SIGMA
SOLUTIONS

Vol. 10 No. 4

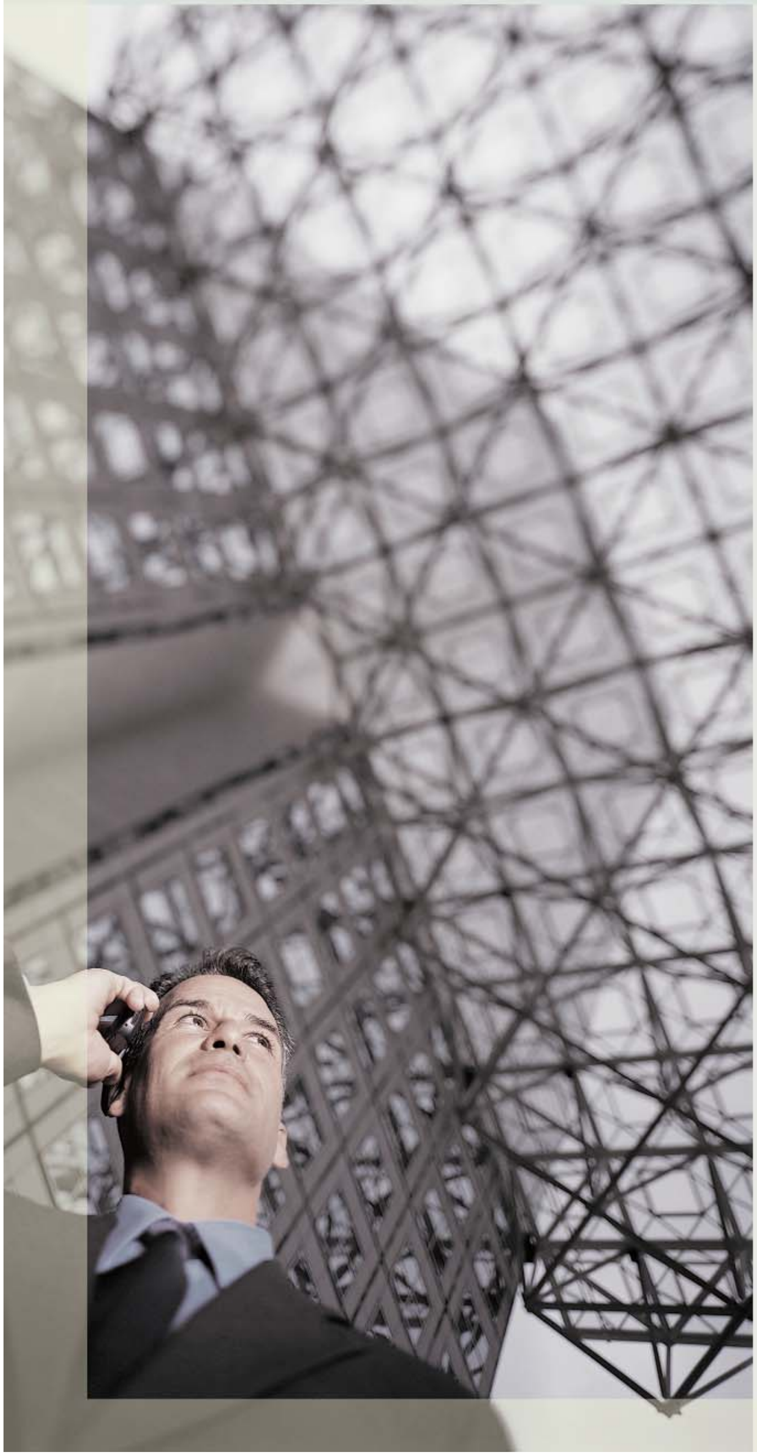
SigmaUptime

THE BIG PICTURE

Digital video is here to stay.
How will your organization deal with it?

SIGMA
SOLUTIONS

Focus on your business



Not on your technology

SIGMA Solutions' portfolio of **cloud services** and **managed services** helps you free up valuable resources so you can focus on strategic initiatives that are core to your business and customers.

