

SigmaUptime

Optimizing
Desktop
Virtualization



UPTIME

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

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 | El Paso, TX
Chicago | New Orleans | Little Rock, AR | Tulsa, OK | Oklahoma City, OK

4 Optimizing Desktop Virtualization

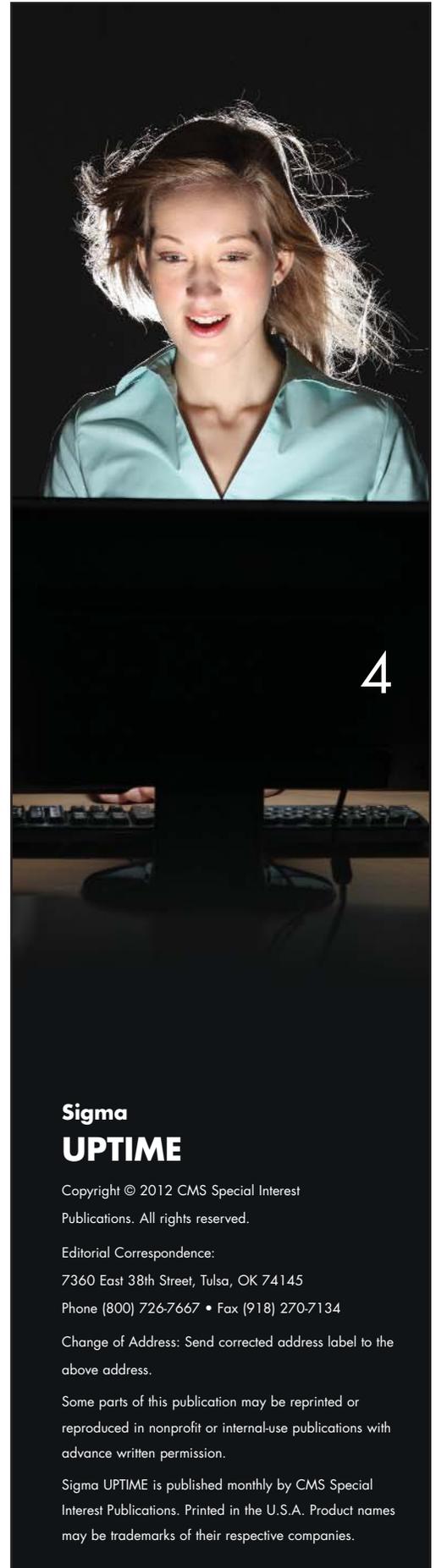
Desktop virtualization creates a user-friendly experience uncoupled from the traditional desktop locked to a location, device or network. However, it also increases demands on the storage infrastructure. Virtual desktop infrastructures based on VMware View integrated with NetApp's Unified Storage improves desktop efficiencies by extending critical operations such as backup and recovery, de-duplication, desktop cloning and storage system monitoring to desktop and server administrators.

8 Users without Boundaries

Distributed computing models and cloud-based services have created new challenges for identity and access management (IAM) solutions, which provide a framework for managing users and their access privileges across the enterprise. Federated identity management provides the mechanism for dealing with these challenges by enabling users to access external resources with a single credential, and by streamlining identity provisioning and management across distributed resources.

10 Who Can You Trust Now?

Certificate authorities (CAs) issue the digital certificates that validate the authenticity of secure websites. However, several major CAs have been hacked in recent months, leading to the release of numerous fraudulent certificates. Experts say enterprise organizations must develop recovery plans for dealing with the possibility of compromised trust providers.



Sigma UPTIME

Copyright © 2012 CMS Special Interest Publications. All rights reserved.

Editorial Correspondence:

7360 East 38th Street, Tulsa, OK 74145

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.

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.

OPTIMIZING DESKTOP VIRTUALIZATION

NetApp unified storage technologies integrate with VMware View to help maximize the efficiency of desktop virtualization solutions.





