computer FRAUD & SECURITY

ISSN 1361-3723 August 2012 www.computerfraudandsecurity.com

Featured in this issue:

The cloud challenge: realising the benefits without increasing risk

The obvious benefits of cloud computing, coupled with rapid advancements in enterprise mobility, have led to the widespread adoption of browser-based applications in the enterprise, with or without the knowledge of the IT department.

However, this encroachment on traditional application delivery has led to enterprise security being downgraded to a 'one size fits all' model that robs CISOs of the granularity required to comply with regulations governing data protection, privacy and corporate governance. Richard Walters of SaaSID examines how to extend corporate policies to maintain security and compliance.

Full story on page 5…

Online privacy: a matter of policy?

Privacy policies are a standard element of most online sites, but can differ markedly in the degree to which they are understandable to users, thanks to the volume of information and the complexity of the language used.

Steven Furnell and Andy Phippen of Plymouth University, UK examine the policies of some leading sites and assess the implications for users. They also consider other ways in which users may tend to seek reassurance if understanding the policy is beyond their ability.

Full story on page 12…

Towards 'social' security

Social networking is a common Catch-22 for businesses – allow access to social media sites and the business is opened up to malicious content, phishing schemes and other evils. Declare all social media sites off-limits and employees become frustrated, find workarounds or work elsewhere.

The key is to achieve a safe compromise – through an acceptable-use policy tailored to each specific organisation's risk profile, and enforced through next-generation technologies. Clearly documenting ground rules, expectations and repercussions for out-of-policy behaviour will ensure that end users are aware of what's considered acceptable use of social vehicles, explains Chris Jenkins of Dimension Data.

Full story on page 18…

Europol to lead anti-cybercrime alliance

European law enforcement organisation Europol is taking the lead role as part of the International Cyber Security Protection Alliance (ICSPA) in a new consultation process designed to help governments, law enforcement agencies and businesses combat cybercrime. Project 2020 will analyse current trends in cybercrime and how they may evolve over the next eight years and beyond

Continued on page 3…

Contents

NEWS

FEATURES

REGULARS

Visit us online at:
www.computerfraudandsecurity.com

The cloud challenge: realising the benefits without increasing risk

Richard Walters

Richard Walters, SaaSID

Public cloud services are moving into the enterprise through the increasing use of employee-owned devices, either as part of formal Bring Your Own Device (BYOD) policies or informally as a result of employees adopting their own web-based applications on corporate devices. In March 2012, Ovum analyst Samok Roy drew attention to the Bring Your Own Software (BYOS) issue, where employees use applications based on public cloud services to process corporate data – often without the knowledge of the IT team. Roy asserted that the ungoverned use of 'freemium' apps, or public cloud services, posed as great a risk to data and corporate compliance as the well-documented BYOD risk.

Roy wrote: "BYOS tools cannot be accessible to groups that handle information protected by regulations, and such groups need to be educated that use of such tools is unacceptable. Also, the risk that the combination of BYOS and employee-owned devices poses to data security norms should force corporate IT to re-evaluate removable storage device policies and data access policies in general."[1]

What is significant is that, globally, Software as a Service (SaaS) is expected to grow five times faster than traditional packaged software, which is seeing declining revenues. IT analyst firm IDC predicts that, by 2014, about 34% of all new business software purchases will be delivered via SaaS, the SaaS segment will be worth $40.5bn and 65% of new products from established software vendors will be delivered as SaaS.[2] Two things are certain: web-based applications are not going away; and CIOs, CISOs and risk and compliance managers need to address how they will enable SaaS, while still controlling access to data and auditing application use.

Corporate data that is accessed via web-based applications is prone to the same insider threats and computer fraud as traditional corporate applications. The browser is simply the new endpoint. Therefore, it needs to be managed and audited in the same way as traditional corporate computing devices.

So let's look at the current status of enterprise security and compliance as SaaS, BYOD and BYOS gain momentum. We will assess the benefits and suggest a means of encompassing these new models of application consumption into enterprise security policies, without risking non-compliance with regulations covering data privacy and corporate governance.

The traditional approach to security

Figure 1 shows the traditional layered approached to enterprise security. While some of these layers still apply to web-based applications, most do not, particularly in the public cloud. Our concern here is with the extension of application-layer security, content security, file integrity and database security to SaaS applications,

