Software-as-a-Service: Performance and security requirements on WANs

White paper

> "To reliably deliver on SLAs and to truly provide consistent performance to customers, SaaS companies need flexible solutions that fit the widest possible range of computing environments."

Executive summary

While software-as-a-service (SaaS) first took hold in small and medium-sized businesses, even large-scale enterprises are now deploying SaaS to cut software acquisition and maintenance costs. However, according to market research, the top three reservations customers have in implementing SaaS are security, lack of control, and the reliability and performance of SaaS applications. Nearly all of these concerns can be addressed with the proper deployment of SaaS. This paper discusses the challenges of delivering secure, reliable SaaS over WAN infrastructures and offers solutions for companies selling SaaS solutions and for potential purchasers of network-delivered applications.

Introduction

While SaaS primarily originated in small to medium-sized businesses as a means to save on software purchases, larger enterprises are now increasingly deploying SaaS applications. (Holinchek, 2006) In 2007, 75-percent of SaaS industry revenue was generated from companies with more than $1 billion in revenue.[1] Regardless of the company size, saving money on software purchases and maintenance is the primary motivator of outsourcing applications. Companies no longer need to spend management resources tracking down software fixes and upgrades, nor do they need to meticulously track software license compliance. The latest version of the application is always online. Licensing is on a per-use basis, not per seat.

Another chief reason for deploying SaaS is that it eases the burden on the customer's computing infrastructure. Buying and installing software has a significant impact on a customer's local storage, network, servers, and desktop resources. SaaS places a lesser burden on these components.

For these reasons, the pay-as-you-go model of SaaS applications has seen tremendous growth over the last three years. However, companies about to deploy SaaS solutions as an alternative to traditional software and service providers offering SaaS applications to customers should take note of the potential pitfalls in delivering software over WAN connections.

Deploying SaaS over WANs

Unless SaaS applications are offered as in-house, firewall-protected applications, they must travel at least part of their delivery route over the public WAN. The conditions on this public network are almost entirely out of the control of either the SaaS customer or the SaaS software provider. The nearly serendipitous routing of traffic over the Internet and the inconsistent traffic and congestion along the routes make predictable

1 eWeek "Ten Things You Should Know About SaaS." September 2007. http://www.eweek.com/c/a/Enterprise-Applications/10-Things-You-Should-Know-About-SAAS/1/

performance impossible. In addition, the open nature of the network leaves data – even secure socket layer (SSL)-protected data – vulnerable to attack, data hijacking, or diversion.

Customer concerns when deploying SaaS

In polls and surveys taken by leading analyst groups, the three top concerns of companies when deploying SaaS are:

- Security
- Lack of control
- Reliability and performance

While companies can ensure security themselves when installing software on their premises, SaaS applications are offsite and beyond traditional security parameters. The nature of SaaS application architecture, such as hosting multiple customers on each SaaS host (multi-tenancy) and storing data on a server outside the enterprise, certainly underscores the sense that data may be at risk.[2] Exacerbating this sense of lack of control is the very nature of data communications over a public network. Many companies are reluctant to outsource mission-critical applications that are delivered over unsecured, public WAN connections.

The inherent unpredictability of public network WAN performance contributes to the uneasiness on the part of some potential SaaS customers. If applications lag, lose data, or crash due to congestion or outages on the public WAN, company productivity suffers. Understandably, many companies will not consider subscribing to SaaS applications until reliability and performance problems are solved to their satisfaction.

Challenges for the SaaS provider

To become successful, SaaS developers must address these security, control, and performance concerns. Doing so requires either a multitude of point product applications or a suite of flexible products that are easily deployed on both the client and service provider sites. Further complicating this scenario of ensuring performance and security is the fact that customer sites have widely disparate computing infrastructures. Delivering a consistent security and performance boost to every customer would require analyzing each customer site for the appropriate approach, adding precisely the complexity to a SaaS deployment that customers are seeking to avoid.[3] But customers insist on such assurances and are requesting ever more demanding service-level agreements (SLA). The issues for SaaS providers are:

- Most SaaS developers have done a superb job of ensuring onsite security of data in a multi-tenancy environment. Once the customer's data arrives at the SaaS server, it is protected. However, data in transit and data at the edge of the enterprise are not so easily protected.
- Even with lightweight web-based applications, SaaS performance can grind to a halt when confronted with unpredictable WAN congestion. Traditional WAN optimization strategies are not an option, as the SaaS developer has no control over customer infrastructure equipment.

2 Ibid.

3 Messina, David, "Troubleshooting SaaS Performance." IT World, September 2008.
http://www.itworld.com/saas/55271/troubleshooting-saas-performance-issues

For these reasons, SLAs are difficult to consistently implement with any degree of certainty.