Desktop virtualization is changing the way organizations deploy and manage desktop computing environments. Desktop virtualization creates a user-friendly experience uncoupled from the traditional desktop locked to a location, device or network. It also frees IT from the distributed desktop management burden through a centralized solution that is easier to support and secure.

At the same time, however, desktop virtualization introduces new complexities in the data center — particularly with regard to storage. Each virtual machine (VM) includes the user's operating system and applications, and can be tied to hundreds or thousands of documents across multiple desktops. As a result, storage capacity requirements for desktop data can reach tens or even hundreds of terabytes, dramatically impacting performance while driving up the costs of the storage stack and the desktop virtualization infrastructure.

"The storage subsystem must be designed to control the size of data volumes and relieve I/O bottlenecks," said Jon Chappell, Competency Center Manager, Sigma Solutions. "Organizations need efficient deduplication, cloning, data protection and replication, as well as high-performance storage. Sigma has found that NetApp's storage technologies can help customers reduce the cost of storage for virtual desktops and accelerate response times for an optimal user experience."

Under the Hood

Desktop virtualization separates the desktop environment from a particular compute resource, application environment and user environment. These "elements" of the desktop are virtualized in the data center so that they can be accessed via a wide range of devices from any location. If properly architected, these elements join together to create a rich user experience indistinguishable from the traditional desktop.

"Desktop virtualization re-creates an end-user's desktop as a virtual machine that combines the core operating system instance, application settings, data and personal settings. The desktop experience becomes just another resource residing on the enterprise network," Chappell said. "It seems complex but it's actually more flexible and easier to manage than the traditional desktop. The user, application, core operating system and endpoint device are decoupled from one another, making it possible to manage each separately. Yet the user experience does not change."

An essential piece of the desktop virtualization puzzle is the data center infrastructure. Desktop virtualization requires a data center that is optimized for virtualization — flexible, interoperable and simple to manage. A hardware virtualization layer such as VMware vSphere provides the numerous VMs that are used to host desktop images for multiple users. A desktop virtualization solution such as VMware View delivers desktop images to end-user devices and provides desktop management and other features.

continued on page 6

Lean Machine

Because it is integrated with VMware View, NetApp improves desktop efficiencies by extending critical operations such as backup and recovery, de-duplication, desktop cloning and storage system monitoring to desktop and server administrators. This not only reduces costs but simplifies desktop data management. The cascading effect of NetApp storage efficiencies across all storage tiers continues to cut storage costs as virtual desktops are added.

“Although VMware View can reduce desktop computing costs by up to 50 percent, it may not show an immediate ROI because of the back-end hardware and storage required to prepare such an infrastructure. Longer-term ROI is realized through more efficient management and scaling of application and desktop resources,” said Chappell. “The integration of NetApp’s unified storage technologies enables VMware View customers to achieve enhanced storage efficiency and virtual desktop scalability.”

VMware View enables the “provisioning” or “cloning” of a single OS image across hundreds or even thousands of virtual desktops to minimize the amount of storage required. The integration of NetApp Rapid Cloning Utility into VMware View Manager enables IT to manage desktops from a single framework. NetApp SnapManager and SnapMirror also integrate with VMware solutions to automate and simplify desktop backups, disaster recovery and failback.

High Performance

NetApp helps significantly improve performance with Flash Cache, which allows

read requests to be served out of high-speed, solid-state cache that can be up to 100 times faster than average high-speed disk drives. Flash Cache speeds data access through intelligent caching of recently read user data and NetApp metadata in the storage controller. Flash Cache enables organizations to increase I/O throughput by up to 75 percent and use up to 75 percent fewer disk drives without compromising performance.

“A positive end-user experience is essential to the success of any desktop virtualization deployment,” Chappell said. “VMware View’s PCoIP display protocol efficiently delivers virtual desktop environments to a wide range of endpoints over low-bandwidth network connections. NetApp complements VMware View by providing low-latency data access that accelerates response times even during intense activity such as boot storms, login storms and antivirus updates.”