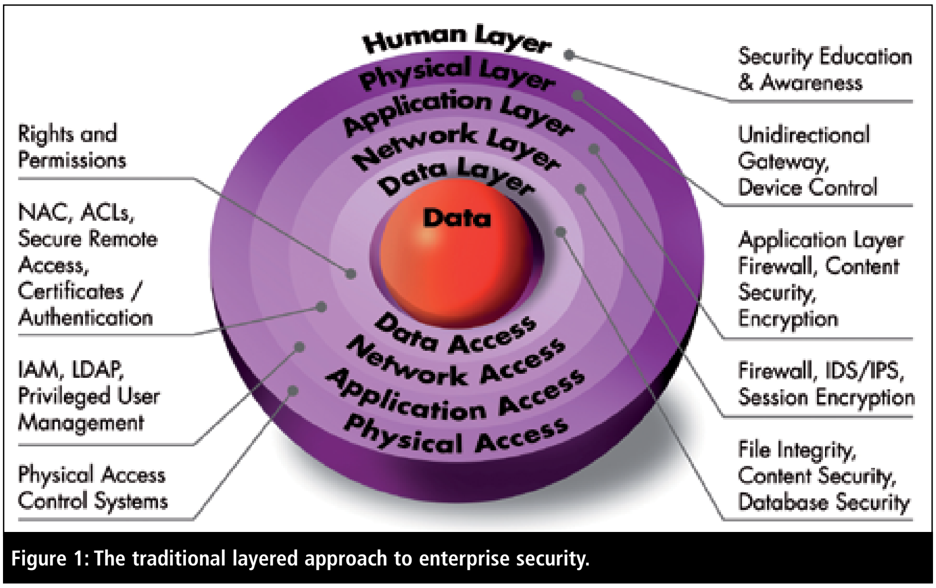
Human Layer
Physical Layer
Application Layer
Network Layer
Data Layer
Data
Data Access
Network Access
Application Access
Physical Access
Rights and Permissions
NAC, ACLs, Secure Remote Access, Certificates / Authentication
IAM, LDAP, Privileged User Management
Physical Access Control Systems
Security Education & Awareness
Unidirectional Gateway, Device Control
Application Layer Firewall, Content Security, Encryption
Firewall, IDS/IPS, Session Encryption
File Integrity, Content Security, Database Security

Figure 1: The traditional layered approach to enterprise security.

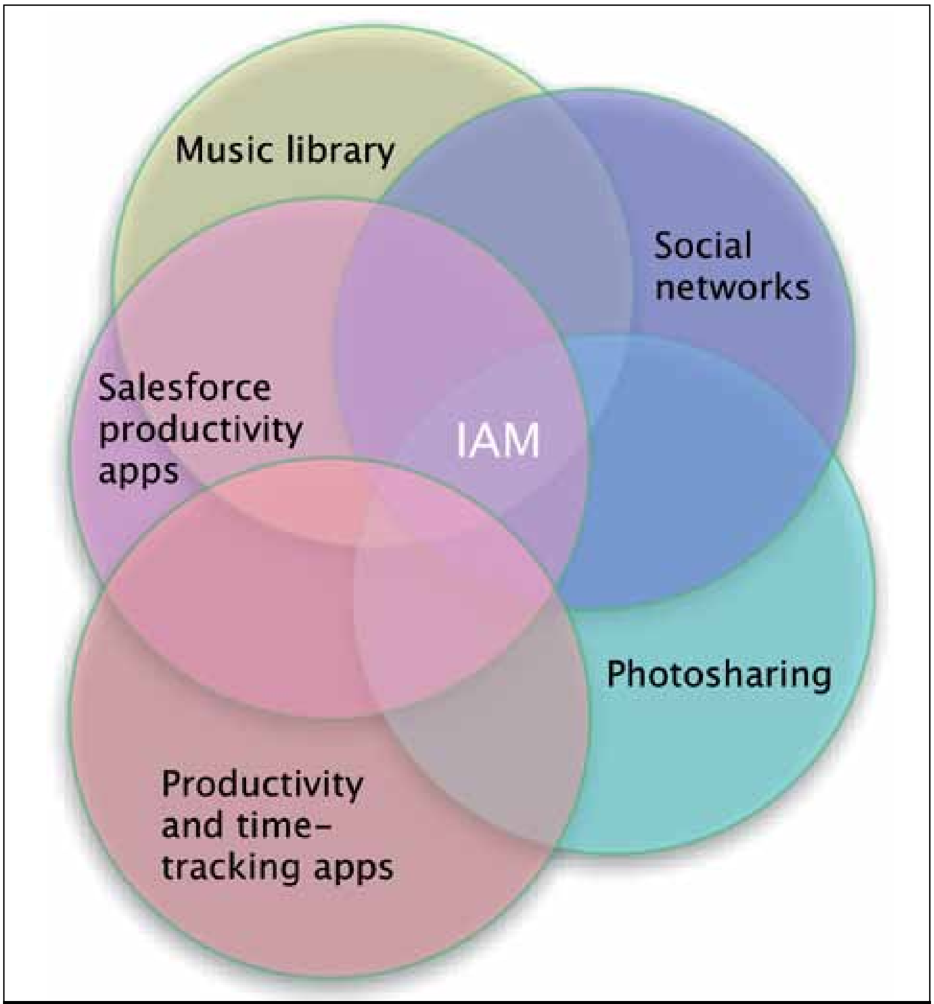
Music library
Social networks
Salesforce productivity apps
IAM
Photosharing
Productivity and time-tracking apps

Figure 2: The 'cloud' is actually a collection of personal computing technologies used by the individual for business and leisure.

through the enablement of rights and permissions, authentication, Identity and Access Management (IAM), Lightweight Directory Access Protocol (LDAP) and privileged user management and auditing on the browser.

"If the browser is tightly locked down and web application access and activity can be managed and audited, then employees can be given much wider freedom"

In many respects, the cloud is simply using the Internet as a computing platform. It's a new way of delivering computing power on a utility basis. The browser is the new interface between the user and corporate data. Therefore, managing access to browser-based applications, gaining more granular control and visibility and auditing users' activity while using those applications, are the new challenges facing CISOs and risk and compliance officers.