Therefore, SaaS developers and providers are in the unenviable position of having few options for addressing two of the chief customer objections to wide-scale adoption of SaaS products, often jeopardizing compliance with SLAs.

Additionally, if confronted by performance issues while using a SaaS application, the customer's own IT staff will inevitably receive the initial deluge of help desk calls from its users, not the SaaS provider. This may further alienate the SaaS customer as support cost savings was one of the chief reasons for deploying SaaS.

Data security and reliability requirements

To reliably deliver on SLAs and to truly provide consistent performance to customers, SaaS companies need flexible solutions that fit the widest possible range of computing environments. In addition, these WAN security and performance products should not disrupt customers' existing networks nor should they require customers to change or add expensive hardware or software components. Ideally, the security and performance of the WAN links to customers should be centrally managed and monitored. Finally, these WAN products must be as "set and forget" as possible. The service provider is in the business of delivering business applications, not full-time WAN optimization platforms.

The Circadence® SaaS solution

Founded in 1993, Circadence focuses on developing products for WAN security and performance. The Circadence MVO™ 1200 WAN Optimization suite, the core of the company's technology, can be deployed in software, hardware, and integrated application configurations. The Circadence MVO 1200 WAN Optimization suite delivers optimal bandwidth, resilient WAN connections, and U.S. Department of Defense (DoD)-grade security as a foundation for delivering SaaS applications. The Circadence MVO 1200 WAN Optimization suite provides a flexible solution for both reliable performance and the highest level of security.

The technology used in the Circadence MVO 1200 WAN Optimization suite is Circadence's patented optimization protocol. The algorithms in Circadence's protocol offer the dual functions of providing accelerated and uninterrupted WAN connections. In addition, Circadence has worked closely with government and defense clients to incorporate sophisticated security features into its optimization protocol. Therefore, data is secured throughout its WAN route – from customer to SaaS application.

Circadence performance

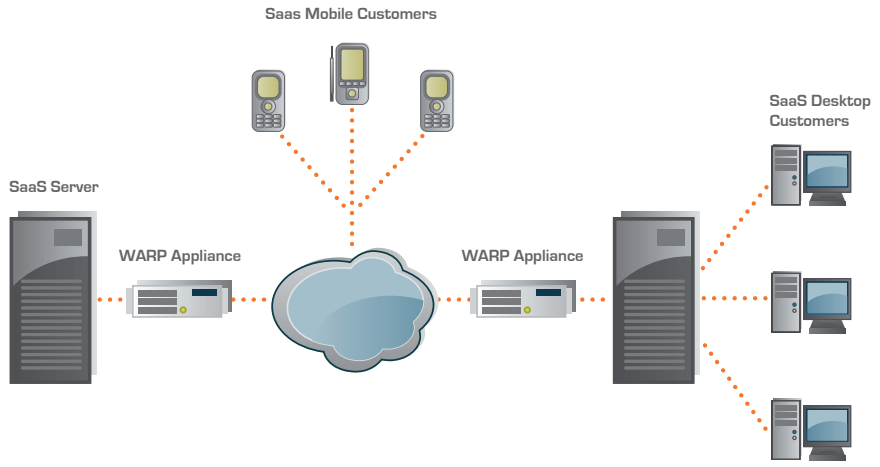
In independent tests, a leading enterprise application developer recently quantified throughput gains when using Circadence MVO products with mobile and wireless laptop devices. Using a mobile field service test scenario, the vendor ran a suite of field service applications over standard and Circadence MVO-enabled wireless connections. The application test bed performed a new customer service request, a service request update, and four other field application operations. To simulate real-world network traffic conditions, the test bed also introduced network congestion to simulate zero to moderate (50-percent) to high (95-percent) network utilization. The results were consistent. Throughput using Circadence MVO was double that of a standard connection in a zero network utilization environment. When operating in a moderately congested environment, Circadence MVO performance was 108-percent better than a standard wireless

connection. Even in highly congested simulations, Circadence MVO-enabled connections provided 110-percent higher throughput than a standard wireless network.

Point-to-point security and resilience

Circadence has a long history of working with the most demanding security-conscious customers. The algorithms deployed in the Circadence protocol meet or exceed the standards of the DoD for providing secure connections. The Circadence MVO Appliance is certified for use at classified government installations. In addition, Circadence MVO connections are secured from point-to-point, unlike SSL security that is shed at the gateway server decryption point. SaaS applications can use SSL, however, in conjunction with the Circadence MVO 1200 WAN Optimization suite to provide an even greater layer of protection. Tests confirm that no degradation in acceleration occurs when SSL is used in tandem with the Circadence MVO 1200 WAN Optimization suite.

