Securing Cloud Computing for Enterprise Collaboration

As the business case for Software-as-a-Service (SaaS) and other cloud computing models solidifies, more and more companies are incorporating cloud computing into their IT programs. The implication is that an ever-increasing amount of critical information is living "in the cloud."

Delegating services to a service provider, and turning to SaaS solutions in the cloud, does not absolve users from legal, ethical or regulatory requirements to maintain data security, especially where customer or account information is concerned. Therefore, when evaluating and choosing a SaaS provider, security must be at the top of the list. This paper explores the state of security in the cloud and what to look for from vendors, particularly when considering SaaS document management and collaboration vendors.

Cloud computing is completely outsourced yet highly affordable, flexible and secure. By moving to a cloud computing environment, organizations can leverage better economies of scale.

INTRALINKS®

1 866 INTRALINKS

New York + 1 212 342 7684
London + 44 (0) 20 7060 0660
Hong Kong + 852 3101 7022

www.intralinks.com

The Benefits of Cloud Computing

Cloud computing has become a genuine and powerful computing phenomenon:

- **Completely outsourced:** Customers buy licenses and provide their users with Internet access; service providers do the rest, including acquiring, implementing and maintaining infrastructure and computing platforms, services and software. ***Summary: Let the provider do it.***
- **Highly affordable:** Costs are often lower than those for stand-alone software, and can be charged as recurring overhead expenses rather than as capital expenditures. This also helps smooth out cash flow, which translates to a more predictable series of monthly bills for services consumed. ***Summary: Overall lower, more manageable costs with business-friendly accounting.***
- **Secure:** Cloud vendors have a sharper focus on their applications and infrastructure. They normally have better security practices tailored towards protecting their infrastructure, application and customer data. ***Summary: Specialized vendors do security right.***
- **Extremely flexible and agile:** Organizations can use as much or as little cloud computing as needed. Working with the right service provider, an organization can reinvent and reprovision its technology infrastructure quickly and inexpensively. The cloud also makes location irrelevant, enabling workers to get their jobs done where it makes the most business sense. ***Summary: More seats when and where you need them, fewer seats when you don't; change your environment on demand.***
- **Scalabilty:** Multi-tenancy lets service providers scale much broader and deeper than even the largest organizations need. Providers can situate centralized infrastructures in low-cost locations, and create environments designed to handle aggregate peak demands that easily accommodate peak demands for individual organizations. ***Summary: Flexible scale produces better economy and a lighter environmental footprint.***

State-of-the-Art Security for Cloud Computing

When it comes to security for any kind of information, best practices dictate that it should be protected at all times, and from all possible avenues of attack. The best security practitioners address four primary areas of concern — application, infrastructure, process and personnel security — each of which is subject to its own security regime.

The Four Pillars of Information Security must lock together to define appropriate protection and controls.

Application Security

When users access SaaS services in the cloud, the need for security kicks in as soon as that activity begins. The best SaaS providers protect their offerings with strong authentication and equally potent authorization systems. Authentication ensures that only those with valid user credentials obtain access, while authorization controls what services and data items individual valid users may access.

As information or services are made available, administrators decide which users are permitted to see and update them. Real-time reports and user activity audits also must be invoked to keep track of who's looking at what, when and which changes have been made. Additional controls should be available to determine who can print, copy or forward materials, and prevent such activity unless it is specifically authorized even after documents leave the enterprise perimeter. Robust watermarking features are often provided to ensure that materials cannot be reproduced or disseminated without permission. Finally, all application-level access should be protected using strong encryption to prevent unauthorized sniffing or snooping of online activities. Cryptography must be used to protect customer data in transit, at all times. Further, a Security Development Lifecycle (SDL) process should be followed when developing and deploying the application.

