SearchSecurity.com
E-Guide

Uniting IAM and data protection for greater security

There's been a new development in the information security world: content-aware identity and access management, an integration of two established, usually separately administered domains. This tip explains why uniting these two domains makes sense and addresses key parts of the identity portion of IAM and how they work in the context of the cloud.

Sponsored By: ca technologies

TechTarget
Where Serious Technology Buyers Decide

SearchSecurity.com

E-Guide

Uniting IAM and data protection for greater security

Table of Contents

Content-aware IAM: Uniting user access and data rights

By Randall Gamby, Contributor

Recently there's been a new development in the information security world: content-aware identity and access management (CA-IAM). CA-IAM is the integration of two established, usually separately administered security domains -- identity and access management (IAM) and data protection.

The first domain, IAM, is used to administer user rights. When security personnel think of tools in the IAM domain, they picture Web access management systems, provisioning systems, portals, Web-based applications and federation technologies. The common theme among these technologies is the configuration of data access based on the adage "the right people, getting the right access to the right information."

However, within enterprises there's another, sometimes darker, domain: data protection. The goal of data protection is to correctly configure data rights for information. The people interested in data protection talk about classification of information (i.e. company confidential, secret, top secret, etc.), data loss prevention (DLP), meta-directories, security information and event management (SIEM), event logging, firewalls, secure communications and encryption. The common theme within this domain is "the right data, getting to the right place securely, by means of the right services." While IAM's focus is to secure communications channels to applications and services for *users*, data protection's focus is to establish secure communications channels to applications and services for *data*: the yin to IAM's yang.

So why does the concept of combining these two domains make sense? There are three reasons: compliance, data transformation and intelligent user rights.

Regarding compliance, combining the user access rights of identity and access management with the information protection rights of data protection solves the overarching business issue of compliance. Under the cover of existing regulations around privacy and protection -- whether government (i.e. SOX, HIPAA, GLBA, Basel II) or industry driven (i.e. PCI DSS) --

the auditors expect companies to have implemented controls around both authorized user access and data protection. Since the tools that implement these controls have been traditionally separated, it makes sense to combine their functionality for the common good of compliance.

Data transformation involves scenarios in which new data sets are added, data is manipulated, and old data sets are expunged. Managing the sensitivity and value of information during these transformations is becoming increasingly more difficult due to the volume of data a typical enterprise manages and the fact that external organizations are often managing key pieces of data via outsourcing and SaaS to enhance a company's data management capabilities. Determining access to the newly updated and created data can be a nightmare. CA-IAM promises to identify how these transformations have affected the data and, if warranted, automatically map new protections to the data, and then go on to assign new access rights to the information based on corporate policies. An example of how this can be used is a recent announcement of an alliance between Microsoft and EMC Corp.'s RSA unit in which the vendors plan to develop a tight integration between RSA's DLP suite and Microsoft's digital rights management technology. The goal of this alliance is to take the best features of RSA's DLP automated data classification services and map them to Microsoft's file management technology to ensure data classifications and rights automatically follow the data.

With intelligent user rights, it has become important to understand the roles and responsibilities of an individual when determining his or her access to applications and services. After determining an individual's rights, CA-IAM can be used to give proper access to the data, providing fine-grained access controls beyond the application down to the actual data itself.

So if CA-IAM provides such great benefits, why haven't more enterprises implemented it? There are several reasons. First, both IAM and data protection had their start in different parts of the enterprise. IT traditionally started managing user access as part of its infrastructure provisioning projects. As users joined the company, IT added their accounts to the systems they needed to do their jobs. Subsequently, as users' roles or employment statuses changed, IT was responsible for managing and updating their permissions, eventually taking away all rights when users left the company.

Data protection started in the traditional risk management and IT security departments. The responsibility of the data protection pros was to safeguard sensitive data and ensure it didn't leave the organization through unauthorized channels. While these two groups usually work well together, they've each traditionally reported up to different parts of the organization. The prospect of integrating these two disciplines presents, if not a managerial problem, at least a serious managerial project.

Also, in order to even consider implementing CA-IAM, an organization must understand its user and data classifications and have defined processes for managing them. Many organizations are still in the throws of doing role-based access definitions, finding and classifying data based upon existing policies, and aligning risks across the organization. In addition, DLP and IAM tools are still being implemented. Without a level technology playing field, integration of IAM and data protection technologies will involve a lot of time, effort and money, and probably a few costly mistakes along the way.

Something else to consider is that CA-IAM is a concept, not a product. Today's organizations are working to solve business problems through technology; tomorrow's technologies are still in the hands of enterprise architects and risk managers. Full enterprise deployments of CA-IAM, and the standards and experience they bring, are still years off. So does this mean companies can't do CA-IAM today? Not necessarily. While a formal deployment is not yet possible, an enterprise that already understands its data and access requirements, has classified its data, user roles and responsibilities, and has strong political clout, should be able, through policies and processes, to begin to create a common framework, even if the tools aren't integrated. This is how traditional IAM technologies started and it's the way that CA-IAM will begin.

cloud security.
can you see beyond the problem?

you **can**

The #1 issue for companies migrating to the cloud is identity and access management.
But for the agile business, *know*-ing users is always better than *no*-ing them.

