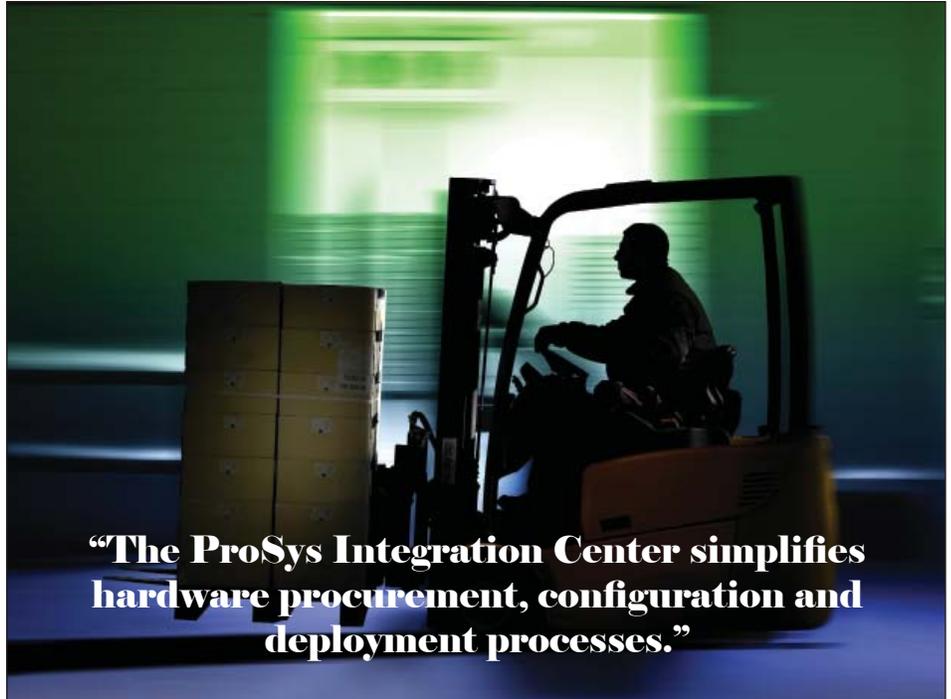
"The ProSys Integration Center simplifies hardware procurement, configuration and deployment processes."

"These challenges are hardly new, but they have become more pronounced in today's IT environment," said Shannon Slaughter, Vice President of Product Delivery. "Projects often become stalled because IT lacks the experience, resources and even physical space to configure, burn in, rack, stack and cable new equipment."

The ProSys Integration Center was developed to relieve these headaches. This state-of-the-art facility is staffed by certified engineers and technicians and logistics specialists who handle staging, configuration and testing, inventory management, shipping and related services. The ProSys Integration Center enables customers to avoid much of the disruption of an onsite deployment by delivering fully configured and integrated solutions to the data center for plug-and-play installation. It also facilitates large-scale roll-outs of desktops, mobile devices and other equipment, and the ongoing fulfillment of end-user equipment requests.

ProSys has now opened a new 138,000-square-foot Integration Cen-

Cover Story

ter that nearly doubles the capacity of its previous facility. Located in the Atlanta metro area, the ProSys Integration Center serves as a hub for configuration, deployment and logistics services for customers nationwide.

"We are very excited to expand the capacity of our Integration Center operations," Slaughter said. "We have successfully served the needs of some of the world's largest companies and are now able to deliver those services to a broader array of businesses."

End-to-End Solution

The ProSys Integration Center provides a comprehensive suite of capabilities that encompass every aspect of IT solution delivery, from equipment acquisition through onsite installation. These services helps organizations relieve operational bottlenecks and gain rapid time-to-value of technology investments.

"The ProSys Integration Center simplifies hardware procurement, configuration and deployment processes, saving both time and money while accelerating IT solution delivery," said Slaughter. "Each project is highly customized to meet the customer's specific requirements — the possibilities are virtually limitless."

In a typical project, equipment is procured and shipped directly to the Integration Center, where bar codes are applied for tracking. Once all the equipment has arrived, the components are assembled, asset tags are applied and serial numbers are recorded. ProSys engineers then complete the configuration and build processes, using testing facilities to run actual workloads in order to fine-tune the configuration prior to deployment.