Infrastructure Security

Cloud services are only as good as their availability. Providers must build a highly available redundant infrastructure to provide uninterruptible services to their customers. If the SaaS provider does not host its services and data itself, it must choose highly reliable and professional partners. A SaaS provider or

partner should use real-time replication, multiple connections, alternate power sources and state-of-the-art emergency response systems to provide complete and thorough data protection. Network and periphery security are paramount for infrastructure elements; therefore, leading-edge technologies for firewalls, load balancers and intrusion detection/prevention should be in place and continuously monitored by experienced security personnel.

Process Security

SaaS providers, particularly those involved in business critical information, invest large amounts of time and resources into developing security procedures and controls for every aspect of their service offerings. Truly qualified SaaS providers will indicate that they have earned SAS 70 Type II certification from the American Institute of Certified Public Accountants (AICPA), or have enacted measures to keep their clients in compliance with appropriate regulations (e.g., the U.S. Food and Drug Administration (FDA) 21 CFR 11 regulations for the Pharmaceutical industry). ISO 27001 certification is a good measure of risk management strategies employed by the provider. These certifications ensure thorough outside reviews of security policies and procedures. Formal reports about such reviews and testing should also be made available upon request.

Personnel Security

People are an important component of any information system. They can present insider threats that no outside attacker can match. Administrative controls such as "need to know", "least privilege" and "separation of duties" must be employed. Background checks of the employees and enforceable confidentiality agreements are mandatory.

Ideally, employees with access to sensitive information will be tested, and possibly even certified, before interacting with clients. In addition, the best SaaS providers ensure their employees keep current by providing ongoing training and certification retesting to verify that skills and knowledge remain at an appropriate level.

SaaS Security Can Beat Enterprise Security

Maintaining security standards for the enterprise is expensive and time consuming for every IT department. IT resources are typically stretched thin and keeping current can be a challenge. SaaS providers offer a number of advantages including:

- **Faster response to threats:** Security enhancements and vendor patches are instantaneously available to all users as there is no need to patch every PC on the internal network.
- **Sharper focus:** SaaS providers have homogeneous environments and a smaller vulnerability surface to secure, which is often not the case with enterprise environments.
- **Network effect:** SaaS providers go through many more vigorous security checks than is possible in traditional Corporate IT departments due to limited resources and time.

Arguably, the burden of security responsibility is even heavier for service providers whose customers demand that they satisfy numerous security requirements, standards and criteria than it is for individual enterprises. This goes a long way toward explaining why SaaS providers' security capabilities often exceed those in many enterprises.

A provider that has designed and implemented a thorough security approach will be able to articulate how it addresses the following:

- **Holistic, 360-degree security:** Providers must adhere to the most stringent of industry security standards, and meet client expectations, regulatory requirements and prevailing best practices. This includes coverage of application, infrastructure, personnel and process security.
- **Complete security cycle:** A competent SaaS provider understands that implementing security involves more than technology — it requires a complete lifecycle approach. Providers should offer a comprehensive approach to training, implementation and auditing/testing.

Your SaaS provider should be willing to provide access to auditors and ethical hackers to perform security assessments of the infrastructure and applications.

"Many factors are driving adoption of SaaS, including the benefits of rapid deployment and rapid ROI, less upfront capital investment, and a decreased reliance on limited implementation resources… Many enterprises are further encouraged by the fact that with SaaS, responsibility for continuous operation, back-ups, updates and infrastructure maintenance shifts risk and resource requirements from internal IT vendors or service providers."

— Gartner Inc.[1]

- **Proactive security awareness and coverage:** The best SaaS providers understand that security is best maintained through constant monitoring, and by close attention to current trends and developments on the threat landscape. They can recognize various types of threats, and take swift, decisive steps to limit potential exposures to risks.
- **Defense-in-depth strategy:** Traditional discussions on this topic usually turn to medieval castles to illustrate how combining a moat, high outer walls, limited access ports (drawbridge) and an inner keep (castle within a castle) made storming such structures so difficult. In a similar way, multiple layers of security protection can interlock to protect sensitive data and assets more effectively than a single, large security implementation. Savvy SaaS vendors understand the value of defense in depth, and can explain how they use this strategy on your behalf.
- **24/7 customer support:** Just as the cloud knows no east or west (it's indifferent to location), it also knows no day or night (the Internet makes the notion of normal working hours irrelevant). Service providers should offer around-the-clock support and assistance to help users deal with software and services, and provide zero-hour responses to security threats. The best service providers operate support and incident response teams at all times.