Figure 1



The Circadence MVO 1200 WAN Optimization suite also includes Link Resilience™, a method of maintaining connectivity over severely degraded or interrupted connections. With Link Resilience, SaaS applications can continue functioning across cellular and wireless network handoffs, and even transparently maintain viability during interruptions of service on public networks. This feature provides a high level of data integrity and application stability.

Flexible and lightweight SaaS solutions

While Circadence MVO products come in a variety of hardware and software solutions, the most unobtrusive and easiest to implement for SaaS customers is the Circadence MVO Windows Client. Requiring less than 1 MB of disk space and less than 200 KB of memory, the Circadence MVO Windows Client uses Circadence's protocol to open a fully optimized and secure tunnel from the customer's desktop to the SaaS provider's central site. No configuration is necessary, and the software is transparent to the user. Because all Circadence MVO products work seamlessly with one another, Circadence MVO Windows Client software can communicate with a variety of Circadence products hosted at the SaaS application site, including a directly embedded link to the SaaS application by

using the Circadence MVO Software suite. Installation of the Circadence MVO Windows Client can be a transparent part of the client's subscription to the SaaS application.

To accelerate and secure WAN connections for SaaS applications, the Circadence MVO 1200 WAN Optimization suite includes:

- **Circadence MVO Windows Client** – Operating as agent software on a Windows PC or server, this Circadence MVO client can connect to any other Circadence MVO component. The software requires slim resources and is transparent to the user. It can be installed on the desktop or laptop of any SaaS application customer during subscription, transparently providing security and reliability.
- **Circadence MVO Software suite** – This software package supports Windows and Linux, and is portable to almost any POSIX-compliant operating system. This software-only solution can be installed on a variety of SaaS application servers, regardless of operating system, to provide consistent security and reliable performance.
- **Circadence MVO Appliance** – This hardware solution not only centralizes Circadence MVO connections, but also ensures survivability during denial-of-service attacks. The Circadence MVO Appliance is DoD-certified for classified installations. It may provide a perfect gateway at the SaaS site to connect to SaaS customers.
- **Virtual Circadence MVO** – This solution provides support for Oracle VM, VMware, Microsoft Virtual Server, Xen, and other virtualization solutions, and can serve as a virtual gateway.
- **Circadence MVO Mobile** – Circadence MVO optimization is available for Windows Mobile, Symbian, and Mobile Linux devices on secure digital (SD), USB, and compact flash (CF) cards. SaaS applications for mobile workforces can be securely delivered and reliably connected. [See the Circadence white paper "Improving WAN Connections for Mobile Workers " for more information.]

Centralized management of SaaS performance and security

Because all Circadence MVO products work together, regardless of configuration or location, one central web-based interface at the SaaS service provider site can be used to configure parameters, monitor performance, and set priorities for all Circadence MVO components. The Circadence MVO 1200 WAN Optimization suite provides device and environment-independent Quality of Service (QoS) guarantees, so desktop agents, virtual machines, or the Circadence MVO Appliance can all address priorities from one interface. Legacy systems of SaaS customers can be upgraded to QoS without being replaced or disrupting existing networks. Because Circadence MVO products use Circadence's patented optimization protocol, DoD-grade security is built into every Circadence MVO connection, regardless of the endpoint in the customer network – from the provider's SaaS server to a customer's desktop or PDA. Installing or monitoring additional software for WAN connections is not needed, and the security is identical throughout the Circadence MVO environment, making uniform SLA criteria a reality.

Conclusion

Potential and current SaaS customers are primarily concerned with security, control, and reliable performance when selecting SaaS applications. These issues, in fact, are the primary reasons for SLA contracts. However, many of the technical factors that affect security and performance over the public portions of the WAN are beyond the direct control of either the customers or service providers. Circadence offers a solution that is unobtrusive and transparent to SaaS customers, yet provides highly secure and highly reliable WAN connections.

About Circadence

Since 1993, Circadence has leveraged the power of advanced technologies to pioneer smarter, faster, and more cost-effective solutions for improving IT performance. What started with an innovative platform for making massively multiplayer online games run faster has quickly grown into the most capable suite of optimization solutions available. Based in Boulder, Colorado, Circadence continues to expand today's possibilities with tomorrow's technologies – addressing new, growing concerns with dynamic, high-performance solutions. Only Circadence offers the most capable IT innovation solutions available – proven to outperform some of the world's most demanding challenges. For more information on Circadence, visit www.circadence.com.

References

Gillan, Paul "CIOs slowly embrace SaaS." SearchCIO.com, November 2006. http://searchcio.techtarget.com/news/column/0,294698,sid182_gci1229107,00.html#

Gartner, "SaaS increasing in large enterprises." November 2006. http://blogs.gartner.com/jim_holincheck/2006/11/29/saas-usage-increasing-in-large-enterprises-not-new-news/