Desktop virtualization can reduce costs, increase IT efficiency and improve security and compliance. It can also enable anytime, anywhere access to information while supporting a wide range of user needs. It’s important to remember, however, that a well-architected storage infrastructure is critical.

“In the past, organizations had to choose between cost reduction and a robust, IT-as-a-service model,” said Chappell. “NetApp’s seamless integration with VMware View optimizes desktop virtualization through a cost-efficient and easy-to-manage solution. It enables organizations to control storage requirements, accelerate ROI and deliver a no-compromise user experience.”

NetApp and VMware teamed to build a global, 50,000-seat desktop virtualization reference architecture — the largest documented virtual desktop deployment — to provide customers with a joint architecture that is easy to replicate and deploy. The flexible and dynamic solution supporting a Windows 7 environment was built using NetApp FAS storage, NetApp Virtual Storage Console, VMware View and VMware vSphere. Cisco, Fujitsu and Wyse also collaborated on the project, providing the server, network and thin-client technology to deliver an end-to-end scalable solution. In addition to getting an industry-leading partner ecosystem with a track record in desktop virtualization, customers also benefit from a proven architecture that easily scales from 5,000 to 50,000+ seats with minimal impact on performance.

The New View

VMware View 5 is the latest release of VMware’s desktop virtualization platform. VMware View 5 delivers new levels of innovation and simplicity with advanced 3-D graphics, scalable unified communications and integrated persona management to help IT organizations empower a more agile, productive and connected enterprise.

VMware View simplifies IT manageability and control, while providing a high-fidelity desktop virtualization experience. It delivers protocol enhancements that provide as much as 75 percent bandwidth improvement over LAN and WAN connections to support voice and video media services.

VMware View 5 enables organizations to deliver a better Windows-based desktop-as-a-service experience while doing more with what they already have. VMware is helping customers move rapidly into the cloud and embrace mobility and collaboration. VMware has truly taken virtualization to the next level.



Better together

Some things just seem to be made for each other — and when it comes to desktop virtualization, VMware® View™ and NetApp® Unified Storage are a perfect pair. VMware View is the No. 1 choice for delivering virtual desktops as a managed service, and NetApp Unified Storage fully addresses the increased storage demands created by desktop virtualization.

Contact Sigma Solutions to learn more about VMware and NetApp integrated solutions.



800.567.5964

www.sigmasolinc.com

Users without Boundaries



Federated identity and access management enables single sign-on and user provisioning across distributed networks and cloud-based services.

Organizations today are increasingly dependent upon partners that span supply chains, brokers and other networks. Likewise, organizations are adopting Software-as-a-Service (SaaS) solutions and creating partnerships with application providers such as Salesforce.com, Concur and SuccessFactors.

These distributed computing models and cloud-based services have created new challenges for identity and access management (IAM) solutions, which provide a framework for managing users and their access privileges across the enterprise. IAM tools include user provisioning, password management, strong authentication, single sign-on and other technologies, which are

increasingly bundled into comprehensive platforms. Traditionally, however, these solutions are designed to operate within the enterprise security framework.

Organizations are now grappling with a new definition of “identity” — one not just contained within internal applications and data. In a supply chain, for example, organizations must figure out how to integrate external user groups into their security controls in order to provide access to appropriate resources. Organizations that use SaaS solutions must also manage user credentials outside the enterprise security framework.

Federated identity management provides the mechanism for handling this new identity paradigm. It enables

business-to-business integration by making identities portable and enabling the exchange of identity data. Federated identity management offers two key benefits: it enables users to access external resources with a single credential, and it streamlines identity provisioning and management across distributed resources.

Federated Single Sign-On

The growing popularity of SaaS applications has increased demand for federated identity management solutions. Many organizations are looking to use federation so that users don't have to manage multiple IDs and passwords for SaaS applications.