Tips for Obtaining Information from Service Providers

When comparing SaaS providers, it is essential to check their ability to deliver on their promises. All SaaS providers promise to provide excellent security, but only through discussions with existing customers, access to the public record and inspection of audit and incident reports can the best providers be distinguished from run-of-the-mill counterparts. Part of this evaluation should include consideration of the provider's existing client base and where they set the bar for security. This can be a good gauge for the strength of a provider's claims. Providers serving financial services, life sciences and government clients must adhere to higher standards than those working predominantly with other industries.

The same is true when it comes to assessing a provider's service and software reliability and availability. Service level agreements (SLAs) should clearly spell out terms and conditions related to uptime, availability and response times. In addition, contacting a random list of SaaS customers to see how well each provider has met its SLAs in the past can help you narrow your list of candidates.

Ideally, obtaining information about security from providers should require little or no effort from prospective buyers. The providers who understand security — particularly those providers for whom security is a primary focus or a key ingredient in effective service delivery — will provide detailed security information as a matter of course, if not a matter of pride. Providers who understand the shared responsibility for data integrity, privacy and confidentiality that they must carry on behalf of their clients also know they must communicate clearly and directly, and, in many cases, provide new insights and thought leadership based on their experience across a wide range of customers and industries.

Further, a security-savvy SaaS provider can deliver tremendous value-adds to its clients. Such providers can enable effective collaboration among colleagues and co-workers, and even among teams assembled across multiple organizations, thanks to easy and secure tools for information sharing and exchange. With the right security apparatus built in, providers can impose highly effective security restraints on SaaS offerings. Likewise, such providers can also ensure that their clients comply with rules and regulations, and employ due diligence in meeting best industry practices and procedures for protecting privacy and confidentiality.

A Checklist of Leading-Edge Security Practices for Protecting Critical Information

Moving to the cloud does not eliminate the three security objectives that IT managers have for the in-house world: *confidentiality, integrity* and *availability*. It is this security triad that provides a good foundation for a checklist of what to ask your provider, and yourself. This section reviews key security practices that differentiate leading SaaS providers who provide enterprise-grade services.

[1] Gartner Inc., "Market Trends: Software as a Service, Worldwide, 2008-2013" by Sharon A. Mertz, Chad Eschinger, Tom Eid, Hai Hong Huang, Chris Pang, Ben Pring, May 2009.

Confidentiality

User Authentication

Q: How are users authenticating to the application?

A: The most common way is to require a user ID and password, but the key is password strength. Does the provider require a password with a minimum length and use of various character sets, or a long password without complexity (such as a phrase that's easily remembered)? Also recommended is that the provider enforces one authentication per session.

Q: Is two-factor authentication available?

A: This is recommended because passwords are not always strong enough to protect certain sensitive information. For example, the Federal Financial Institutions Examination Council (FFIEC, an inter-agency body representing five security agencies) requires online banks to use two-factor authentication. Information must be segmented and protected by various user access levels.

Security Triangle

Data Protection

User Roles

Q: Are separate user roles supported?

A: The vendor should support the use of separate roles for users — not every user should have access to everything. Assignment of resource-level permissions ensures that administrators, owners and users are granted only as much access as they need.

Q: How granular are the permissions to applications feature/functions?

A: A good application will not extend higher levels of access or privilege to users than they need to do their jobs (principle of least privilege). Every type of access to every resource in the application needs to be specifically assigned — by person or role. Otherwise, permissions become hard to track.

Data Separation and Classification

Q: Is it possible to segment data by its sensitivity?

A: Military and government applications as well as some corporations require this separation. The way the application handles data should make it possible to map to your enterprise's data classification schemes so you can group them and grant access accordingly.