SIGMA **cloud services** provide a complete technology stack to host your application without the burden of hardware acquisition, provisioning, system administration, or maintenance. SIGMA owns the assets with responsibility for guaranteed uptime. You only pay for what you need and when you need it with elastic capacity on demand.

SIGMA **managed services** transfer the lifecycle support of your infrastructure to our team of highly skilled engineers, who are orchestrated with a comprehensive methodology. We can provide blended support with your staff to manage systems in your building or in co-location facilities. All critical components of your data center can be protected and maintained including backup, administration, monitoring, change management and recovery.

SIGMA's local presence and flexibility provide the custom solutions your organization needs for large-scale project implementations, short-term initiatives or one-time engagements. Whatever your needs, SIGMA is the best technology partner to solve your data center problems.

800.567.5964 www.sigmasolinc.com

San Antonio, TX | Austin, TX | Dallas, TX | Houston, TX | New Orleans, LA | Tulsa, OK | Oklahoma City, OK

Contents

Sigma
UPTIME

Editorial Correspondence:
4941 S. 78th E. Ave., Tulsa, OK 74145
Phone (800) 726-7667 • Fax (918) 270-7134

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

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

the BIG PICTURE

Digital video is here to stay.

How will your organization deal with it?

If a picture is worth a thousand words, what is a video worth? It's a legitimate question for organizations in the YouTube age. Consumer demand for video content has never been greater, and the surge is naturally spilling over into the workplace in the form of videoconferences, Webcasts, training aids and more.

"The proliferation of video content in the enterprise is just another example of a 'bottom-up' technology that gains a foothold through personal use and eventually becomes ubiquitous within an organization. Instant messaging and social networking are other examples of technologies that gained widespread grassroots popularity before being brought under the official IT umbrella," said Marc DeHoyos, Senior Business Video Engineer, Sigma Solutions. "Video is perhaps the most compelling of these consumer technologies, and potentially the most disruptive to corporate IT. Organizations need the right tools to effectively create, deliver and support video across the enterprise."

Cisco offers a broad array of systems that use the network as the platform for video solutions that create powerful visual experiences across multiple devices and endpoints. The Cisco Digital Media Suite (DMS), for example, is an integrated platform for video collaboration, digital signage, and live and on-demand IPTV applications. It is designed to deliver compelling communications as well as an improved marketing and branding experience.

"A key component of Cisco's Business Video portfolio, Cisco DMS delivers a full spectrum of digital media applications," said DeHoyos. "Cisco DMS helps organizations take full advantage of video as a communications and collaboration medium."

continued on page 6

Changing Focus

Digital media offers organizations an incredibly valuable technology for improving external and internal communications. With video, organizations can provide relevant information in a compelling format, creating a richer experience for end-users and customers while improving collaboration, training, marketing and more.

Traditionally, however, digital media solutions were built with components from multiple vendors, requiring complex integration that significantly increased costs and limited scalability. In addition, traditional content management and distribution tools were too difficult for the average business user to operate.

"Cisco saw the need for an integrated solution that could handle the creation and management of video content and publish that content to a wide range of digital displays and endpoint devices," DeHoyos said. "Cisco DMS does that, and flexibly supports standard formats for live and on-demand video content publishing."

Cisco DMS includes Cisco Digital Signs, a complete digital signage solution, Cisco Cast, a business IPTV solution, and Cisco Show and Share, a social video system that enables highly secure online video communities. Cisco Digital Media Manager provides centralized, remote control for Cisco DMS applications and endpoints. Cisco's large-format, professional-quality LCD displays also form an integral part of Cisco DMS, creating a complete end-to-end solution for Cisco Digital Signs and Cisco Cast applications.

"Cisco is helping to transform media through medianet, a video and rich media architecture designed to help network operators and IT managers more effectively manage and deploy multiple video systems. Cisco's Enterprise Medianet Application Components — including digital media, video collaboration, IP video surveillance and telepresence — make it radically easier for customers to deploy and use video across the enterprise," said DeHoyos.