Federated identity management enables organizations to provision

users, roles and entitlements to partner applications in a secure, open-standard format. If users regularly access applications hosted by a business partner that leverages federation technology, Federated Single Sign-On (FSSO) will act as a bridge, allowing internal user credentials to be transformed and accepted by those partners. As such, federation facilitates single sign-on across third-party providers, allowing users to seamlessly access applications that are hosted by a partner. Upon clicking a link posted within an enterprise portal, the user is seamlessly logged into the external application or resource — no user ID or password required.

The end result is a seamless SSO experience for the user. Whether partner applications are private (such as a distributor's warehousing application) or cloud-based (such as Salesforce.com), FSSO can help improve user productivity, reduce help desk calls for forgotten passwords and improve identity lifecycle management.

Various open-standard protocols have emerged to address the challenge of extending IAM to external applications. These protocols, which allow independent parties to securely share identity information, form the basis of federation. FSSO relies on open-standard protocols, such as Security Assertion Markup Language (SAML) and Web Services Federation (WS-Federation), that are platform and technology agnostic. The parties need not be concerned with the operating systems, software or other technologies implemented on either end of a federated relationship. Federation protocols enable existing identity information about a user to be securely transmitted between the two parties.

Improving Security

Maintaining a discrete set of user identities within cloud applications is more than a hassle — it's a security threat. In June 2011, Google announced that computer hackers in China broke into the Gmail accounts of

several hundred people, including senior government officials in the U.S. and political activists. Google believes Chinese hackers used phishing scams to trick people into sharing their passwords. This attack highlights the need for enterprises to take control of user credentials and authentication for SaaS applications.

The good news is that many SaaS providers are now exposing mechanisms that enable programmatic management of identities within their environments. For example, Google allows enterprise customers to leverage the SAML protocol to delegate the control of authentication. Companies can safely keep their Gmail user credentials where they choose and take control of the Gmail authentication process away from Google.

Federated identity management can also help organizations share their Web applications with partners in a cost-effective and timely manner. Utilizing federation services, organizations can easily accept federated assertions of identity such as SAML, WS-Federation and OpenID, allowing business partners to log in seamlessly without the need for a native user ID and password. This improves productivity for users, increases the appeal of the organization's services, and eliminates the need for partners to maintain another set of IDs and passwords.

Organizations that integrate extensively with third parties or utilize SaaS solutions must deal with an increasing number of user accounts maintained on affiliate or partner applications. As a result, managing application accounts across the business-to-business boundary is becoming a priority. Federated identity management can help streamline and standardize the process of business-to-business identity management by enabling organizations to securely share user credentials with business partners. Federation allows organizations to share identity credentials and facilitate single sign-on for access to external resources.

OASIS to Define Trust Elevation Standard

The OASIS international open standards consortium has begun work to define a set of standardized protocols that online service providers may use to elevate trust when authenticating electronic identity credentials. The goal of the new OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) Technical Committee is to extend interoperability among online service providers — such as banks and healthcare providers — and make e-transactions easier for end-users.

The OASIS Trust Elevation protocol will be vendor-neutral and product-agnostic. It will promote interoperability among multiple identity providers as well as among federations and frameworks. The work will reconcile the fundamental gap between credential-based trust approaches used in e-government and transaction-risk-mitigation-based trust approaches used in business-to-business applications.

The Trust Elevation Committee was formed in response to governments calling for national and global identity infrastructures to be developed through private-sector cooperation among providers, users and subjects of trusted identity systems.

OASIS (Organization for the Advancement of Structured Information Standards) is a nonprofit, international consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for security, privacy, cloud computing, SOA, web services, the Smart Grid, content technologies, business transactions, emergency management, and other applications.

Who Can You Trust Now?

Venafi calls on enterprises to formulate certificate authority disaster recovery plans in the wake of widespread breach.

