SIGMA
A PIVOT COMPANY

SigmaUptime

volume 16 number 4

UPTIME

Cisco-Apple alliance produces improved enterprise mobility, collaboration tools.

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

Technology services to help you streamline operations, reduce costs and improve business processes.

Companies today must align IT strategy with their corporate objectives, strategy and business model. Pivot has created a portfolio of operating companies and partners with a focus on helping you enhance and extend the capabilities of your technology assets.

Pivot provides technology services ranging from initial needs assessment and design, through procurement and implementation, to on-going support. As an adjunct to your IT team, we provide the resources that allow your team to offload some of the day-to-day operational challenges and focus on innovations that will drive business value and competitive advantage.

Contact us to learn more.

PIVOT
TECHNOLOGY SERVICES

www.pivotts.com 888-895-0495

Contents

5 **Working Together**

The Cisco-Apple alliance is producing business mobility and collaboration benefits with a series of solutions that make it easier to use iOS-based devices such as the iPad and iPhone across Cisco networks.

8 **Wi-Fi's Next Wave**

Wave 2 of the 802.11ac standard is bringing significant improvements to wireless networks. Industry analysts say Wave 2 products will enable organizations to support more devices as well as a new generation of high-performance, high-bandwidth applications.

10 **Prepare for GDPR**

The European Union's General Data Protection Regulation (GDPR) goes into effect in less than a year, and experts say it could be the strictest data privacy law ever enacted. Although it applies to many U.S. companies, studies suggest they are not doing enough to become compliant.

Sigma Uptime

Editorial Correspondence:

10221 East 61st Street, Tulsa, OK 74133

Phone (800) 726-7667 • Fax (918) 270-7134

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

Sigma UPTIME is published bimonthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.


GLOBAL MAP
Application Form

Working Together

Cisco-Apple alliance produces improved enterprise mobility and collaboration tools.

The Apple Macintosh, introduced in January 1984, is generally considered to be the first successful personal computer to feature a mouse and a graphical user interface (GUI). Despite that remarkable innovation, Apple technology did not make serious inroads into the world of business technology for the better part of three decades.

That has changed. With the iPhone and iPad, Apple has worked its way into enterprise computing consciousness. These devices and the iOS operating system they run have helped drive new levels of mobility, simplicity and security in business computing.

Cisco has capitalized on this momentum, teaming with Apple to create a fast lane for accelerating the business use of iOS devices on Cisco networks. Over the past two years, the two tech giants have collaborated on solutions designed to marry Apple's strength in devices and applications with Cisco's expertise in enterprise networking.

"This Cisco-Apple collaboration makes a lot of sense in terms of digital transformation," said Michael Hritz, Senior Business Development Manager, Sigma. "Everyone is looking for ways to use mobility, collaboration and innovation to really rethink traditional business processes. No mobile platform has done more to drive that transformation than iOS, and Cisco really understands how to push those benefits throughout an organization."

Business Solutions

Certainly, Microsoft remains the dominant force in the desktop space. By some accounts, roughly 91 percent of desktop computers run on

continued on page 6

continued from page 5

Windows. However, the iPhone and the iPad have helped create a more mobile workforce.

In a recent survey of IT professionals from 300 business organizations, Dimensional Research found that 99 percent have iPhone and iPad users in their workforce, and 91 percent have Mac users. Large percentages reported that iOS is as easy or easier to manage than other operating systems for the following tasks: deployment (93 percent), security (90 percent), device configuration (91 percent), software and app deployment (90 percent) and support (89 percent).

"It's clear that people want to use iPhones and iPads for work," said Hritz. "Cisco is helping to give organizations and their employees the resources they need to make the best use of the iOS ecosystem."

A key early success in the partnership was the development of a mechanism for optimizing Wi-Fi for iOS devices on Cisco infrastructure. With support for a variety of Wi-Fi standards, they made it easy to move seamlessly between access points (APs) within a Cisco wireless network. These standards include 802.11r for fast roaming, 802.11k for radio resource management, and 802.11v for wireless network management.

"This ensures that delay-sensitive applications such as voice and video aren't interrupted when you're on the move," said Hritz. "Your iOS device will identify the best available access point and select it by default. It's a seamless process that dramatically improves application reliability."

The Fast Lane

Prioritizing traffic has always been a bit complicated in Wi-Fi networks. Although numerous standards and software queueing mechanisms can be used to prioritize traffic throughout the network — across switches, routers and controllers — there's never been a good way to prioritize traffic between client devices and APs.