Q: Is elevated authentication available to access sensitive data?

A: The application should provide for appropriate authentication based on data classification — different types of data require different access levels.

Personnel

Q: Are background checks performed on personnel?

A: Understand the vendor's background check policy and map it to your own organization's policy at the highest levels.

Q: Are confidentiality agreements mandatory?

A: You may want to ask for a copy and/or have a trusted third party verify the agreements.

Q: How does the provider control security risks presented by third-party software?

A: The provider should follow closely what patches are released. Ideally, it also should use vulnerability reporting services.

Cryptography and Encryption

Q: Is cryptography used to protect customer data?

A: Insist that your data be protected at all times. Don't allow a vendor's concerns about negative impact on performance be an excuse for insufficient encryption. You should have a clear idea of how information is protected both at the vendor server site (at rest), in transit (upload/download) and in use (when you open applications to view documents).

Q: How does the vendor retire outdated encryption algorithms and implement new ones?

A: Your vendor is responsible for updating algorithms appropriately. Ask for a standard battery of

A SaaS provider that specializes in security is at the pinnacle of a demanding area of technical and professional expertise.

tests and security checks to ensure that application processing routines are not disrupted or negatively impacted by algorithm changes.

Q: How does the vendor manage encryption keys?

A: Key management is the most important part of cryptography. Understand how the keys are generated, stored and renewed. Best practices mandate tiered keys (where a master key is used to protect data keys). Each file will have a unique data key generated by the system.

Integrity

Q: Is document watermarking available?

A: Because technology makes it easy to capture screens and share information instantly, a watermark is an important part of protecting yourself legally.

Q: How is protection for " in-use" data implemented?

A: Data should be protected while in use by Information Rights Management (IRM). Your provider should support IRM for a wide variety of file formats, such as Adobe PDFs and Microsoft® Office. By protecting a wide array of file formats, you won't have to continually convert to PDF or some other format.

Q: Is user activity related to data manipulation audited?

A: You should know who accesses data and when — and not just the last time, but every time. Are vendor reports accessed easily through the application or do you have to call customer support?

Q: Is privilege authorization audited?

A: You should be able to determine who assigned the privilege to the user, not just who accessed the document. This becomes especially important in litigation, leak investigations and post-transaction reviews.

Q: Are reports available that show the history of data within the application?

A: The vendor should be able to tell you when the file was uploaded/updated and be able to easily provide this information as a real-time dashboard or interface, rather than having customer service pull reports on request.

Q: Are reports available that track changes to the application environment and setup?

A: Verify that the vendor tracks changes to the application environment and setup, and has a change control process in place. This way it knows why something worked yesterday, but not today.

Availability

Q: Does a disaster recovery site exist for the data center?

A: Make sure the vendor has a disaster recovery site, as up-time is a critical consideration for most SaaS users.

Q: Does a data center disaster recovery plan exist?

A: How often is the plan tested? The vendor should have clearly written disaster recovery procedures and a current checklist. The plan must be tested regularly as people and hardware change over time.

Q: Is it a warm or cold site?

A: How often is the secondary site tested? Warm sites should be tested at least twice a year; cold sites should be visited and/or reviewed on the same schedule.

Q: How far apart are the primary and secondary sites?

A: According to The National Institute of Standards, a minimum of 300 miles of separation is recommended. The sites should use separate power grids, water supplies, telecommunications providers and major roadways.

Q: How is the back-up implemented?

A: Regardless of whether back-ups go to tape, disk or into a storage server across the network, they must meet your data coverage and retention needs. Ideally, back-ups cover at least the last 30 days of activity.

Q: How does performance testing and capacity planning take place?
A: This is a key component to any high-quality vendor. Ordinarily, a company has an internal team that monitors this exclusively and takes action proactively.

Q: How are Internet latency issues for global customers resolved?
A: If you have a global user base, make sure the vendor provides appropriate performance no matter where people are located.