The Secure Socket Layer (SSL) encryption and authentication technology built into every Web browser relies upon the concept of trust. When a browser requests a secure page, the web server sends its public key with its certificate. The browser checks that the certificate was issued by a trusted party, usually a root certificate authority (CA). If the certificate is still valid and related to the site, the browser proceeds — all because of the implicit trust in the CA. Most browsers and applications have already loaded the root certificate of well-known CAs.

What if the CA is compromised?

That very chilling scenario has become a startling new reality in the world of SSL encryption. Over the past few months, attackers have hit several major CAs, including Comodo, StartSSL and DigiNotar. The attackers have stolen certificates and, in some cases, issued fraudulent certificates to themselves. An attacker even published one of RSA's private encryption keys.

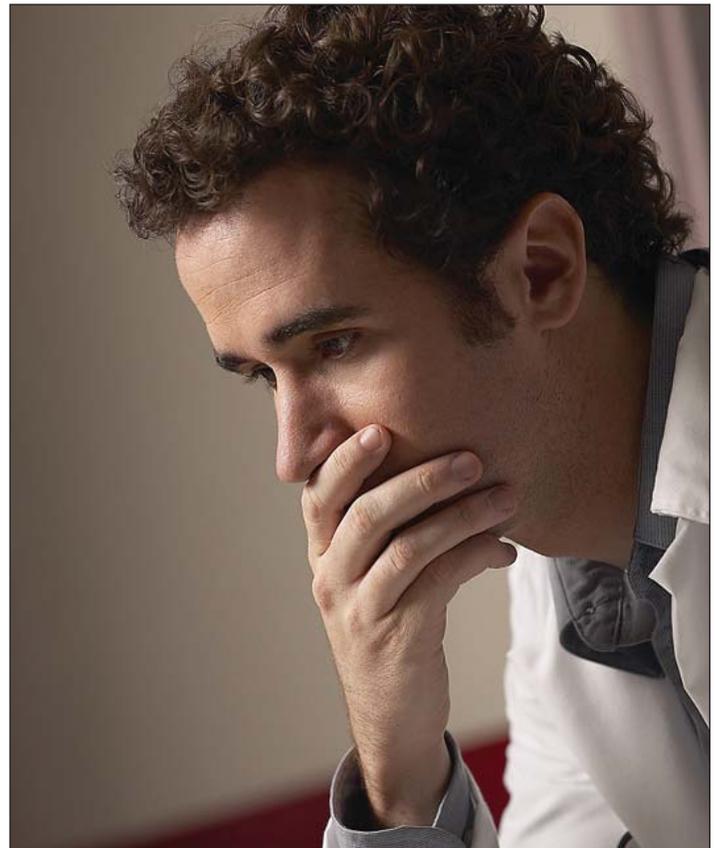
The implications are serious and far-reaching. A signed certificate cannot be modified, so a certificate is not secure until it is signed. However, you can sign a certificate using itself — a so-called self-signed certificate. All root CA certificates are self-signed.

By some estimates, more than 530 certificates have been stolen. This may include so-called intermediate signing certificates, which would enable the attackers to sign and validate certificates that seem to come from trusted sources. How do you know that you are dealing with the right web site if you can't trust the certificate or the person who signed it?

Tip of the Iceberg

With DigiNotar recently joining the ranks of Comodo, StartSSL and RSA as a trusted third-party CA compromised by hackers, enterprises need to move past the shock and begin formulating their own compromise recovery and business continuity plans, say experts at enterprise key and certificate management (EKCM) firm Venafi.

"People have not given much thought to the impact or ramifications of a certificate authority compromise," said Venafi CEO Jeff Hudson. "The attack against DigiNotar marks 2011's fourth major breach of a trusted third-party security provider. There will be more breaches of third-party trust providers like this in the future."



Hackers apparently used the fraudulent certificate to intercept Iranian users' email, among other items. The attack went undetected by the users because their browsers trusted the DigiNotar certificate.