Evolution of the endpoint

As discussed, the endpoint is no longer a fixed desktop or notebook PC, it could just as easily be a smartphone, tablet, set-top box, digital TV, games console or in-car system. The 'iGeneration', in particular, is not as fixated on a particular device, but on whether a browser is available. 'Work' is an activity not a place. Embedding enterprise-class security within the browser has significant benefits. It enables organisations to introduce flexible BYOD schemes and embrace the use of personal computing services for business purposes, with the attendant availability and productivity benefits. If the browser is tightly locked down and web application access and activity can be managed and audited, then employees can be given much wider freedom over the device they choose, regardless of whether it is owned by, or even known to, the enterprise.

The consumer cloud

In a recent conversation with the head of security for a major global bank it was estimated that 65% of staff have a personal Dropbox, Google Drive, Microsoft SkyDrive, Apple iCloud or other personal cloud storage account. Another CISO said that he had discovered more than 30 instances of Salesforce.com being used in his FSA-regulated organisation, none of which were connected or audited. A global study undertaken by Avanade (www.avanade.com) in 2011, found that 60% of executives were concerned by this unregulated use of public cloud services within their organisations, dubbed 'Cloud sprawl'. A fifth of these executives believed that it was impossible to manage all of the different cloud services being used within organisations.[3]

"Functional and organisational roles for who has access to data must be determined before a BYOD policy can be established"

However, a more recent consumerisation of IT study, conducted for Avanade by Wakefield Research in October 2011, surveyed more than 600 C-level executives and IT staff in 17 countries and found that 88% were using personal computing technologies for business purposes.[4] This latter survey found that organisations are embracing the adoption of cloud services because it allows employees to work anywhere. It also cited the fact that employees using these browser-based applications were more willing to work after hours: as we have stated, work is an activity not a place. Lian-James analyst Martin Banks also believes that the 'Cloud' is in fact a collection of personal clouds. An individual appears in the intersection of the Venn diagram of business, consumer, sport, entertainment and social network clouds. Gartner research director Michael Gartenberg predicts that, by 2014, this personal cloud will overtake the PC as the centre of people's digital lives. [5]

I browse, therefore IAM

IT teams need to accept that the consumer cloud has come into the enterprise environment, along with the use of personal devices. To ensure risk management and compliance, IT must embrace the use of these services and provide equivalent secure alternatives.

Enterprise IAM expert Randall Gamby, writing on the integration of Mobile Device Management (MDM) into enterprise identity and access management programmes to facilitate BYOD, states: "Functional and organisational roles for who has access to data must be determined before a BYOD policy can be established. Often this is based on the value or sensitivity of the data. MDM tie-ins into the enterprise LDAP or roles-based directory can make this task easier."[6]

We can draw the same conclusions from SaaS applications, whether they are introduced to the enterprise environment via BYOS, or the enterprise app store. Gamby asserts that: "Mobile credentials should be of the same type and level of security as any other corporate device. Tying the MDM into the corporate authentication directory, like Active Directory, can leverage existing credentials and even supply single sign-on capabilities."

Access control: the case for single sign-on

As more applications are accessed via the browser, the issue of password security becomes increasingly pressing. Recent password database hacks have served as a reminder of the risks that consumerisation of IT poses to the data and assets stored within the corporate IT environment. Too often, people use weak, easily cracked passwords for social networking applications, which they proceed to reuse across multiple SaaS applications.

The HBGary hack demonstrated the risk posed by password reuse. This was a determined and multi-layered attack, starting with an SQL injection attack on the password and username database of partner company, HBGary Federal. However, one of the factors that increased the company's vulnerability was the CEO's reuse of the same login details for his corporate email, a support server and his Twitter account. After an IT admin was socially engineered into releasing login details – to a person he believed to be the CTO who was "locked out of the server" – the hackers were able to piece together login information from different sources and access the CEO's email.[7]

Reflecting on the HBGary attack, its CTO, Greg Hoglund, stated that the company should have applied two-factor authentication (2FA) to Google Apps. "Anybody using the cloud should enable two-factor, if it's an option. If they have any services on the road, such as sales people or technical people, they should have two-factor authentication," advised Hogland.[8]

"Single sign-on capabilities are set to become one of the key requirements for businesses as they move to the cloud"

In June 2012 the passwords of 6.5 million LinkedIn users were published on a Russian hacker's site. The very next day, online dating site eHarmony had its database hacked, with some 1.5 million passwords leaked. The following day, user credentials for online music site Last.FM were breached.[9] These three incidents, affecting up to 10 million users, further demonstrated the fact that SaaS platforms with large user bases attract the attention of organised hackers and hammered home the reasons why login credentials should never be reused for multiple web-based applications.

Following the hacks, Rapid7 released its analysis of the top 10 most commonly used passwords. The top LinkedIn password was 'link'. Others in the top 10 included '12345', 'job' and 'work'.[10] Once again, this showed why organisations need to enforce strong passwords as part of their data security strategy. It also pressed the case for using Single Sign-On (SSO) for cloud-based applications, to minimise the risk of employees sharing or writing down passwords or logging in under the guise of their colleagues.

Ten years ago, the Organisation for the Advancement of Structured Information Standards consortium (OASIS) announced Security Assertion Markup Language (SAML) v1.0 as the new standard for authorising identity and controlling access to web services. SAML (saml.xml.org) was developed by OASIS from the federated identity and authorisation work undertaken by VeriSign, Netegrity, Jamcracker and Securant, to provide a standard means of confirming the identity and entitlement of users, to control access to online partners' services and applications that are used outside of the enterprise intranet. One of the most important current applications of SAML is to enable SSO to online applications. Martin Banks recently wrote: "Single sign-on capabilities are set to become one of the key requirements for businesses as they move to the cloud. The advantages of having the majority of the information management resources a business requires delivered by SaaS will soon be lost if every user has to keep signing in to every service."

