

Cisco Software-as-a-Service (SaaS) Access Control

Overview

The benefits of using Software-as-a-Service (SaaS) solutions - software solutions delivered via the cloud-computing model - are clear for many organizations, and can include significant cost savings and greater workforce productivity. However, adoption of these services also presents a major challenge for IT administrators: managing access control.

Without effective management of user identity, access and credentials (and the ability to track who is using what application and when), organizations risk compromising their network and data security. They may also fail to meet the demands of compliance regulations, and possibly, hinder the success of a forensic investigation following a data loss event. These potential downsides can undermine any benefit derived from the use of SaaS solutions.

Meanwhile, as the number of SaaS applications in use in the enterprise grows, the need for an effective and easy-to-administrate SaaS access control solution increases. At many organizations, that number may be climbing rapidly - without the awareness of management and IT. Adding to the access control challenge is the fact that, in today's enterprise, more people are working from more places outside of the organization, and using more types of devices to access a wide range of applications and sensitive data.

The SaaS Surge

The recent economic downturn prompted many companies to explore using cloud computing and SaaS solutions in an effort to control costs. They discovered that these technologies - ranging from collaboration services such as Cisco WebEx™ to online application suites like Google Apps and Zoho - not only help them to improve their bottom line, but also allow their workers to share ideas and complete assignments more efficiently than ever before.

Employees have been quick to embrace SaaS solutions, recognizing that these tools do improve their work processes and enhance collaboration with others inside and outside the organization. These benefits have been particularly important to workforces dramatically downsized during the recession. However, employees often fail to get approval or even inform IT before signing up for a SaaS service to "try it out" or to work on an assignment with a partner or client who is already using the service.

Companies are often unaware of just how many SaaS applications are in use within the enterprise until an audit reveals what is often an eye-opening number. For example, a recent audit of SaaS services at Cisco®, which has more than 60,000 employees worldwide, showed that over 300 SaaS applications are in use throughout the company.

It is likely that the number of SaaS applications will only grow at most companies, as more solutions become available and businesses look to take advantage of them as a way to add value and sharpen their competitive edge. In fact, Gartner predicts tremendous growth for the worldwide SaaS market over the next four years. The research firm expects SaaS revenue - which totaled US\$7.5 billion in 2009 and represented a 17.7 percent increase over 2008 revenue of US\$6.4 billion - will nearly double to US\$14 billion for enterprise application markets by 2013¹.

¹ "Gartner Says Worldwide SaaS Revenue to Grow 18 Percent in 2009," Gartner, Inc., press release, November 9, 2009: <http://www.gartner.com/it/page.jsp?id=1223818>.

Mobile Workforce Adding to the Challenge

As companies adopt more SaaS applications, they are seeking effective ways to control which users have access to specific services, as well as their access rights within each service. However, the increasing number of users moving outside the traditional enterprise security boundary and toward a “borderless network” complicates this already difficult challenge.

More remote and mobile workers are accessing the network, and SaaS applications, from wherever they need to work - an airport, at home, a corner café - and through different devices, from smartphones to laptops to netbooks. In addition, they are passing sensitive data, such as sales or customer information, through these devices, which may or may not be supported by the enterprise, and often, are used for both professional and personal computing.

IT administrators cannot extend the same level of security and control to remote users who access SaaS applications without going through the corporate infrastructure. So, as IT struggles to apply access controls that will help ensure that the correct people have access to the appropriate parts of the network and associated applications, there is also an urgent need to find an effective and efficient way to accommodate users accessing SaaS applications remotely.

The Need for Control and Visibility

To prevent the loss of sensitive data, IT administrators also need the ability to revoke SaaS access rights in a timely fashion - for example, following a user's departure from an organization. However, the current process for revoking SaaS access rights is far from expeditious or efficient.

When an employee leaves the company, he or she usually retains access to SaaS applications until the next sync-up between the corporate user directory and the applications. This lag time in the revocation of user access rights leaves an open window for disgruntled employees to steal corporate data. And again, with so many SaaS applications in use today at any given organization, there may be no way of knowing for certain just how many accounts a user had access to before he or she departed the company - and whether or not that employee was able to take critical data out the door.