Q: How are web resources protected from denial of service (DoS) attacks?
A: Verify that the vendor monitors your web presence continuously and is able to take proactive action against DoS attacks.

Q: How is the application source code maintained and protected?
A: Multiple development teams — including those offshore — may contribute to the source code. Therefore, the vendor should have procedures in place that ensure only the authorized code makes its way into the final build.

Q: How do software upgrades and patches get promoted to the production environment?
A: Verify that only authorized patches get deployed to production. Procedures and controls are key to ensuring the appropriate approvals are in place before updates are rolled out to production.

Conclusion

Highly affordable, flexible and secure, cloud computing allows organizations to leverage better economies of scale. As a result, an increasing number of companies are incorporating cloud computing into their IT programs.

When it comes to security for SaaS models like cloud computing, it should be protected at all times using a comprehensive approach, which includes application, infrastructure, process and personnel security. As such, when evaluating and choosing a SaaS provider, it is important to verify that the provider can deliver the level of service and capabilities your company requires.

About the Authors

John Landy

Chief Technology Officer

John Landy is Chief Technology Officer at IntraLinks, where he is responsible for advancing the architecture and performance of the IntraLinks SaaS platform, while maintaining the strict security requirements necessary for critical information exchange. He brings more than 17 years of leadership experience in architecture and technology to IntraLinks, with a focus on SaaS solutions and distributed systems.

Prior to joining IntraLinks, Landy held technology leadership positions at both software and financial services firms including, JPMorgan, Kronos, Workscape and Fidelity Investments.

He received his B.S. in computer science from Lehigh University, M.S. in computer science from Villanova University and MBA from Babson College.

Mushegh Hakhinian, CISSP

Security Architect

Mushegh Hakhinian leads the application security practice at IntraLinks. A veteran in the technology industry, he has been managing security initiatives for the past 16 years.

Prior to joining IntraLinks, Hakhinian worked at an online banking software company managing application development security lifecycle, application security features and relationships with customers' security departments and internal operations security teams. Previously, he worked at Central Bank of Armenia as the head of the Electronic Security department.

Hakhinian received his B.S. in Computer Science from Yerevan Polytechnic Institute in Yerevan, Armenia (Magna Cum Laude). He is an active member of OWASP Boston Chapter.

About IntraLinks

For more than a decade, IntraLinks' enterprise-wide solutions have been facilitating the secure, compliant and auditable exchange of critical information, collaboration and workflow management inside and outside the enterprise. Our SaaS-based solutions adhere to industry-mandated regulatory requirements, including SAS-70 Level II and ISO 9000 certifications. More than 800,000 users across 90,000 organizations around the world rely on IntraLinks including, 50 of the 50 top global banks, 10 of the top 10 life sciences companies, 25 of the top 25 law firms, and 14 of the 15 largest private equity firms.

To learn how IntraLinks can transform your business, visit **www.intralinks.com** or contact us at:

Tel: 1-866-INTRALINKS (US),
Tel: +44 (0) 20 7549 5200 (EMEA)
Tel: +852 3101 7022 (APAC)
info@intralinks.com

Terms of Use

Although IntraLinks has made every effort to provide accurate information in this document, IntraLinks makes no representations as to, and does not warrant, the accuracy and/or completeness of the information herein or its suitability for any particular purpose. The reader assumes all risk and responsibility for his or her reliance on, or use of, any of the material contained in this document.

ALL INFORMATION IS PRESENTED "AS-IS," AND INTRALINKS DISCLAIMS ALL EXPRESS OR IMPLIED WARRANTIES AND CONDITIONS WITH REGARD TO THE INFORMATION, INCLUDING THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT. IN NO EVENT SHALL INTRALINKS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST REVENUES OR LOST PROFITS, THAT MAY RESULT FROM THE USE OF THIS DOCUMENT.

1 866 INTRALINKS

New York + 1 212 342 7684
London + 44 (0) 20 7060 0660
Hong Kong + 852 3101 7022

www.intralinks.com