"Each device can be preconfigured for the customer's environment, including site-specific settings. Software images

are applied using state-of-the-art tools. We can also apply special application settings, machine naming and password settings, update BIOS settings and revision levels, and perform OS and application updates," Slaughter said.

An increasingly popular option is customized "rack-and-stack" services. ProSys can deploy server, networking and other data center equipment in fully configured and tested racks to simplify onsite installation. Cabling is completed according to the customer's precise specifications, and color-coded labels applied to simplify identification. Sophisticated software is used to track serial numbers, MAC addresses, location information and other data.

"We can consolidate multi-item orders of equipment from multiple vendors onto a single purchase order," said Slaughter. "Precise configuration and implementation processes ensure consistency and streamline IT operations and support. Proven logistics and field deployment services reduce the cost and complexity of large, ongoing and time-sensitive projects."

Business Benefits

The need to procure, configure and integrate complex multivendor technology solutions creates an equally complex technology supply chain, with complicated quote processes and long product lead times. Inaccurate fulfillment and warehousing constraints can impact implementation schedules and increase the burden on resource-constrained IT teams.

"ProSys helps eliminate these chokepoints by validating multivendor configurations, ensuring consistent pricing, and quickly initiating order fulfillment," Slaughter said. "We can procure, inventory and warehouse equipment until ready for deployment, enabling customers to gain the price benefits of volume purchasing while adopting a 'just-in-time' IT delivery model. At the same time, we help organizations reduce

facilities and maintenance costs by eliminating the need to overprovision IT resources."

ProSys can help reduce product lead times by analyzing the customer's IT consumption patterns and keeping commonly used equipment in stock. This minimizes project-based ordering and facilitates large-scale roll-outs.

ProSys helps reduce maintenance costs by consolidating and co-terminating support agreements. ProSys Integration Center services also include processes for repurposing equipment and decommissioning assets that have reached the end of their useful life. This enables customers to reduce IT inventory and minimize the number of idle assets.

"ProSys Integration Center services have a positive impact on the top and bottom line," said Slaughter. "ProSys speeds the deployment of IT services while relieving in-house staff of the burden of traditional configuration, integration and implementation processes. As a result, ProSys enables organizations to grow and accelerate revenue, and see a more rapid return on the technology investment."

The accelerating pace of business demands an IT infrastructure that is agile and responsive. However, organizations seeking to rapidly scale IT solutions across the enterprise face daunting technical and logistical challenges. ProSys overcomes these challenges through full-lifecycle services that dramatically simplify and accelerate the delivery of customized technology solutions.