In fact, agile businesses, using our Content-Aware Identity and Access Management solutions, have been able to reduce security risk while improving productivity, access and efficiency. More effective compliance, reduced IT risk, broader, more secure customer and partner relationships.

That’s what happens when *no* becomes *know*. And security turns into agility.

To see how we can help make your business more agile and secure, visit ca.com

agility
made possible™

ca®
technologies

Top cloud identity management considerations

Identity and access management (IAM) is a system of technical and non-technical mechanisms to ensure the proper establishment and control of identities, the assignment of privileges to those identities, and then controlling access based on those privileges. Most organizations that are planning on utilizing cloud computing services need to ensure those mechanisms are appropriately integrated into their cloud plans. In this tip, we'll address key parts of the identity portion of IAM and how they work in the context of the cloud. When thinking about cloud identity management, two of the most important questions or architecture decisions that need to be made are:

- What type of Identity validation is acceptable?
- Will you trust others' identity stores or only use your own?

Cloud identity management: identity validation

There are two primary mechanisms by which identities are validated: organizational and personal.

Organizational: In an organizational validation, there is a process by which the identity of a person is confirmed or asserted by the organization that is creating the identity. This is basically the process by which users are assigned IDs within an organization. There is typically some level of trust that is associated with the validation.

Personal: When someone says who they are. There is typically no additional validation of the information the user gives. For example, I can register a username with a well-known Web mail account and self-assert that I am John Wayne or Bill Gates or Steve Jobs, or some other famous person. There should be a much lower level of trust associated with this type of validation, as compared to the organizational type.

Companies should utilize organizational-based assertions for business-related purposes, but if you have consumer-focused services, self-assertion may be an acceptable option. It's important to note that in order for you to be successful in implementing or using organizational identities for cloud identity management, you will need to be doing it right in the enterprise first. So, if you do not have a mature identity management environment in your enterprise, start there.

Cloud identity management: identity sources

The next question you need to answer is what sources of identity will accept? Will you, or even can you by policy/contract/regulation, rely on identities that others have asserted? Do you require all identities to be something that you have vetted? The answer to these questions will have a fundamental impact on how you proceed. The former is typically associated with federated identities, whereas the latter is a local identity store. The advantage of federated identities is leveraging the identity management aspects of the different organizations that are part of a federation. The disadvantage of federated identities is they require trust in those other organizations (more below). The trade-off between federated and local is management versus trust. As a side note, if you are looking at federated identities, there are two main standards that you will need to consider: Security Assertion Markup Language (SAML) and WS-Federation.

Cloud identity management: Who do you trust?

One of the issues with trust is likely to get down to how those other organizations actually assert identities, or validate the identities of their users. You should likely be much more trusting of an organization that validates their users' identities, as opposed to one that allows users to self-assert their identities. Further, if the federation is a limited community, it may have some inherent trust within it.

Think of organizational assertion as utilizing your corporate identities to authenticate to a partner. The partner is relying on the fact that your organization has vetted you and is assigned you an IDE and takes your organizations assertion of who you are. It's important to note that in order to enable this type of identity assertion, your enterprise IAM will need to be extended into the cloud.

Steps to take

Extending an organization's identity services into the cloud is a prerequisite for strategic use of on-demand computing services. Much of your decision will be determined by the type of cloud computing that you are planning on utilizing, public or private, as well as IaaS, PaaS or SaaS. These will have a significant impact on your ability to choose an IAM solution. Organizations looking at extending their enterprise into the cloud should to do the following for cloud identity management:

- Inquire of proposed cloud service providers to see what type of IAM integration they have with the services you are looking at using;
- Plan on utilizing organizational assertion of identities;
- Create a project to figure out how to extend your current enterprise IAM solution to your cloud services, most likely utilizing SAML;
- Extend your organization's IAM practices, processes and procedures to your cloud services.

Resources from CA Technologies

[Identity Governance: The Business Imperatives]

[Protecting Your Information - Top 10 Deployment Success Factors]

About CA Technologies

CA is one of the world's largest IT management software providers. Our software and expertise unify and simplify complex IT environments-in a secure way-across the enterprise for greater business results. We call this Enterprise IT Management (EITM)-our clear vision for the future of IT. It's how you can manage systems, networks, security, storage, applications and databases securely and dynamically. You can build on your IT investments, rather than replacing them, and do it at your own pace. Our more than 5,300 developers worldwide create and deliver IT management software that keeps our vision real. And we've taken our decades of experience solving complicated IT problems and developed practical paths for you to get from where you are today to where you want to be.