Managing and securing user identities in the cloud is getting complicated. Here's how to keep it under control.

By Ericka Chickowski

PLUS Security’s big headache: The evolving user
Security’s Pain In The Neck: Evolving Users

Security would be so much easier if users were like lamps. You turn them on, they do what they’re supposed to. You turn them off, they’re no longer something to worry about. You know where a lamp is all the time. You can monitor it to find out its status.

Unfortunately, users are not lamps. If you look at the history of security breaches, almost all of them started with an end user mistake: a misplaced laptop, a user falling for a phishing attack, a curious employee downloading the wrong software. And yet even tech-savvy companies like Sony and RSA can’t completely stop breaches.

One of the chief reasons is that users aren’t static. They change their locations and are now doing work from homes and coffee shops. But mobility is only one way users change. They change their job responsibilities, their projects and the tools they use. They get promoted. They quit. They get fired. This “evolution” of users has been a problem for businesses since the early days of computing. Most IT organizations want to provision users with everything they need and then be finished. Changes create more work, sometimes forcing IT to repropose a user who’s already been provisioned. It’s annoying.

But failing to monitor a user’s changing responsibilities and access requirements can lead to nightmares. Matthew Keys, who is accused of helping hackers deface the Los Angeles Times website earlier this year, is a former Tribune Co. employee who had a user name and password that still worked two months after he was fired. In 2009, a fired IT employee used his still-active credentials to plant a logic bomb at Fannie Mae. These are just a couple of instances in which an employee’s change in status wasn’t updated quickly enough by IT, and disaster ensued.

The problem, in a nutshell, is that there is still not much connection between a user’s identity — as defined under Active Directory or in the corporate system registry — and the user’s real identity, as defined by what he or she does for the organization. Employees get transferred, and nobody tells IT. A user is terminated, but IT never disables his access. A new employee is given too much privilege and taps into the wrong data.

As companies begin to tie into cloud services and other outsourced infrastructure, this problem becomes even more acute. In today’s Dark Reading digital issue, we examine the challenges of user provisioning and identity management in the cloud, which adds a new level of complexity to the access management picture. The cover story points out the need for more efficient methods for provisioning new users and changing access privileges as users’ jobs change.

Security would be easier if users were like lamps. But they’re pretty complex — they change and evolve, and they get into places they shouldn’t. Enterprises would do well to build access management strategies that recognize these realities — and adapt to them.

Tim Wilson is editor of DarkReading.com. Write to him at timothy.wilson@ubm.com.
EXTEND ENTERPRISE SECURITY TO CLOUD APPLICATIONS

- 56% of organizations use 6 or more SaaS applications
- 76% of network intrusions exploit weak or stolen credentials
- 81% of employees use SaaS applications without IT approval
- 20% of all Americans have 20 password-hungry online accounts
- 147M cumulative malware samples captured

"Among the nine threats identified in the Cloud Security Alliance’s ‘Top Threats to Cloud Computing’ research, account hijacking is one of the most serious on the list, and abuse of credentials is not far behind." —SANS Institute

Control WHO has access to cloud applications

McAfee® Cloud Single Sign On
McAfee One Time Password

- Single sign-on for hundreds of popular cloud applications.
- Multifactor authentication to reliably verify users’ identities and prevent account breaches.
- Easy user account provisioning and de-provisioning.
- Cloud activity monitoring and logging.

Control WHAT they can do with that access

McAfee Web Gateway
McAfee Data Loss Prevention
McAfee Global Threat Intelligence

- Thwart malware infection with zero-day detection.
- Block malicious URLs with site reputation and threat intelligence.
- Prevent confidential data from leaking with DLP policy control.
- Encrypt files stored in the cloud.
- Blacklist and whitelist cloud applications.

McAfee helps you leverage cloud applications without compromising security.

FIND OUT HOW McAFFEE CAN HELP:
www.mcafee.com/identity
www.mcafee.com/webprotection

---

4. AP Twitter Hack Shows It’s Time for the Post-Password Era, CNBC.
5. McAfee Threats Report, Second Quarter 2013, McAfee Labs.
As companies add more cloud services to their IT environments, the process of managing identities is getting more complex.

When companies use cloud services — services they don’t control themselves — they still must develop sound policies around role-based access. They still must grant rights to users who need information to get work done. And they must be able to automatically take away those privileges when people leave a company or change roles. On top of it all, companies using cloud services are also bound by any compliance rules that govern their identity and access management (IAM) initiatives.

With the collection of cloud services now holding sensitive data, organizations have to contend with a smorgasbord of new login

Identity Management In The Cloud

Managing and securing user identities in the cloud is getting complicated. Here’s how to keep it under control.