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

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

Lexington, KY
Phone: 859-887-1023
Toll-Free: 800-863-9778
dclemmons@prosysis.com

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

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

New York/Metro
Toll Free: 800-634-2588 ext 3
nymetro@prosysis.com

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

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

Ready to Wear
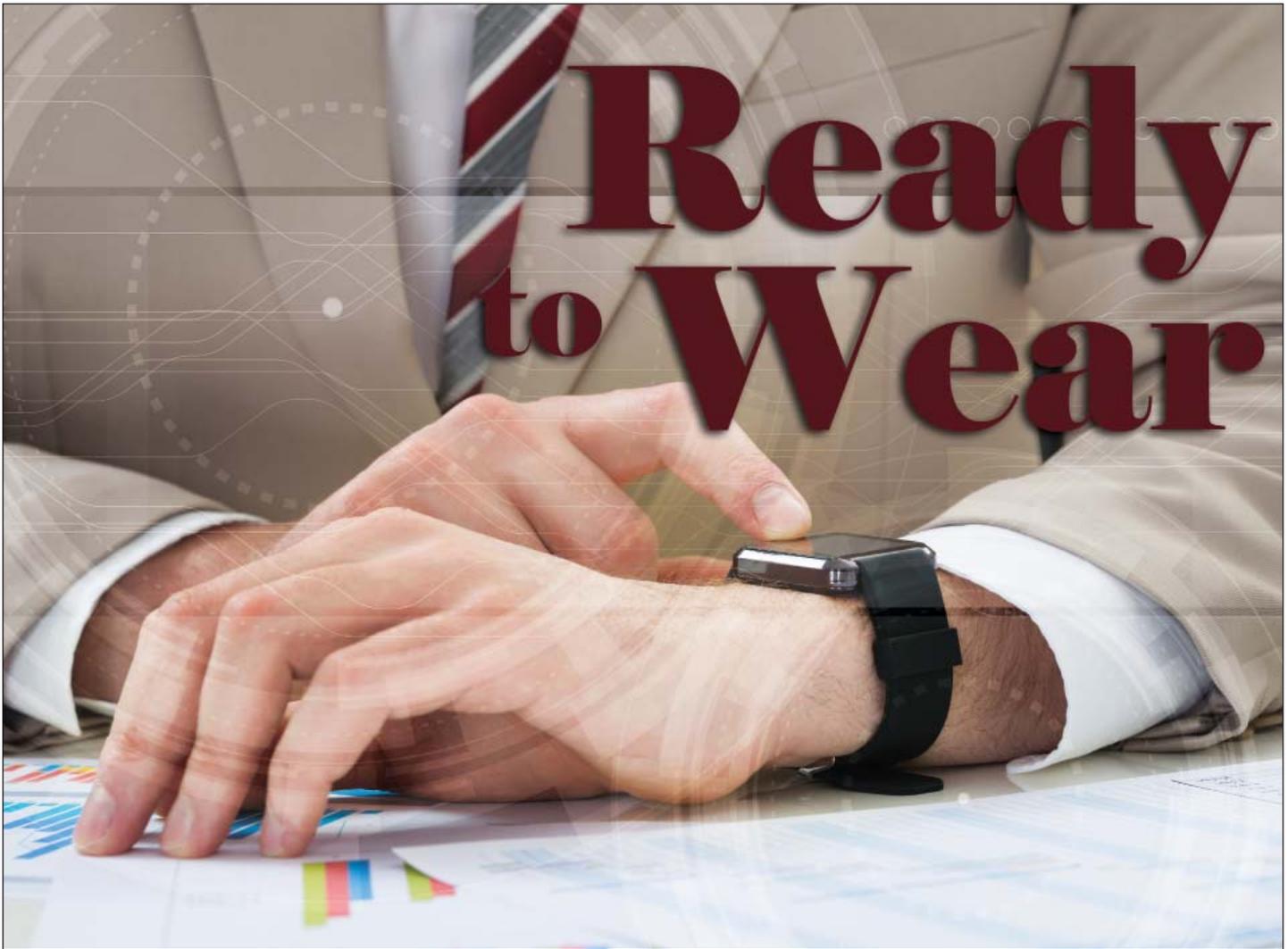
Wearable technology expected to gain rapid acceptance in the enterprise.

A Forrester Research survey of technology and business decision-makers has called 2015 "the year of the wearable," due in large part to the introduction of the Apple Watch. Although the most popular wearable technology has focused on fitness applications, including smart shirts and wristbands, new wearable solutions are making their way to the enterprise. In fact, nearly seven in 10 respondents to the Forrester study believe wearables are a priority for their organization, while slightly more than half view wearable technology as a moderate, high or critical priority.

Wearable technology refers to Internet-connected devices that can be worn on the body and exchange data with a network. Given the association between fitness and wearables, it's relatively easy to connect the dots between wearables and healthcare solutions that monitor heart rate, respiration rate, blood pressure and oxygen levels. However, wearable technology is capable of transforming virtually any business process.

The enthusiasm for wearables in the enterprise generally springs from the potential for increased productivity and collaboration. Analysts envision scenarios in which employees are able to work more efficiently by gaining hands-free access to critical data while operating manual tools or equipment. Video collaboration is another exciting possibility, allowing remote workers to be connected over distance to experts who can see exactly what conditions are being encountered in the field.

New research from Salesforce shows that 76 percent of early adopters of wearables in the enterprise report improvements in business performance, and 79 percent claim wearables are or will be strategic to their organiza-

tion's success. The use of wearable technology is expected to triple in the next two years, with implementations focused on improving the customer experience.

More than 60 percent of respondents to the Salesforce survey say they are using, piloting or planning to use smartwatches within two years to improve sales intelligence and create a more personalized customer experience. The use of data is a key growth area as only 8 percent of adopters claim to be ready to leverage employee and customer data produced by wearable technology. The expansion of the wearable application ecosystem for the enterprise and the development of more sophisticated devices are expected to drive adoption.

Salesforce cites a number of instances in which wearables deliver value to the enterprise:

Augmented sales intelligence. For a sales team that works remotely or on-the-go, sales reps can use natural language speech input to send information directly from a smartwatch to a CRM system.