Wide Audience

The medianet technologies in Cisco's Media Processing portfolio are optimized to enable better video experiences, faster delivery of rich media content and simplified media sharing across the network. A key component is the Cisco Media Experience Engine (MXE), which gives customers access to a wide variety of media-processing services that enable live and on-demand video and rich media to be consumed on any device at any time, regardless of format. The create-once-and-share-anywhere Cisco Media Processing platform provides media conversion, editing, formatting and network distribution capabilities in a single networked solution.

"The Cisco MXE delivers the ability to transform a single source of content so that it is playable on PCs, mobile devices and other digital screens. If the media is not in the right format for the endpoint, it can be automatically adapted to deliver an outstanding experience," DeHoyos said. "Cisco MXE also provides real-time post-production and processing capabilities such as voice and video editing, text and image overlays, and noise reduction to create broadcast-quality video."

Cisco's suite of plug-and-play, medianet-enabled endpoints include embedded intelligence that enables the network to automatically recognize and configure the endpoints when they are deployed. These auto-configuration capabilities simplify deployments and help reduce the ongoing operational costs of rich-media applications.

"These 'smart' endpoints include Cisco Digital Media Players, which offer customers flexibility in the type of content they can create. They also enable delivery of high-definition video and Adobe Flash technology to digital displays," said DeHoyos. Cisco Digital Media Players and Digital Media Encoders are key components of the Digital Media Suite."

Rave Reviews

Built into these endpoints is the Cisco Media Services Interface, which gives the network visibility into the applications and applications visibility into the network. This tight integration helps organizations scale, optimize and enhance the deployment and performance of video, greatly improving user experience.

"Cisco DMS utilizes the underlying network as a platform for the efficient distribution and streaming of digital media content to a large and dispersed user base," DeHoyos said. "It complements the inherent quality of service and traffic-management capabilities of the network to support live streaming and provide on-demand access to video files. It prioritizes, secures and separates video traffic for optimized viewing while reducing video bandwidth to minimize its effect on network traffic."

YouTube has helped make video ubiquitous, with the vast majority of Internet users regularly watching video online. Organizations that see video applications as irrelevant to their operations risk alienating employees and customers who want video communication services. Digital video is here to stay, and smart organizations are investing in the tools they need to take maximum advantage of it.

"Video can have a significant impact on the way we interact and manage, educate and promote," said DeHoyos. "Cisco Digital Media Suite helps customers use video more pervasively while also helping to solve challenges around video delivery, interoperability and quality. It also extends digital media to new applications for real-time and on-demand communications."

Cisco Digital Media Suite Snapshot

■ **Cisco Digital Signs** provides scalable, centralized management and publishing of high-quality content to networked, on-premises digital signs. Digital signs offer many applications in retail sales and marketing, event broadcasts, training, directions and other useful information.

■ **Cisco Cast** allows organizations to deliver live and prerecorded content that is controlled by the end-user. Content can include sales and marketing information, training, corporate communications, news and entertainment.

■ **Cisco Show and Share** creates highly secure communities for video discovery and harvesting across the enterprise. It gives users access to video on demand and live webcasts, and allows them record, upload and edit video. Digital media can be browsed, searched and viewed through an easy-to-use interface.

The Front Lines of Security

More organizations are investing in endpoint security solutions to reduce the risk of security breach and the loss of sensitive data.

In the thick of battle, it's sometimes hard to sort out the bad guys from the good guys. That's increasingly true in network security. While combating a growing array of security threats, network administrators must also support the mobile workers, business partners, consultants, contractors and customers who require access to corporate network resources. These end-users have a wide range of options for gaining access thanks to pervasive wireless connectivity and a proliferation of mobile devices, yet they often fall outside IT's direct control.

For all their productivity and collaboration benefits, those devices and connections create multiple avenues for introducing viruses, worms and other malwareinto an organization. They also make it difficult to control access to applications and data, and expose sensitive corporate information to loss or theft. Endpoint security solutions can help separate friend from foe, and ensure that end-users have the access they need without increasing network security risks.

Halt! Who Goes There?