He added: "Yet that is only part of the issue, for SaaS services can also bring a new raft of operational management problems. Because the services are only consumed

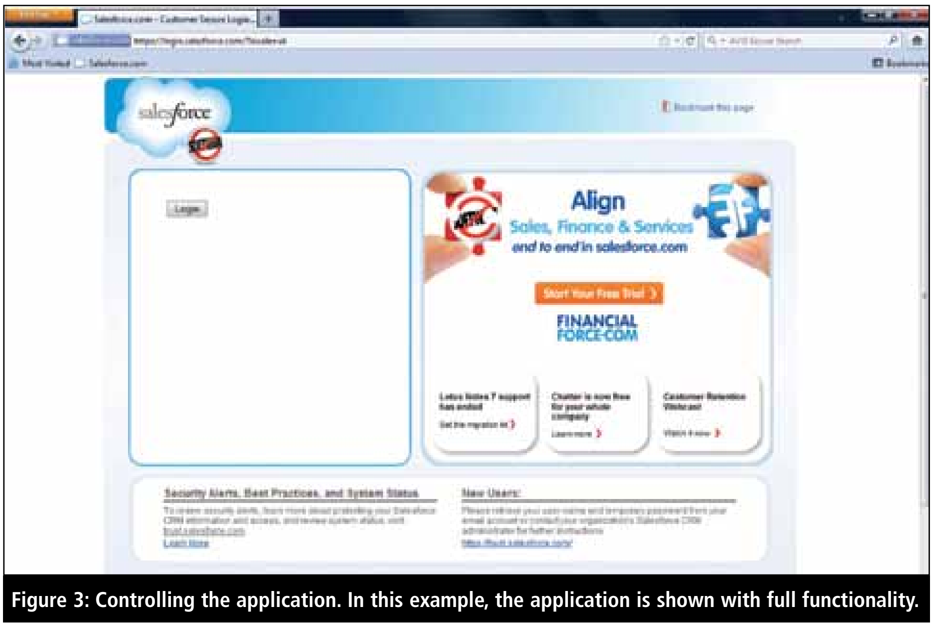
salesforce
Login
Align
Sales, Finance & Services
end to end in salesforce.com
Start Your Free Trial
FINANCIAL FORCE.COM
Security Alerts, Best Practices, and System Status
New Users:

Figure 3: Controlling the application. In this example, the application is shown with full functionality.

on premise, but run somewhere else, authenticating users to use a service is only a small part of the problem. The much bigger part is managing what they do when they are connected."[11]

Social media networks

Enterprises face a policy dilemma when it comes to allowing users to access social media networks. Their use by marketing teams, particularly for press relations and in B2C environments, is increasing. The emergence of the 'social enterprise' has seen an increasing number of sales coming through non-traditional channels as the result of comments and reviews on forums, weblogs, social blogs, walls, microblogs, wikis and podcasts. But with the use of social media comes the risk of exposing sensitive information. Is this risk sufficient to prevent access to sites such as Facebook and Twitter for the majority of users when using company-provided devices?

The 'iGeneration' has grown up using social networking sites and expects to have access to social media 24x7. If the policy suddenly changes to prevent access, this can have a negative impact on morale. The ability to make sites such as Facebook entirely read-only when accessed from company-provided devices is a highly attractive solution. This enables employees to keep up with what their friends are doing, while addressing the risk of them posting sensitive or regulated information. Applying a read-only policy also addresses the associated corporate vicarious liability for staff using company resources to share inappropriate content on a public forum.

Application shaping in the cloud

One of the biggest inhibitors to the increase in SaaS deployment is the forced downgrade to the 'one size fits all' security model offered by the vendors. The vendor models typically lack granularity, which risks non-compliance. Organisations should look to restore on-premise equivalent access control and auditing on web-based applications, independently of the cloud vendor if necessary. This will allow organisations to maintain compliance by detecting and preventing insider misuse of applications, whether inadvertent or intentional.

> ***"Logging, monitoring and alerting should be available for SaaS applications, just as it is for enterprise applications"***

Technologies are emerging to address the challenges that the cloud brings, while still allowing enterprises to benefit from the scalability and portability of cloud-based applications. These technologies take the logical step on from MDM and SSO tools and enable authentication, application shaping and auditing of browser-based activity. This extends corporate governance to any device or interface being used by authorised users and enables CISOs to create an audit trail of activity for compliance with industry or national regulations.

Figure 4 shows how certain tabs can be hidden to prevent activities such as 'export', 'print', 'copy', 'paste' or 'save as'. Financial information can also be masked for compliance purposes. This shaping of the application allows CISOs to regain control over the use of SaaS applications, in line with individuals' access controls. This allows for a consistent security policy across the organisation, regardless of whether the applications are being accessed on traditional server/client models, or over the browser.