Enhanced customer experience. Customer service reps wearing a smartwatch in retail settings can be alerted of key customer preferences, allowing them to deliver a high-touch, highly personalized experience.

Seamless onsite experience. In resort settings, RFID badges and lanyards can be deployed to transact payments and manage access to rooms or VIP areas. The devices also generate data, which can be analyzed for insights about better traffic flow within an event site or at particular times of day.

Minimize downtime for field service. Smart glasses can provide immediate support to remote field-service reps. For example, a repairman on an oil rig can connect to technical diagrams via smart glasses that show the steps required for a repair.

More and more enterprises are finding that unified communications (UC) applications are a natural fit for wearable technology. Just like fitness solutions are capable of sensing different types of exercise and automatically adjusting the workout mode, wearable UC can integrate all forms of communication into one portable, multifunctional solution. This capability only adds to the improvements in productivity, speed and customer service that traditional UC solutions provide.

"Wearables are the next phase of the mobile revolution. Like smartphones before them, the key to success for wearables in the enterprise is all about the killer business apps," said Lindsey Irvine, Global Director of Strategic Partnerships, Salesforce. "This research demonstrates the tremendous opportunity for wearable use cases to drive significant business value."

Changing of the Guard

Once-formidable SSL 3.0 encryption protocol is showing its age as security flaws are exposed.

I n 1996, Janet Jackson became the highest-paid musician of all time, Beanie Babies were "must-have" Christmas presents, AOL ruled the Internet and the Macarena was the most popular dance in the world.

Things change.

Version 3.0 of the Secure Sockets Layer (SSL) protocol became an indispensable element of network security when it was released back in '96 to protect data being sent across the Internet by providing encryption and authentication between servers and applications. Compared to other developments of the day, it has had spectacular longevity — it's still supported by as much as 98 percent of the world's most popular web sites, by some accounts.

It's had a good run, but just like the "Rachel" haircut and Hootie and the Blowfish, SSL 3.0 is past its prime.

Several recently uncovered flaws have essentially made the protocol too vulnerable to be of any practical value. The POODLE, FREAK and Logjam attacks all are designed to exploit SSL 3.0 vulnerabilities through "man-in-the-middle" attacks that will force security downgrades and make encrypted information easier to crack. The Google researchers who uncovered the POODLE attack say SSL 3.0 is "an obsolete and insecure protocol."

The 'Downgrade Dance'

SSL 3.0 actually was replaced with an improved protocol — Transport Layer Security (TLS) version 1.0 — back in 2011. TLS 1.0 was based upon SSL 3.0 and is considered only marginally more secure. Versions 1.1 and 1.2 of TLS are significantly more secure and fix many of the vulnerabilities in SSL 3.0 and TLS 1.0. In April 2014, the National

Institute of Standards and Technology (NIST) issued guidelines recommending that government agencies use TLS 1.1 and 1.2.

However, most TLS implementations include provisions for backward compatibility with SSL 3.0 to interoperate with legacy systems and ensure a smooth user experience. A protocol "handshake" process negotiates the latest protocol version common to both the client (browser) and the server (website), and then implements that version for authentication.

A team of Google researchers announced last fall that they had uncovered a significant flaw they termed POODLE, which stands for "Padding Oracle on Downgraded Legacy Encryption." In a POODLE attack, the attacker interferes with the protocol handshake process and forces browsers and websites to accept SSL 3.0. In a process Google calls the "protocol downgrade

dance," the attacker simply interrupts secure connections, forcing the browser to retry with the next-lower protocol. Once the downgrade process has moved through all versions of TLS to SSL 3.0, the attacker can exploit known vulnerabilities to decrypt secure HTTP cookies, which could let them steal information or take control of the victim's online accounts.

Freak Show

FREAK is another man-in-the-middle attack designed to force a downgrade in security measures. The flaw, which stands for "Factoring RSA Export Keys," was announced in March by a group of cryptographers who discovered a weakness in the SSL/TLS protocols that had actually been introduced on purpose decades earlier for compliance with U.S. security regulations.

This flaw allows an attacker to force secure connections to a lower lev-

el of encryption — 512 bit — which can be read and attacked with relative ease. It is an artifact of 1990s U.S. security policy requiring software being exported out of the country to be limited to "export-grade" encryption with key pairs of 512 bits or less. The idea was to make it easier for the U.S. to break the codes of any foreign adversaries.