IBM recently released results from a survey of nearly 300 IT decision makers on their companies' endpoint security initiatives. The study, conducted by Zogby International, revealed that 90 percent of business leaders are investing in resources to better manage the security of their endpoints. Over half of those surveyed are also extending security to smartphones and other instru-

Experts estimate that by 2015 there will be approximately one trillion connected devices. Each will be generating, transmitting, consuming or analyzing data.

mented devices, with plans to increase spending in this area.

Endpoint security solutions encompass an array of tools that help IT ensure that endpoint devices are compliant with security policies. The most basic solutions check to see if the endpoint device has up-to-date antivirus software; if not, a centrally managed tool pushes updates out to the device. Endpoint security is expanding, however, to include intrusion detection and prevention and behavior-blocking applications that look for activity associated with malicious software.

The most sophisticated endpoint security systems incorporate network access control (NAC) to grant access based upon the end-user device. NAC solutions help organizations enforce their security policies by extending traditional definitions of authentication, authorization and access control to include more detailed endpoint inspection. NAC software validates the end-user's credentials, scans the device for compliance with policies requiring up-to-date operating systems, malware prevention and mandatory corporate applications, and ensures that no unauthorized software is installed. Devices that do not match policy mandates may be denied access, quarantined or granted limited access.

These solutions work hand-in-glove with identity management to create seamless security for the distributed network. In addition to making users prove their identities, endpoint security makes the devices themselves prove they're secure before they can log onto the network.

Assessing the Risk

Experts estimate that by 2015 there will be approximately one trillion connected devices, whether traditional PCs or laptops, mobile devices such as smartphones or tablets, point-of-sale (POS) systems, ATMs, retail kiosks, or sensors in smart meters, buildings and other off-premises devices. Each of these devices will be generating, transmitting, consuming or analyzing data, and it is critical that they remain available, secure and configured in accordance with company and regulatory policies and requirements.

As the survey results indicate, organizations recognize they are facing an evolving security landscape, given all of the new computing endpoints being added to their networks every day. Organizations must not only manage the security of PCs and laptops, but keep up with demands to secure the influx of smartphones and other instrumented devices interacting with their corporate infrastructure. Eighty percent of survey respondents expect their organization to add new endpoints to their network in 2011.

Although 73 percent of the business leaders surveyed currently allow nontraditional endpoints such as mobile devices or tablets to connect to their corporate networks, 36 percent feel that these devices are not adequately protected and would like to see their companies invest more in managing the security of smartphones, POS systems and other smart devices. Nearly 40 percent of those surveyed indicated that their company is planning to increase their investment in security to manage and protect nontraditional endpoints.

While 72 percent of respondents say that PCs and laptops pose the greatest danger to their firm's IT security, smartphones and tablets are viewed as a growing threat. A third of all respondents acknowledged that a lack of visibility into all endpoints is their greatest security concern.

The War on Data

However, research suggests that organizations are more confident in their ability to detect and control malware and security breaches than in their ability to secure data on endpoint devices. The IBM X-Force 2010 Trend & Risk Report indicates that while vulnerabilities and attacks exist, exploitation of endpoint devices is not prevalent yet. Instead, most IT professionals view the data that can be stored on them and how that can be misused or lost as the main security threat associated with these devices.

The risks are very real. According to the Ponemon Institute, data breach incidents cost U.S. companies $214 per compromised record in 2010, compared to $204 in 2009. Average total per-incident costs in 2010 were $7.2 million, compared to an average per-incident cost of $6.75 million in 2009.

Clearly, enterprises must ensure control of their data regardless of where it is stored, including employee-owned or business-issued smartphones and other smart devices. Experts say that advanced password management and data encryption are the best defense against data leakage from endpoints. Effective data protection not only reduces the risk of a costly breach but improves regulatory compliance.

Mobile computing and smart devices offer the enterprise significant benefits, but security still remains a primary hurdle for organizations managing the influx of these devices. Endpoint security solutions can help ensure that only friendly devices gain access to the network, and that data is protected across the extended enterprise.

Are You Cloud-Ready?