By Ericka Chickowski
@ErickaChick
systems and proprietary connector APIs that often don’t work well with internal IAM systems. “I bet that not many IT professionals thought they would look nostalgically at large, complex, on-premises deployments, but now many do,” says Julian Lovelock, VP of product marketing for identity assurance at smart card manufacturer HID Global.

Managing cloud IAM means “using a complex set of one-off procedures,” says Nishant Kaushik, chief architect for cloud IAM provider Identropy. This approach may lead to “chaos and an inability to audit any of the systems.”

But sound identity management and governance is core to nearly all IT security functions. That’s why security experts are advocating that companies improve how they manage identities in environments that mix cloud services and enterprise networks. “In this new world, you have to stitch the identities together,” says Todd McKinnon, CEO of cloud IAM provider Okta.

Building Policies

Ask any enterprise IT administrator if his or her organization has a process for managing new software deployments, and the answer is invariably yes. You’ll also likely get all hands raised if you ask about password management and user account management controls, says Greg Brown, VP and CTO of cloud and data center solutions for McAfee. But there aren’t nearly as many raised hands when you ask how many have a procedure for someone to buy infrastructure-as-a-service, or...
for on-boarding users in a new software-as-a-service (SaaS) application, he says.

Two of the most fundamental policies of IT are which software can be used and how the credentials to use them should be administered, says Brown. These policies govern which applications, devices and people have access to which pools of sensitive information. Companies have these policies largely in place for on-premises systems, but they often do not know which users are leveraging SaaS — and whether they’re compliant with corporate and regulatory policies.

The need for security and compliance is driving some companies to find better ways to bridge enterprise IAM and cloud provider applications, often by provisioning user identity through cloud-capable, federated single sign-on (SSO). “In a bridge, the enterprise maintains control of its own identities and its own authentication,” says Allan Foster, VP of technology and standards for ForgeRock, an open platform provider of IAM systems. “And since the service transaction is initiated by the enterprise, it can maintain auditing as to who accessed the service and when, although not about what was done.”

Many companies are achieving this bridge through Active Directory (AD) and Lightweight Directory Access Protocol connections, setting policies that can be enforced through group membership based on the users. Enterprises have been pressuring cloud providers to embrace standards including SAML, OAuth and OpenID for easier exchange of authentication information between the cloud provider and the enterprise.

An employee using a federated single sign-on system is given one set of credentials to access multiple cloud accounts. This user is only authorized to use those cloud accounts permitted by the group he or she belongs to. For example, if a user is in the sales group in Active Directory, he or she would be given secure access to Salesforce.com as well as the enterprise’s in-house sales applications. This approach aids the rapid rollout of new cloud services to large groups of users. Even more importantly, using AD to aggregate identities in cloud environments speeds up the deprovisioning of cloud applications to employees when they leave the company or change roles.

“Enforcing the use of federated SSO — and not using passwords with cloud apps — means that users can only log in to cloud apps if they have an account in AD,” says Patrick Harding, CTO of cloud IAM company Ping Identity. “Terminated users are usually imme-
diately disabled in AD by IT and will not be able to access any cloud apps."

This type of single sign-on provides more control over the cloud sign-in process, but it’s only at the first stage of maturity for efficiently getting people onto the system. This initial operational focus mirrors the maturation that happened with on-premises IAM years ago, says Kaushik. “Once the cloud operational things are solved, people realize they have governance problems and compliance problems,” Kaushik says. “It isn’t simply about being able to create accounts. It’s also how to create an account, when to create an account and how to deprovision an account.”

As companies get accustomed to cloud single sign-on, they often find that cloud identity services lack fine-tuning for authorizing and monitoring a user’s access to cloud resources.

**Cloud Identity Control Gaps**

Even after companies implement single sign-on, one of the biggest headaches they face in managing identity in the cloud is that IT managers still can’t control, or even see, what people do with the application after they log on. For example, cloud app authorization at most organizations relies on a role or group member status to determine if a person has access. So the single sign-on system knows a person has access to, say, a Salesforce account, says Kaushik, but SSO doesn’t know whether the person can just view or also access customer information. One risk is that tracking and monitoring becomes nearly impossible once a user is logged in to the system, and many companies are required by internal and regulatory rules to track who performs which actions to data, and when. A cloud system might only track that a company’s account took a particular action.

Right now, to get granular understanding of what account holders do in a cloud application and with cloud data, many companies resort to manually customized controls involving “complicated road mapping” that can’t easily be audited, Kaushik says.

Much of the blame lies with the cloud software providers, which haven’t given companies much access to the internal software controls that providers use to manage user rights within the system. Similarly, user provisioning in cloud services is centered on proprietary APIs, and connectors frequently break and create holes in IAM. Many companies move to the cloud as a cost saver and don’t have the resources to build connectors, Kaushik notes. Cloud vendors spend considerable time developing APIs and connectors around business functionality, but most haven’t invested in APIs that connect to data feeds that enable identity governance, such as information about account privileges.