Cisco and Apple have tackled this issue with Fast Lane Quality of Service (QoS) marking. It allows administrators to create a profile for iOS devices running on Cisco networks. The profile defines all business-critical applications on the device and assigns each application a QoS mark, in much the same way an airline stamps tickets for first-class, business or economy.

"When Fast Lane is enabled, traffic from business-critical applications such as Cisco Spark or WebEx is whitelisted and given priority all the way from the iPhone or iPad throughout the network," said Hritz. "In addition, Fast Lane increases the number of QoS service classes from five to nine, which makes it possible to fine-tune prioritization levels."

The companies have announced upcoming simplicity and security enhancements for iOS devices on Cisco networks. When the latest version of iOS (11) is released in the fall, it will become even easier to use Apple devices for collaboration. With access to a new Cisco Spark software development kit for iOS, developers will be able to embed audio and video capabilities directly into apps for iPhone and iPad with just three lines of code. Additionally, iOS 11 updates will make it possible for users to join Spark and WebEx meetings directly from within calendar notifications, without switching apps.

Focus on Security

Security has always been one of the compelling features of Apple's iOS platform. It is a closed-ended system, which makes it less vulnerable to malware attacks, and Apple closely scrutinizes all apps available on its App Store to further reduce malware exposure. Apple device security within Cisco networks will be significantly enhanced this fall with the Cisco Security Connector.

Cisco Security Connector offers security functionality from Cisco Umbrella and Cisco Clarity in a single app. It can be deployed on enterprise-supervised iOS devices via a mobile device management (MDM) solution such as the Cisco Meraki Systems Manager. Cisco says the app will improve an organization's ability to meet risk and compliance requirements and will ultimately encourage further enterprise iOS adoption.

Specifically, Cisco Security Connector will safeguard corporate data and users by encrypting Internet (DNS) requests, and it will protect iOS device users from connecting to malicious websites, whether on the corporate network, public Wi-Fi or cellular networks.

In fact, Cisco and Apple executives argue that their integrated ecosystem is so secure that organizations using these products should be able to get a break on cybersecurity insurance. They recently announced their intent to work with insurance industry heavyweights on the development of a measurable reference architecture that would qualify for reduced premiums.

"The way people work has fundamentally changed, with people in most industries spending much more time out of the office and away from their desks," said Hritz. "The modern workforce is becoming reliant upon a diverse mix of devices and applications to collaborate with others and share information. The integration of Cisco and Apple technologies is facilitating that movement by creating a more secure and collaborative mobile experience."

World-Class Wireless with Cisco DNA

With Cisco Digital Network Architecture (DNA) at the core of your network, you give wireless users the performance and convenience they require while maintaining tough security and the flexibility to meet changing needs. Cisco DNA is an open, extensible and software-driven architecture designed for automation. DNA-ready access points and wireless controllers support the latest 802.11ac standard to deliver faster wireless speeds and an overall better experience. **Contact Sigma to learn more about bringing Wi-Fi into the digital age with Cisco DNA.**

SIGMA
A PIVOT COMPANY

www.sigmasol.com | 888.895.0495

Wi-Fi's Next Wave

Latest wireless networking standard delivers speed necessary to support more devices and applications.

Since its introduction in 2013, the 802.11ac Wi-Fi standard has had a dramatic impact on wireless networks, delivering marked improvements in speed, availability and reliability. It has rapidly become established in the enterprise, accounting for roughly 80 percent of access point shipments in 2016. Analysts with IDC expect 802.11ac to push the previous IEEE standard, 802.11n, into obsolescence by the end of 2018.

The best is yet to come, however.

Products based on Wave 2 of the 802.11ac standard are now available and promise to deliver even better data rates and throughput. Industry analysts say this will enable organizations to more easily support the growing number of de-

vices connected to their wireless LANs (WLANs), as well as a new generation of high-performance, high-bandwidth applications.

Shipments of 802.11ac Wave 2 access points doubled in volume in the third quarter of 2016, according to statistics from IHS Markit. The new technology accounted for about 10 percent of all wireless access points shipped during the third quarter, up from 5 percent in the previous quarter.

CERN, the European Organization for Nuclear Research, recently upgraded its wireless network with Wave 2 gear. That is a significant development, considering CERN operates the world's largest physics lab and is the birthplace of the World Wide Web.