IT administrators also need a single repository of user access reports for all SaaS applications in use in the organization. Having visibility into and documentation of each SaaS user's access history can save valuable time in a forensic investigation following a data breach. It also helps to ensure that the organization is meeting the demands of compliance regulations that are designed to protect certain types of sensitive data, such as a customer's social security number.

So, as SaaS traffic balloons, and the number of remote and mobile users accessing these applications from different devices and unmanaged endpoints swells, IT administrators are finding it impossible to handle the following three activities critical to network and data security in a way that ensures the enterprise is protected:

- Managing user identity.
- Managing user access.
- Managing user credentials.

Managing User Identity

For each SaaS application, user identity data must be replicated in the cloud, so the SaaS application recognizes which access rights to grant to which user. This process is cumbersome and prone to errors; it also requires constant sync-ups to remain up-to-date.

To overcome these issues, some enterprises give each SaaS vendor access to their active corporate user directory via a “tunnel.” However, while this approach may be manageable for one or two SaaS applications, it presents a

significant challenge for administrators to maintain as the number of applications scales. It also poses a significant security risk, since there is the potential for misuse of user directory information by vendors.

Managing User Access

IT administrators do not have a single place to enforce which users can access which SaaS applications. In addition, access controls exist separately for each SaaS application. For example, an employee accessing Salesforce.com does so directly using login credentials that are separate from his or her enterprise network login.

If an employee leaves the organization, the company must disable each user account associated with each SaaS application to which the user had access. However, companies often have no idea how many SaaS applications an employee may have been using.

Revoking user access is also becoming an area of concern for organizations that outsource or offshore operations; employee and contractor turnover is often high among third-party service providers. And as mentioned earlier, IT's inability to extend the same level of security and control to remote users who access SaaS applications from unmanaged endpoints, and do not go through the corporate infrastructure, is another significant security pitfall.

Managing User Credentials

Username and passwords vary between different SaaS applications, making it difficult for users to remember them all. This results in help desk calls, which, over time, can be very costly for organizations - particularly in terms of lost productivity for employees and IT.

Another key risk area is that user credentials pass over the internet, which makes them vulnerable to attacks.

Also, because each SaaS vendor has a different policy for password strength and changes, it is difficult for the enterprise to adhere to corporate standards. Meanwhile, compliance regulations such as the Sarbanes-Oxley Act (SOX) and the Payment Card Industry Data Security Standard (PCI DSS) require that these standards be enforced, especially for users who have access to data such as sensitive patient information or financial records.

The obvious complexity of managing SaaS access control makes it impossible for organizations to take full advantage of these solutions without putting their data and network security at risk.

To help address the challenges just described and ease the management burden on IT, Cisco is introducing a standards-based SaaS Access Control mechanism to its AsyncOS® for Web 7.0 solution.

With Cisco SaaS Access Control, IT administrators retain control over user identity and associated access rights. And users enjoy a seamless experience, accessing all of the SaaS applications that they are authorized to use with one corporate username and password.