Consider exit, at entry

When researching a SaaS solution, a key feature to look for includes the ability to rapidly add new employees and applications, without requiring costly recoding of the back end applications. The recent Avanade survey found that significant IT investment is being made to manage the consumerisation of IT. To enable BYOD and BYOS (subject to the regulatory environment in which the organisation operates) there should be support for different standards and an ability to apply SSO to 'closed' applications. Equally, the ability to rapidly and easily revoke access to cloud-based applications is a crucial consideration. Revoking access to corporate applications in a timely fashion can prove cumbersome in large organisations with thousands of employees. Having the ability to rapidly revoke or increase access whenever employees change roles or leave the organisation should be part of the specification when selecting a SaaS solution.

> ***"It is in the interest of individual IT managers, the IT department as a whole and the overall business to have measures in place to control and monitor privileged users"***

As Gamby wrote, it is important to retain a consistent level of security across the organisation's applications and devices. Therefore, logging, monitoring and alerting should be available for SaaS applications, just as it is for enterprise applications.

Privileged user management

In line with traditional insider threat strategies, when setting up application shaping and auditing in the cloud, it is important to ensure that sysadmin activity can also be monitored. In its 2009 report, IT analyst firm Quocirca wrote: "Privileged User Management, it's time to take control". It added: "The ISO27001 standard for IT management, which is adopted by about 40% of the respondents to this survey, explicitly states that 'the allocation and use of privileges shall be restricted and controlled'. Despite widespread claims to have adopted the standard, many businesses admit to bad practices with regard to privileged user management (PUM) that are in direct contravention to it. It is in the interest of individual IT managers, the IT department as whole and the overall business to have measures in place to control and monitor privileged users. Manual processes are ineffective and do not provide an audit trail that would satisfy regulators. The one way to ensure this is to put in place tools that fully automate the management of privileged user accounts, the assignment of privileged user access and enable the full monitoring of privileged user activity."[12]

Can this be achieved for privileged user management and auditing on browser-based applications?

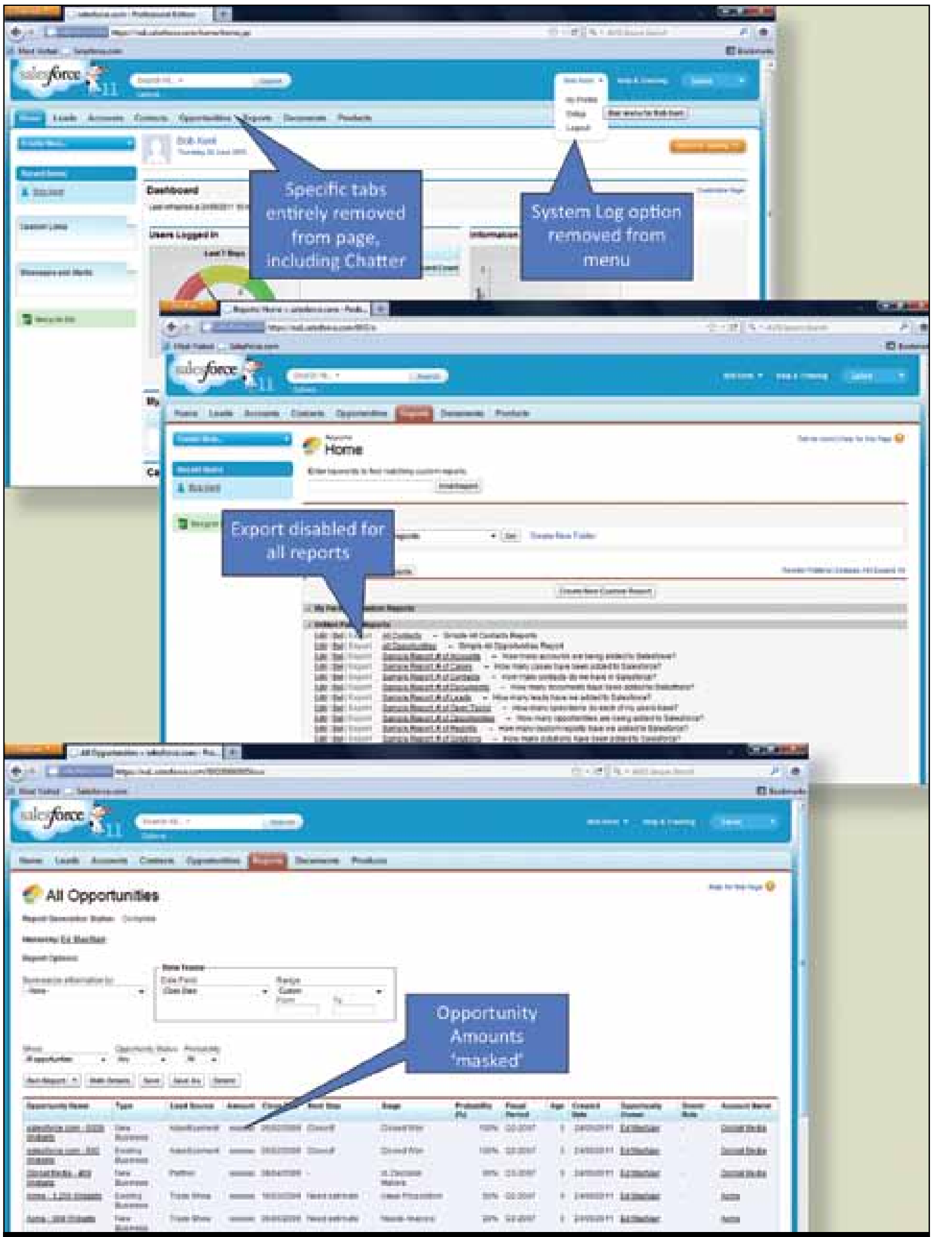
Specific tabs entirely removed from page, including Chatter
System Log option removed from menu
Export disabled for all reports
Opportunity Amounts 'masked'

Figure 4: Tools allow tabs to be hidden to prevent activities such as 'export', 'print', 'copy', 'paste' or 'save as'.