CERN wanted a modern, mobile-first network to accommodate the nearly 20,000 different devices that need to connect to the network daily. The upgrade is designed to provide reliable coverage across campus, enabling visiting scientists and workers to use their own mobile devices. CERN also wanted the ability to properly sandbox visitor devices and detect rogue access points.

"With the mobility demands of our staff and scientists increasing, we knew that installing the right wireless infrastructure was critical to enabling a productive workplace," said physicist Tony Cass, leader of the Communications Systems Group at CERN.

Relieving Bottlenecks

While Wave 1 access points deliver speeds of up to 1.3Gbps, Wave 2 products are capable of almost doubling those speeds to multiple devices at the same time. The ability to wirelessly connect multiple users at full speed is extremely important in high-density environments such as offices, universities, hotels and hospitals — especially during peak times when bandwidth demands are highest.

Wave 2 technology can also quadruple the number of supported users, according to many experts. This is accomplished by using wider bandwidths and eight spatial streams, and introducing multi-user, multiple-input multi-output (MU-MIMO) technology. MU-MIMO creates greater separation between spatial streams and allows multiple data streams to be sent simultaneously on the same frequency channel. MU-MIMO relieves bottlenecks by allowing networks to transmit data to many users simultaneously instead of just one at a time.

While deploying Wave 1 products required minimal upgrades, making the jump to Wave 2 isn't as simple. Although 802.11ac is a wireless standard, the wired network needs to be able to support it. Upgrades to cabling and the network backbone are often necessary to avoid bandwidth bottlenecks.

Upgrade Considerations

Organizations using Gigabit Ethernet technology will have to upgrade to higher capacity switches to support Wave 2 wireless speeds and traffic. New specifications are currently being defined for both 2.5Gbps and 5Gbps Ethernet standards, which would enable organizations to get more bandwidth from existing Cat5e and Cat6 cabling. However, new switches would be needed to deliver faster speeds.

The larger leap is to 10Gbps, which would take full advantage of 802.11ac Wave 2, although it would likely require new cabling. However, an update to the cabling plant may be in order given trends toward ever-greater network speeds. Some companies are already looking at 40Gbps and even 100Gbps to ensure adequate capacity and avoid another upgrade down the road.

Another area that many experts believe will need to be addressed is the edge of the network, where wireless traffic is entering the network through the WAN or the Internet. If these pipes aren't wide enough to support increased wireless traffic, users won't experience the kinds of connection speeds that 802.11ac Wave 2 technology is capable of delivering.

"With the second wave of 802.11ac emerging in the market, network managers have greater choice in how to approach future wireless network upgrades," said Rohit Mehra, vice president, Network Infrastructure, IDC. "Wave 2 brings new capabilities for the WLAN to better serve as a tool for business innovation but may require deeper infrastructure upgrades. Network managers should engage in a thoughtful analysis on how to best deploy 802.11ac Wave 2 and extract maximum value."

Prepare for GDPR

Deadline nearing for tough, new data protection standard with a global impact.

The European Union's General Data Protection Regulation (GDPR) goes into effect in less than a year, and data security experts say it could be the strictest data privacy law ever enacted. Although it is designed to standardize data security legislation across Europe, it also has significant implications for U.S. companies.

Slated to go in effect in May 2018, the GDPR applies to all companies — no matter the size or location — that handle the personal information of anyone living in any of the EU's 28 member countries. U.S. companies with customers or employees in the EU could face fines of up to 4 percent of their global revenues for noncompliance. Small to midsized businesses (SMBs) are subject to the same regulations, although they are given some consideration due to the smaller amount of risk they present compared to large enterprises.

Despite the high stakes, many analysts say U.S. businesses are lagging in their compliance efforts. Gartner predicts that, by the end of 2018, more than 50 percent of companies affected by the GDPR will not be in full compliance with its requirements.

"The GDPR will affect not only EU-based organizations, but many data controllers and processors outside the EU as well," said Bart Willemsen, research director at Gartner. "Threats of hefty fines, as well as the increasingly empowered position of individual data subjects, tilt the business case for compliance and should cause decision-makers to re-evaluate measures to safely process personal data."

Getting Personal

GDPR requirements regarding personally identifiable information (PII) are particularly troublesome for U.S. companies. The regulation mandates that all companies must know exactly where every instance of someone's personal information is located. Furthermore, article 17 of the GDPR establishes a "right to erasure" that requires businesses to act on requests from individuals to have their data purged if it is no longer relevant or necessary.