Some cloud providers and SaaS developers are beginning to recognize identity management as an opportunity to differentiate themselves. For example, ClickSoftware, a developer of mobile workforce management software, has invested heavily in CA IdentityMinder, SiteMinder and SiteMinder Federation for self-provisioning, which helps enterprises identify
and authorize user access for its cloud-based software. “One of the main challenges every cloud company faces is the ability to provide its customer a way to self-provision services they are getting over the cloud,” says Udi Keidar, VP of cloud services for ClickSoftware. “A real cloud or SaaS service should give users the utmost independence to run and maintain the service by themselves.”

HID Global’s Lovelock cuts cloud vendors more slack over not offering customers greater IAM control: “That’s not entirely the cloud provider’s fault — good standards have yet to emerge.”

A new standard called System for Cross-domain Identity Management concentrates on accounts and attributes and has received the endorsement of applications vendors such as Salesforce and Cloud Foundry. But SCIM is still in its infancy. “The questions with SCIM is, one, can it be broadly endorsed by the SaaS application providers themselves?” McAfee’s Brown says. “And then, two, can we make sure that we can build in the administrative controls on the corporate side so that [the applications] are administered through the same interface?”

Until SCIM or another standard takes root, organizations must consign themselves to negotiating with each SaaS provider to get identity control into contracts. For example, John Michener, chief scientist at security consulting firm Casaba, says that when it comes to platform-as-a-service, a typical cloud provider will likely have some kind of authentication and authorization framework that users can employ to access a specific enterprise’s instance of a cloud application.

Companies should negotiate that a SaaS vendor provide full knowledge of all actions taken by users, including authentication attempts, monitoring alerts on repeated failures, and auditable tracking of problems using a monitoring tool of their choice.

Identity management in SaaS is a little trickier than on-premises software because the available administrative features are usually limited by the cloud service’s functionality. Some SaaS providers may not have features that are capable of tracking a user’s access privileges, number of account log-ins, type of data accessed or downloaded, or amount of time spent in a system. They also may not let a company limit how much data or what type of data users can access through the SaaS application. Finally, cloud services may not have the API capabilities to connect with existing on-premises IAM tools.

Companies should check on whether the cloud vendor is properly managing privileged access controls for administrative accounts. A recent survey conducted by CyberArk showed that 56% of organizations had no idea what their cloud provider was doing to protect and monitor privileged accounts.

“The cloud isn’t magical IT,” says Lovelock. “It’s made of servers, software and all the normal stuff of any IT service. That means there are administrative accounts. Someone has those passwords and access to your important data.”

Adding User Value Through IAM

Sometimes the business need for a cloud app will outweigh concerns IT has about the ability to track what a user does inside the app. In those cases, IT organizations can try workarounds that may offer more insight into user behavior in the cloud. Brown says organizations should think about coupling single sign-on with data enforcement policies to audit SaaS activity using firewall or gateway logs, and then monitor user access via data leak prevention (DLP) tools. “Using that data enforcement policy, you can say, ‘I’m going to look at this SaaS application for these users,’” he says. “You can use the enforcement capabilities in DLP to say what is appropriate or inappropriate to be
published out to an online sharing site.”

As standards evolve and would-be buyers pressure cloud app providers to let them tap into the proper identity-related data feeds, companies should be building cloud identity portals to track and control user access rights and SSO projects that enhance the business case for cloud services. The more value security adds through IAM, the easier it will be for the IT department to rope rogue cloud deployments back under the IT governance umbrella.

IAM can make it easier to shift gears between different cloud applications without having to log in using different credentials. Implementing SSO makes it possible to safely use one set of credentials for everything, with very little interaction with IT required.

“If you make it highly functional, then users will be glad to use it, and then you’ve captured the prize,” Lovelock says. “Make the portal fancy enough to plug into apps from the on-premises side and the cloud. Make the password reset integrate right into the portal. Allow access from anywhere, but perhaps apply rules where some apps can be accessed from the coffee shop and some cannot.”

If IT is seen as an inhibitor, Brown warns, then business units are more likely to spin up ad hoc cloud deployments. But if SSO is seen as an easier way to log in to everything, users will demand their new deployments work through the system.

Brown offers the example of an enterprise customer that reined in deployments of Amazon Web Services by offering single sign-on. Staff from different business units used multiple AWS accounts, using native AWS sign-in capabilities for each account. IT worked with each unit to regain control of the cloud contract and do logins through a corporate SSO system.

This made it easier for IT to track AWS use and helped users by letting them use their everyday password through AWS, rather than having to remember multiple credentials. And the company had better clout in negotiating with Amazon.

If more groups take this lesson to heart, they may find that identity management not only helps IT set up the foundation to make security improvements to the cloud model, but it can improve IT operations that are fragmenting across the company.

Write to us at editors@darkreading.com.