Agents vs proxies

The proxy-based approach to managing web applications is a valid solution for sites that are delivered using the traditional model where each individual page within the application has a unique URL. Proxies are able to filter by URL and block access to specific pages. However, proxies cannot be used effectively to manage content when a web application is a Single Page Application (SPA), also known as a Single Page Interface (SPI) application. An SPA is a web application that has a single URL (only the parameters associated with the URL change) and is intended to provide a user experience more in line with that of a desktop application. Within an SPA typically all necessary code (HTML, JavaScript, and CSS) is retrieved with a single page load. Updates to the page, as the user interacts with it, may or may not involve further interaction with a server. The page doesn't automatically reload during user interaction with the application and control doesn't transfer to another page. The URL in the browser, the attribute that a proxy-based solution relies upon, rarely changes across the entire functionality of the application.

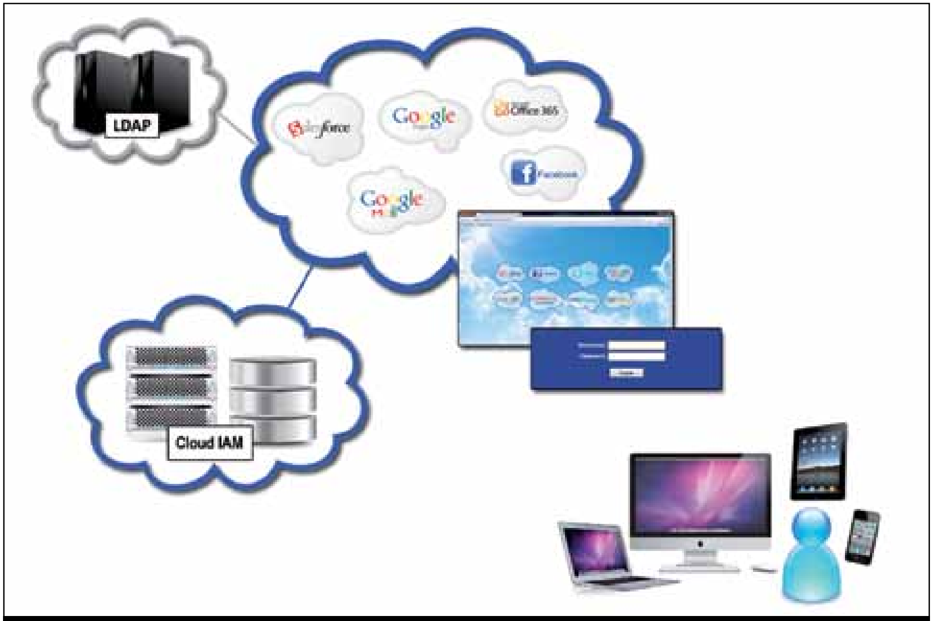

Figure 5: Proxies cannot be used effectively to manage content when a web application is a Single Page Application (SPA).

Google Apps is a well-known SPA. Within Google Apps, as the user accesses GMail and Google Calendar for example, the core URL never changes. Only the URL parameters are modified. With a proxy-based solution there is one choice: allow access to Google Apps in its entirety or block it completely. For filtering individual components, such as specific buttons, links or menu options on the screen, or within the page, proxies simply cannot be used. The majority of modern pages are built on the user's machine and rendered within the browser window. The base HTML is delivered to the client's browser first and then additional functionality is delivered (by JavaScript, for example) that enhances the core structure with event handlers and builds the page up into a richer Document Object Model (DOM).

"To provide restrictions to specific page elements, such as removing tabs and disabling links, the only option is to use an agent"

With proxies, specific URLs must be filtered. The choices are therefore limited to either blocking the base page, or individual scripts within a page. If the base page is blocked then the user will see no content at all. Blocking individual scripts typically breaks all functionality within the page: while the user may see some or all content, the application is effectively crippled. To provide restrictions to specific page elements, such as removing tabs and disabling links, the only option is to use an agent on the device, alongside the browser.

The agent-based approach not only allows highly granular control over access to individual page elements but also delivers additional benefits including:

- Enabling control over access to browser functions such as 'print', 'copy', 'save as', 'view source'.
- Providing CISOs with the option to take a screenshot of the browser content to provide a visual audit trail for compliance (and forensics).
- Forcing users to always access applications via the agent. While proxies can be bypassed if accessing applications outside of the corporate network, agents always require the user to authenticate to the agent first before accessing cloud-based resources, no matter which device they are using.
- Gaining visibility of every user of the application also provides the CIO with a strong cost recovery position. Duplications and underuse of web applications become apparent through the use of agent-based authentication and access control.
- The delivery of SSO across a wide range of devices, not just those known to, or owned by the enterprise.