Solving the Access and Identity Problem

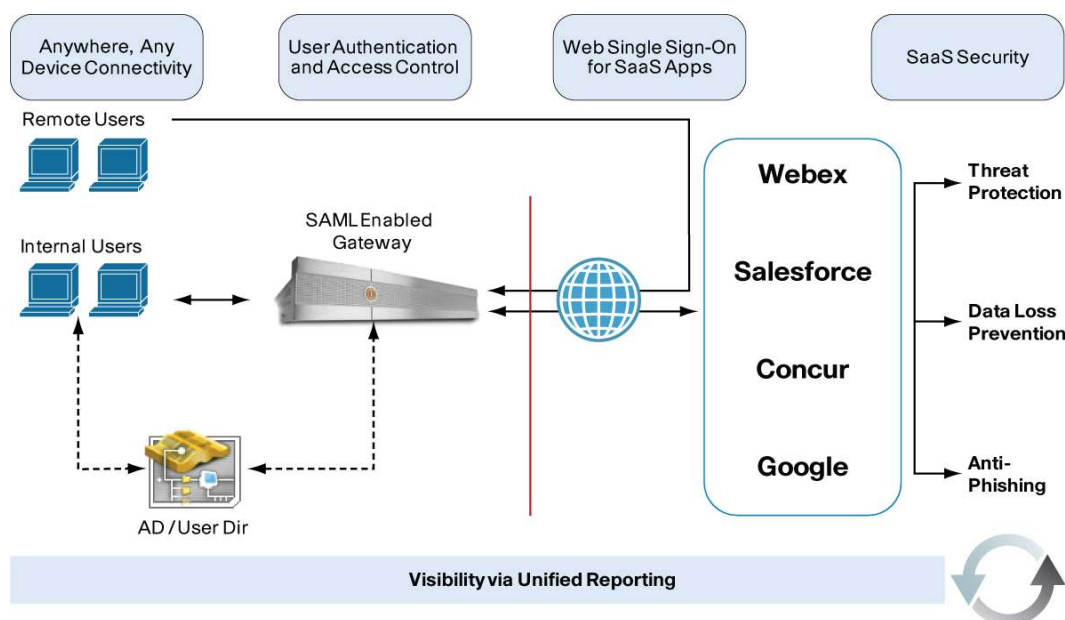
To respond to the security and data management problems inherent in a SaaS environment and a highly mobile workforce, organizations need an access control solution that is:

- **Seamless** - Easy to implement and invisible to the end user.
- **Secure and Controllable** - Allows administrators to control authentication and authorization for legitimate users, to revoke access as needed, and to gain visibility into user behavior via access reports.
- **Standards-based** - Uses technologies and languages that are employed by SaaS vendors.
- **Mobile-ready** - Accommodates users who are accessing SaaS applications via mobile devices, or who are outside of the corporate network.
- **Intelligent** - Delivers attributes relating to user access to SaaS providers (for instance, which users have access to which channels of information).

The Cisco SaaS Access Control solution, built into Cisco IronPort® S-Series Web Security Appliances, addresses the challenges presented by adoption of SaaS solutions, and provides IT managers with the controls necessary for managing access to SaaS applications and enforcing security policies. The SaaS Access Control solution uses Security Assertion Markup Language (SAML) to authorize access to SaaS applications.

With SAML, IT administrators retain full control over authentication and authorization of workers who use SaaS solutions, and users gain the ease of use associated with a single corporate sign-on for all of their SaaS-based activities. See the box on page 6 for more information about the SAML standard. (SaaS applications must support SAML 2.0 in order to exchange information with the SaaS Access Control solution).

Figure 1. Extending Security and Control with Cisco SaaS Access Control.



SaaS Access Control, Step by Step

The Cisco SaaS Access Control solution allows IT administrators to easily and securely manage identity, access and credentialing for access to SaaS applications. For both administrators and users, the process works as follows.

Configuring the Solution

Step 1. The IT administrator establishes user authentication and authorization via SAML on the SaaS application and the Cisco IronPort Web Security Appliance (WSA). The administrator:

- Creates a unique URL through which users can access the application (for example, <http://saas.mycompany.com/SSOURL/GoogleApps>), and configures the URL so that it can be identified by the Cisco IronPort WSA.
- Obtains the service provider metadata from the SaaS application vendor, and imports the file to the Cisco IronPort WSA.
- Uploads an enterprise digital certificate to the SaaS application, and to the Cisco IronPort WSA, to ensure secure communication.

Step 2. The IT administrator creates policies for the SaaS application - for instance, how given user groups can gain access, as well as access rights that are dependent on the user's location (remote workers versus users within the network).

Step 3. The IT administrator can send the unique URL to all users, or create a bookmark with the URL on the company intranet.

Granting Access to Users

Step 1. The user accesses the SaaS application via the unique URL. If the user is not already authenticated, the Cisco IronPort WSA authenticates the user. This authentication can be seamless to the user, or can be completed via a browser authentication prompt, depending on the configuration.

Alternatively, the user can visit the SaaS provider's website and enter the company domain name and other specific account details. The SaaS provider then redirects the user to the Cisco IronPort WSA for access control.

Step 2. The Cisco IronPort WSA intercepts access, identifies the user, and generates the SAML information to represent the user.