Upfront assessment of applications, architecture key to successful cloud initiatives.

Cloud computing promises to dramatically increase the speed with which applications are designed, built and delivered. To reap all these benefits, however, organizations must do their homework and make good decisions up front. An excellent starting point is a cloud readiness assessment.

A readiness assessment can help organizations determine what applications can most effectively be shifted to a cloud platform. Despite the overwhelming industry hype, the cloud isn't always the most suitable choice for certain applications, particularly those with heavy computing power, network bandwidth and online transaction processing (OLTP) requirements.

Only by aligning the architecture — compute, network, data center, power and storage resources — with applications can an organization be on the path to achieve the reliability and performance it requires within a cloud environment.

"In cloud computing, true protection is an outcome of the right architecture for the right application," said Janel Ryan, senior product marketing manager at SunGard Availability Services. "Organizations need to fully understand their individual application requirements and, if using a cloud platform, the corresponding cloud architecture. With that knowledge, they can make informed decisions about what cloud platform best meets the reliability and performance requirements of their specific applications."

Here are five considerations for companies looking at cloud computing architectures.

AVAILABILITY. Not all applications are created equal, nor are all cloud platforms the same. Organizations need to tier their applications, identifying which applications need to be highly available, which can accept downtime and how much downtime is acceptable. They need to understand the business risk associated with a lack of availability of their data. For those applications that need to be highly available, businesses should consider enterprise-class technologies that have been rigorously tested versus looking at building something internally. It's also important to look at multi-site solutions and disaster recovery/business continuity planning. For most businesses, this means working with a service provider or consultant because they usually have access to greater levels of expertise and provide these services as their core business.

SECURITY. Security is still the primary concern for businesses regarding the cloud. Concerns include the loss of control of their sensitive data, the risks associated with a multitenant environment, and how to address standards and compliance. Organizations need to know how a shared, multitenant environment is segmented to prevent customer overlap. How is the solution architected? Is the service provider's cloud infrastructure — network, virtualization and storage platforms — secure?

MANAGEABILITY. Businesses need to determine what they are accountable for versus what they expect from a service provider. Most public cloud vendors do not provide administrative support. Organizations need to have the technical expertise in-house to design the right solution or seek the services of an outside provider. They should define what level of management their applications require and have an identified change management process.

PERFORMANCE. As with a more traditional hosting model, it's important to understand workload demands on the infrastructure and what the potential bottlenecks are. Organizations should perform their own testing to evaluate how a cloud environment affects compute, storage and network resources.

COMPLIANCE. Organizations need to determine where their data will reside as well as who will interact with it and how. They need to understand which areas of compliance the service provider controls and how to audit against the standards and regulations to which they need to adhere.

5 REASONS CUSTOMERS CHOOSE SIGMA SOLUTIONS

STRENGTH – Sigma has an unmatched ability to respond to customer needs due to our scale, locale and experience in the data center. We are small enough to deliver local, personalized service yet large enough to handle highly complex project requirements.

INNOVATION – Our goal is to help customers leverage IT solutions to streamline business processes, drive innovation and reduce time to market. To that end, Sigma delivers technologies from industry-leading manufacturers coupled with consulting and engineering services that maximize business value.

GUIDANCE – Our customers turn to us for expert solution design and project governance services that accelerate the success of their IT initiatives. Sigma mitigates our customers' risks through our experience and commitment to excellence in everything we do.

MANAGEMENT – Sigma is uniquely positioned to serve as a single point of contact for full lifecycle management, maintenance and support of converged and integrated technologies. Our expertise across the data center and strong relationships with industry leaders enable us to quickly resolve problems in today's complex IT environment.

AGILITY – Sigma's comprehensive services enable our customers to partner with one technology provider for solution design, implementation and ongoing service. Sigma serves as the focal point for initiatives incorporating diverse technologies and multiple IT disciplines.

SIGMA
SOLUTIONS

800.567.5964
www.sigmasolinc.com

AUSTIN | DALLAS | HOUSTON | SAN ANTONIO | TULSA | OKLAHOMA CITY | NEW ORLEANS