Summary & conclusion

Cloud computing offers cost centre and P&L-changing benefits to organisations. Along with reduced cost, it delivers greater flexibility and availability. The low capital cost, pay-as-you-go utility computing model, with the agility of on-demand, near-instant provisioning of additional services, is highly appealing. Services are available on a wide range of devices wherever there is a wired, or wireless, network connection. However, the benefits are heavily conflicted, with increased risk, loss of control, forced downgrade to a one-size-fits-all simple security model, lack of evidence of compliance and accountability issues.

"Extending enterprise policy enforcement, access control and auditing is the best route to enabling BYOD and SaaS"

Ultimately organisations have the ability to choose what they move into the cloud. The one thing that cannot be outsourced is accountability. Understanding and managing how users interact with data, no matter where it resides, will remain fundamental to governance, risk and compliance.

IAM expert and former Burton analyst Randall Gamby predicts that current SAML-as-a-service models will evolve into Internet identity provision, where authentication and authorisation is managed for all users. However, we must not forget the audit trail.[13] Extending enterprise policy enforcement, access control and auditing is the best route to enabling BYOD and SaaS, while retaining granular control of data and assets, without impeding the productivity of your best employees.

About the author

Richard Walters is CTO of SaaSID (www.saasid.com), a vendor of security and compliance technology that manages and audits applications accessed via the browser. He has more than 20 years' experience working in the IT industry, complemented by experience in end user roles. Prior to joining SaaSID, he was CTO at Integralis and has worked with blue-chip vendors including Digital, Dell, and Panasonic. SaaSID is a privately held company, founded to address the security and compliance issues created by web-based application use, the consumerisation of IT and the influx of mobile devices into the enterprise IT environment.

Resources

- Hogben, G; Dekker, M. 'Procure Secure: A guide to monitoring of security service levels in cloud contracts'. ENISA. https://www.enisa.europa.eu/activities/application-security/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts.

References

1. Roy, Somak. 'Bring-your-own: software as big a problem as devices'. Ovum, 12 Mar 2012. Accessed Jul 2012. http://ovum.com/2012/03/12/bring-your-own-software-as-big-a-problem-as-devices/.
2. Mahowald, Robert. 'Worldwide Software as a Service 2010–2014 Forecast: Software Will Never Be the Same'. IDC, May 2010.
3. Lauchlan, Stuart. 'Cloud 'sprawl' spreading'. Business Cloud 9, 8 Jun 2011. Accessed Jul 2012. www.businesscloud9.com/content/cloud-sprawl-spreading/5572.
4. 'Global research findings: dispelling six myths of consumerisation of IT'. Wakefield Research on behalf of Avanade. Accessed Jul 2012. www.avanade.com/en-uk/approach/research/pages/consumerization-of-it.aspx.

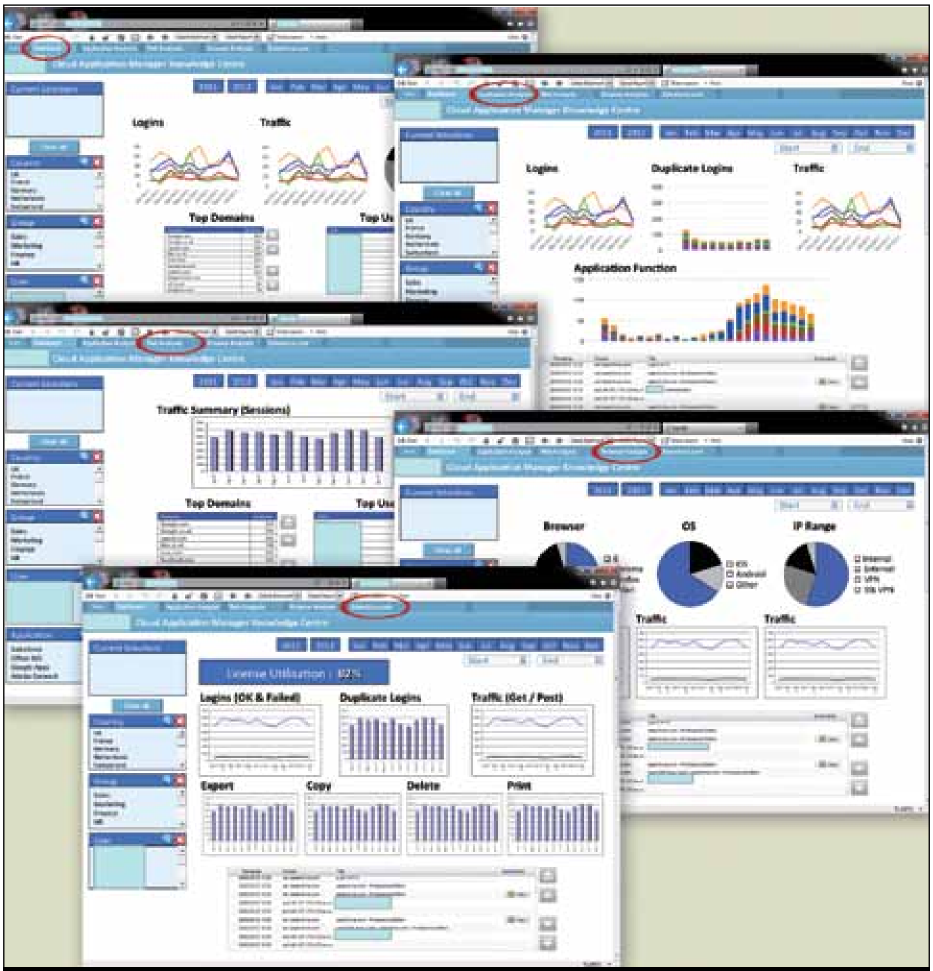

Figure 6: Increased visibility enabled by agent-based management and auditing of applications accessed via the browser.