However, analysts say the combination of data fragmentation and unstructured data hoarding within organizations will make it incredibly difficult for companies to comply with these provisions. The lack of visibility into dark data and information held outside of corporate IT systems complicates compliance. In a recent survey of 400 U.S. and European companies conducted by the market research firm Vanson Bourne, 85 percent of CIOs admitted that it is difficult to know exactly where all their customer data resides.

The growing use of unmanaged cloud-based file storage and consumer file-sharing services have become particularly problematic. A quarter of respondents to the Vanson Bourne survey admitted to using cloud-based services such as Dropbox, Google Drive, Syncplicity or Microsoft OneDrive against their current company policies. Another 25 percent reported running unrecognized offsite file storage services, making it even harder for IT departments to manage their use with recognized tools.

There isn't even a consensus on what comprises PII. Credit card, banking and health information are clear-cut examples, but what about IP addresses? PII is generally considered to be any information that can be used to distinguish one person from another. Jessica Rich, director of the Federal Trade Commission's Bureau of Consumer Protection, noted in a recent blog post that persistent identifiers such as static IP addresses, MAC addresses and cookies should be regarded as "personally identifiable."

Websites with data-capture forms fall within the scope of GDPR because they collect personal data. In a recent analysis of nearly 100,000 live websites, the security firm RiskIQ found that more than 30 percent would be in violation of GDPR because they are not securely capturing and processing personal data. In most cases, they were not using any kind of encryption or they were using very old encryption algorithms with known vulnerabilities.

Benefits of Compliance

With the deadline approaching, organizations should not waste time before beginning their compliance efforts. They must assess the IT environment, identify weaknesses and correct any flaws. Organizations must either appoint or outsource a data protection officer to oversee data management processes.

"Good data management practices are key to GDPR compliance success," said Carla Arend, Program Director, IDC. "Understanding where you have personal data — in which applications, on-premises or in the cloud, which processes use this data, and who owns it — is an important first step."

Although compliance will require significant time and resources, the new regulation shouldn't be seen just as a burden. It also presents an opportunity to improve operations and create competitive advantages.

Data quality is a key benefit. Poor data quality and haphazard data organization often keep data analytics from reaching its full potential. By forcing refinements in data collection and storage practices, GDPR can help organizations analyze data for deeper insights, improved workflows and cost efficiencies.

Improved data security delivers incalculable benefits. It reduces the risk of a breach, protects valuable data and diminishes the chance of financial losses from fines and remediation costs. Data security also improves an organization's reputation and boosts customer relationships.

GDPR compliance poses a challenge for companies of all sizes, but organizations should remember that the law's objectives are ultimately complementary to the objectives of most executives and organizations. Ideally, compliance should be seen as an investment that also helps an organization improve its ability to manage and protect its valuable information assets.

COMPLIANCE TIPS

Dell Technologies offers the following tips and strategies to help organizations achieve compliance with the European Union's General Data Protection Regulation (GDPR):

Appoint a data-protection officer (DPO). This is a requirement for GDPR, but companies have some flexibility. It can be a full-time, dedicated position, or it can be filled by an employee with other responsibilities. Smaller organizations can use an outsourced agency.

Deploy an access-governance solution. Companies must control who uses applications that permit access to the personal data of an EU resident. Governance generally requires periodic review of access rights by managers who must certify that the permissions align with their job roles and do not compromise data security.

Control access. Identity and access management tools can help ensure employees and contractors have proper permissions, but nothing more. Multifactor authentication, secure remote access, risk-based/adaptive security and granular password management can help provide control over user credentials and activity.

Protect the perimeter. Deploy next-generation firewalls (NGFWs) to reduce exposure to network attacks that could result in data leaks. NGFWs feature deep-packet inspection, real-time decryption and inspection of SSL sessions, adaptive, multi-engine sandboxing, and full control and visualization of applications.

Improve mobile security. Implement a mobile security strategy that ensures data protection while allowing employees to gain mobile access to critical apps and data.

Ensure email security. Mitigate the threat of phishing and other email-based attacks with a solution that delivers malware protection, secure messaging and encryption, and data leak prevention.

Focus on your business. We'll take care of the rest.

With a predictable, monthly cost structure, Sigma's comprehensive managed services reduce IT costs and risks. Contact us today to learn more.

SIGMA
A PIVOT COMPANY

www.sigmasol.com | 888.895.0495