Step 3. The Cisco IronPort WSA sends the SAML assertion to the SaaS application. This can include user identification information, such as username, as well as configured attributes, such as location. The SAML assertion is sent securely using the digital certificate configured on the WSA and the SaaS application. Note that the user password is not sent to the SaaS application.

Step 4. The SaaS application responds with the requested resources and grants access to the user.

Solutions for All Access Challenges

Cisco SaaS Access Control addresses the three key problem areas that IT departments face when expanding their use of hosted applications.

Managing User Identity

With Cisco SaaS Access Control, IT administrators do not need to replicate user identity data for each SaaS solution, nor do they need to grant SaaS vendors access to their corporate user directories via tunnels. Once administrators have configured authentication and authorization rules via SAML, the solution is maintenance-free.

Managing User Access

Administrators can use the Cisco IronPort WSA as the single place to enforce which users can access which SaaS applications, and how they can access these solutions. For instance, administrators can indicate that only sales employees can access certain areas within Salesforce.com, or that only executives at the VP level or above can access certain information.

In addition, administrators can also manage access for mobile users who are accessing SaaS applications, with the same level of security and control for onsite employees within the corporate network. With Cisco SaaS Access Control, all access to SaaS applications is managed by the Cisco IronPort WSA - even for mobile workers. This ensures uniform enforcement of an organization's security policies.

Along with consistent enforcement of user access policies, the solution revokes access to all SaaS applications once corporate user accounts have been disabled - with no delays from sync-ups between corporate user directories and the SaaS applications. (Note that while the solution does manage access to SaaS applications, it does not provide for the creation or deletion of SaaS user accounts.)

This real-time control reduces opportunities for data loss, whether inadvertent or intentional. Administrators may also view access reports to gain information about user behavior, or to conduct forensics in the event of data breaches.

What is SAML?

Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains - in other words, between an identity provider (such as an enterprise) and a service provider (such as a SaaS company). SAML's value comes into play for organizations that need to share authentication and authorization information, without putting corporate security at risk. With SAML, enterprises don't need to grant outside vendors access to their user directories.

Many SaaS providers, including Salesforce.com, Cisco WebEx, and Google Apps, have adopted SAML 2.0 as their standard for authentication and authorization (see list of service providers that have adopted SAML at <http://saml.xml.org/wiki/list-of-organizations-using-saml>). Cisco has chosen SAML to drive the user authentication process within its SaaS Access Control solution because of its ease of use and security. Note that SaaS Access Control only helps manage access for SaaS applications that are compliant with SAML 2.0.

The Cisco Advantage

Cisco SaaS Access Control is integrated with Cisco IronPort Web Security Appliances, reducing IT management headaches as well as total cost of ownership. Other vendors that provide federated identity solutions require additional appliances or add-ons via cloud computing - thus placing key controls outside the network edge. The Cisco IronPort Web Security Appliance uniquely manages control challenges within the web gateway.

Managing User Credentials

With Cisco SaaS Access Control, employees need only their corporate username and password to log in to all SaaS applications. This creates a faster and more streamlined experience for corporate users, who no longer need to manage multiple login names and passwords for each SaaS application. In turn, this reduces dependence on the IT help desk, and improves worker productivity.

The use of a single username and password allows organizations to consistently enforce their policies for password strength and changes. Such enforcement makes it easier for enterprises to comply with password standards under regulations like SOX and PCI DSS.

Since the sign-in process takes place via corporate networks, and not over the Internet, login names and passwords are far more secure and less vulnerable to hacking or theft.

Conclusion

The question for enterprises not yet using SaaS applications is not **whether** they will adopt them, but **when**. Also, as they embrace more of these solutions, how will they address the complexity of managing user access and security for multiple SaaS applications?

Cisco's SaaS Access Control mechanism in AsyncOS for Web 7.0 gives organizations the freedom to take advantage of the cost savings, ease-of-use, and productivity enhancement of SaaS applications without undermining security or compliance. IT can securely and actively manage user access from a single, central location that provides visibility into user activity related to SAML-compliant SaaS solutions in use by the enterprise.

Cisco SaaS Access Control also allows employees to access SaaS solutions whenever and wherever they need to - and from any device. This ability will be particularly important to organizations as they adapt their security policies and embrace new solutions to support the emerging borderless enterprise.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco.Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)