Cloud standards organisations and resources:

There are numerous alliances, consortia and organisations working on providing consistent guidelines on security and compliance in the cloud:

- Cloud Computing Assurance Maturity Model (CAMM), a consortium that includes the European Network and Information Security Agency (ENISA), has published a report on cloud computing and a framework for risk assessment: www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.
- Cloud Security Alliance promotes the use of best practices for providing security assurance within cloud computing: https://cloudsecurityalliance.org.
- FedRAMP in the US provides a standard approach to assessing and authorising cloud computing services and products: www.info.apps.gov/content/federal-risk-and-authorisation-management-program-fedramp.
- NIST provide various resources on cloud computing including a detailed definition – now at version 15: http://csrc.nist.gov/groups/SNS/cloud-computing/index.html.
- Open Cloud Consortium supports the development of standards for cloud computing and interoperation between clouds: http://opencloudconsortium.org/.
- Open Management Group maintains a wiki at http://cloud-standards.org/wiki which is a rich single source of information from some of the groups and initiatives above.

5. Gartenberg, Michael. 'Gartner Says The Personal Cloud Is Poised To Eclipse The PC As The Hub Of Consumers' Digital Lives By 2014'. Gartner, May 2012. Accessed Jul 2012. www.gartner.com/it/page.jsp?id=2008517.
6. Gamby, Randall. 'MDM architecture considerations for enterprise identity management'. SearchSecurity.co.uk, TechTarget, 12 Jun 2012. Accessed Jul 2012. http://searchsecurity.techtarget.com/answer/MDM-architecture-considerations-for-enterprise-identity-management.
7. Thomas, Keir. 'Security tips from the HBGary hack'. PC World, 7 Mar 2011. Accessed Jul 2012. www.pcworld.com/businesscenter/article/221504/8_security_tips_from_the_hbgary_hack.html.
8. Lemos, Robert. 'HBGary's Hoglund identifies lessons in Anonymous hack'. CSO Online, 17 Mar 2011. Accessed Jul 2012. www.csoonline.com/article/677340/hbgary-s-hoglund-identifies-lessons-in-anonymous-hack.
9. Townsend, Kevin. 'Week of the password breach, LastFM is latest victim'. Infosecurity Magazine UK, 8 Jun 2012. Accessed Jul 2012. www.infosecurity-magazine.com/view/26226/week-of-the-password-breach-lastfm-is-lastest-victim.
10. Wing Kosner, Anthony. 'Unbelievable: Top ten hacked LinkedIn passwords'. Forbes, 11 Jun 2012. Accessed Jul 2012. www.forbes.com/sites/anthonykosner/2012/06/11/unbelievable-top-10-hacked-linkedin-passwords/.
11. Banks, Martin. 'SSO now drives Cloud user policy control'. Business Cloud 9, 7 Jun 2012. Jul 2012. www.businesscloud9.com/content/sso-now-drives-cloud-user-policy-Accessed control/10867.
12. Tarzey, Bob; Longbottom, Clive. 'Privileged user management – it's time to take control'. Quocirca, Faregna, Mariateresa, CA. Oct 2009. Accessed Jul 2012. www.quocirca.com/media/reports/102009/430/Quo%20-%20Priviledged%20user%20management%20-%202009.pdf.
13. Gamby, Randall. 'SaaS access management, finding the best single sign on technology'. SearchSecurity, TechTarget, Mar 2012. Accessed Jul 2012. http://searchsecurity.techtarget.com/answer/SaaS-access-management-Finding-the-best-single-sign-on-technology.

Online privacy: a matter of policy?

Steven Furnell and Andy Phippen, Plymouth University, UK

Privacy is a key topic of interest and concern for those involved with any aspect of online activity. While the concept of privacy may have existed for many hundreds of years, it has become more important as the value of personal data has increased. Indeed, in Magna Carta, one of the first definitions of the rights of the individual in history, there is no mention of privacy, and personal information had little value. With the advent of the merchant classes came competition and with it the concept of competitive advantage, the value of personal information began to increase and with it the need for privacy. However, it is only in post-war capitalist societies that we see an exponential interest. It was the advent of the Internet, with its facilitation of global instant access to information at virtually no cost, that has raised massive concerns for the privacy of one's personal data. And this is due to the number of companies and organisations wishing to access such information, and their reasons for doing so.

Authentication and protection

When considering the ways in which service providers protect our privacy, and the capabilities of end users to ensure their personal data protection, we generally see a mix of fundamental authentication and data protection techniques (eg, logins, user-driven privacy settings) and policy statements. The service provider will usually propose that, through publication of the privacy policy, it is clearly articulating to end users how their data is used and how it is protected. However, privacy policies often come in for criticism for being too verbose and complex to truly allow end users to appreciate the implications of divulging 'their' information while using the service.

Our aim here is to explore the nature of privacy policies in terms of how they are presented and the complexity of the language used. Data drawn from the I in Online project, which explored young people's attitudes toward data protection (including their appreciation of privacy policies), highlights a tension between the understanding of what a policy is, and what it actually conveys. Further exploration of key policies illustrates the complexity or verbosity of language, and the lack of adherence to standards