"A third-party trust provider represents an extremely high value target for hackers. Once attackers can access and steal trust credentials, they can commit various cybercriminal acts in pursuit of their own nefarious agenda," Hudson said.

Hudson went on to explain that SSL and PKI remain solid and reliable technologies. That does not mean that enterprises can relax. They need to be aware that any individual third-party trust provider, like a CA, can be compromised and is therefore a known risk.

"And," he added, "known risks require solid, well-conceived contingency plans."

Beyond the Browser

Mozilla, Google and Microsoft have implemented browser updates that will revoke trust in certificates signed

by compromised CAs, which will safeguard users of those browsers. The ripple effects of a hack like this do not stop at the browser, however.

“All enterprises need to look at their highest-value assets — servers, VPN concentrators, SSL off-loaders, application servers and applications where sensitive and regulated data flows, and that are protected by certificates,” Hudson said. “Plans must be in place to recover anytime the trust provider is compromised.”

Hudson says there are steps organizations must take to deal with a compromised CA. First, they must use multiple CAs so that if one is compromised, the other non-compromised CA and its certificates and keys are available for continued use. Second, organizations must have an accounting of all the CAs that they use as third-party trust providers. Third, they must have a complete inventory of the owner and location for each certificate in the enterprise. This often numbers in the thousands and even tens of thousands or more in Global 2000 organizations.

Finally, every organization must have an actionable and comprehensive plan in place to recover from a CA compromise. The time to recover needs to be measured in hours, not weeks or months.

Cover Your Assets

Hudson said that most enterprises have glaring holes in their certificate inventories. An organization may estimate that it has, say, 3,000 certificates, when in reality it has two or three times that number. That many unidentified certificates represent significant unmanaged and unquantified risk.

Further, few organizations have a management platform in place that gives them the power to replace compromised certificates quickly. Otherwise, the replacement of known, compromised certificates is largely a manual effort. This forces organizations to continue operations in a compromised condition — possibly for many months — while the thousands of compromised certificates are manually replaced. In some cases that may not even be an option and entire systems may have to be shut down until remediated.

“None of us knows where the next breach will occur,” Hudson said, “or whether it will occur in a week or three months. Enterprises must ready themselves to respond immediately if they implement the four steps of CA compromise recovery. The very serious implication is that you better wake up. Get out of denial. Understand that this is a huge issue of business continuity. And don’t think you won’t be compromised, because you will.”

In theory, SSL certificates provide proof that you are talking to a bona fide entity on the Internet. That theory is being challenged by a rash of security breaches at root CAs. If you can’t trust the trusted third party, who can you trust?



welcome to the **secure** borderless network

An influx of technology, devices, and communications infrastructure has expanded our ability to collaborate and stay connected. While the benefits are clear, this brings additional risk and poses a new challenge for security professionals.

Cisco® Secure Borderless Networks enable today’s workforce to stay productive, while helping businesses control the cost and complexity of network security. By integrating security into the distributed network, the Cisco Secure Borderless Network extends security to the right people, devices, and locations, enabling customers to build solutions that keep their organizations secure, and positioning them to address continuously evolving business and security challenges.

Contact your Sigma Solutions representative to learn how the Cisco Secure Borderless Network can keep your entire organization secure and ready to meet your business objectives.

SIGMA
SOLUTIONS

800.567.5964
www.sigmasolinc.com

Copyright © 2012 Cisco Systems, Inc. All rights reserved. CIS-100



REASONS CUSTOMERS CHOOSE SIGMA SOLUTIONS

S **TRENGTH** – 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.

I **NNOVATION** – 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.

G **UIDANCE** – 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.

M **ANAGEMENT** – 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.

A **GILITY** – 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
S O L U T I O N S

800.567.5964
www.sigmasolinc.com

SAN ANTONIO | AUSTIN | DALLAS | HOUSTON | EL PASO | CHICAGO | NEW ORLEANS | LITTLE ROCK | TULSA | OKLAHOMA CITY