"The 512-bit export grade encryption was a compromise between dumb and dumber," cryptographer Matthew Green of Johns Hopkins University wrote in a blog post explaining the vulnerability. "In theory it was designed to ensure that the NSA would have the ability to 'access' communications, while allegedly providing crypto that was still 'good enough' for commercial use."

The group that uncovered the flaw discovered that support for this weaker "export-grade" encryption was still baked in to numerous Web servers, browsers and other SSL implementations. The bug affects SSL/TLS servers and clients, and Microsoft, Google, Apple and Mozilla all have patches in the works.

Shutting It Down

In May, a second group of cryptographers announced they'd found another flaw based on cryptographic export restrictions. Unlike a FREAK attack, which tricks both ends of a conversation into accepting downgraded security, a Logjam attack exploits a vulnerability in the key exchange to make both believe they are running stronger keys than they actually are. The middleman in the attack can then eavesdrop or actually insert data into the communication path.

In response to this rash of flaws, Microsoft, Apple, Google and Mozilla have all issued patches for these vulnerabilities and are working to make their browsers more secure. Mozilla disabled SSL 3.0 in Firefox 34, as did Google with Chrome 40 and Microsoft with Internet Explorer 11. Apple has not gone that far yet, but it did block Safari's use of vulnerable cryptographic ciphers and has stopped using SSL 3.0 for its push notifications service.

In the long run, organizations likely will work to reconfigure web servers to address the SSL issue at its root. In the meantime, security experts say organizations and users should take a proactive approach to the vulnerability by updating to the latest version of their chosen web browser, or turn off support for SSL 3.0. A comprehensive guide for turning off SSL support in a variety of browsers is located at https://zmap.io/sslv3/browsers.html.

When it was introduced, SSL 3.0 represented a quantum leap in Internet security, and it was the de facto standard for cryptography for the better part of two decades. By providing an authentication process that ensured data confidentiality and integrity, it allowed millions of websites to protect online transactions with customers. However, POODLE and other exploits have now exposed critical flaws in the protocol, and there's no room for nostalgia in data security.

New PCI-DSS Standard Addresses SSL Flaw

To address vulnerabilities within the Secure Sockets Layer (SSL) encryption protocol that can put payment card data at risk, the PCI Security Standards Council published an updated version of the PCI Data Security Standard (DSS) on April 15. Version 3.1 went into effect immediately, with version 3.0 retired on June 30.

The move comes in response to word from Google researchers about a serious SSL flaw called POODLE (Padding Oracle on Downgraded Legacy Encryption) that enables hackers to obtain passwords and other confidential information that can be used to access a user's private account on a website. Upgrading to a current, secure version of TLS is the only known way to remediate the vulnerabilities that have been exploited by POODLE.

To address this risk, PCI DSS 3.1 removes all references to SSL and early versions of TLS from requirements 2.2.3, 2.3 and 4.1 of the standard. Although the revisions are effective immediately, impacted requirements have a sunset date to allow for organizations with affected systems to implement the changes:

• SSL and early TLS cannot be used as security controls to protect payment data after June 30, 2016. However, existing implementations that use SSL and/or early TLS must have a formal risk mitigation and migration plan in place prior to this date.

• Effective immediately, new implementations must not use SSL or early TLS. New implementations are those that have no existing dependency on the use of the vulnerable protocols.

• Point-of-sale (POS) devices that can be verified as not being susceptible to any known exploits of SSL and early TLS may continue using these protocols as a security control after June 30, 2016.

PCI 3.0 became mandatory on January 1, and brought sweeping changes to the rules organizations must follow in securing payment data. Chief among these is a new mindset that encourages a "continuous compliance" approach to data protection. Although PCI 3.0 was published in 2013, many organizations are still struggling to adapt to the new requirements. Version 3.1 adds a new layer of complexity.

Networks that work for you

A complete portfolio of transformational technologies that drive network simplicity.

Campus Networking
Wired and wireless solutions with unified management.

Data Center Networking
Network fabric that provides connectivity for virtualized compute, storage and cloud.

Software-Defined Networking
A complete solution with apps, infrastructure and technology to enable network automation.

Contact ProSys to learn more.

PROSYS
A PIVOT COMPANY

www.prosysis.com   888-337-2626