

TECHNOLOGY BRIEF

January 2012

CA Technologies point of view: Content-Aware Identity and Access Management

Sumner Blount

Security Management, CA Technologies

agility
made possible™



table of contents

EXECUTIVE SUMMARY	3
<hr/>	
SECTION 1: Challenge	4
<hr/>	
SECTION 2: Content-Aware IAM	5
<hr/>	
SECTION 3: The CA Technologies architecture for Content-Aware IAM	8
<hr/>	
SECTION 4: Scenarios for Content-Aware IAM	11
<hr/>	
SECTION 5: Conclusions	14

executive summary

Challenge

There are several key drivers for most IT organizations today. First, they must reduce risk, and maintain privacy of corporate and customer information. Second, they must comply with regulatory and industry mandates. Third, they must improve operational efficiencies. And, finally, they must enable the business for growth.

A key requirement for each of these areas is the ability to efficiently manage all your user identities, and control their access to critical systems, applications, and information. But, it's not enough to merely control users and their access to these resources. Stopping at the point of access gives you less control—you must also control information usage after it has been accessed. The protection of information from both unauthorized access and improper usage is essential in order to provide the compliance and security that your business, your customers, and your partners rightly demand.

Traditional identity and access management systems often cannot easily handle these increasingly complex requirements. New models of identity systems are required.

Opportunity

Content-Aware Identity and Access Management from CA Technologies helps you strengthen and automate your security controls, because it enables you to control user identities, their access, and their information usage. While traditional identity and access management stops at the point of access so organizations have less control, CA Technologies goes beyond this by providing control starting at the user all the way to the information and how it is used. This granular control helps you prevent misuse of your data, including improper disclosure or theft from the organization—improving your compliance posture and protecting your critical information assets.

Benefits

Content-Aware Identity and Access Management from CA Technologies helps you respond to the key IT drivers above. It helps to automate identity-based security processes (such as user provisioning, entitlement certification, etc.), which increases efficiency and reduces IT costs. It strengthens security and reduces risk. It helps simplify compliance and reduce audit effort and costs. And, it enables you to more quickly deploy new online services and applications, thereby increasing your business agility so that you can respond quickly to market and competitive events. It provides you the control you need to confidently move your business forward.

Section 1: Challenge

The challenge of identity and access management

Identity and access management (IAM) has been an important technology area for most enterprises, and continues to grow in both use and importance.

IAM provides a number of key benefits when successfully deployed. It provides the foundation for effective security by helping to enforce that all users have only the appropriate level of access rights to all protected resources—systems, applications, and information. It protects these resources by enforcing policies that specify who can access each resource and the conditions under which access is allowed. It helps lower administration costs by automating many security processes, such as the provisioning and deprovisioning of accounts and access rights. IAM can also enhance regulatory compliance by automating your security controls and simplifying your compliance audits. Finally, it can help you quickly deploy new online services, as well as support secure partner ecosystems for improved business growth. Reduced risk, reduced costs, improved compliance, and business enablement—these are very powerful benefits that IAM can provide.

But traditional IAM systems have focused on two areas simply because these were viewed as the most critical to most companies—controlling user identities and controlling user access to systems and applications. The first area relates to managing user identities and their roles, provisioning users for access to resources, maintaining compliance with identity and access policies, and monitoring user and compliance activity. Controlling access involves enforcing policies relating to access to systems, web applications, and information.

Limitations of traditional IAM systems

Despite the important advantages that these IAM systems provide, there are several key problems that they cannot adequately address:

- **They protect information access but not usage** Traditional IAM controls access to key applications and information, but they don't control what you can do with the information once you get it. It is common for someone to be authorized to access certain data, but there are some actions that they could take with that data that need to be prevented. For example, you might allow them to view it, but not email it to someone external to the company. Traditional IAM systems simply do not provide sufficient granularity of their access policies to be able to provide this protection.
- **Classification of information is difficult and manual** Every organization has sensitive information that needs to be classified as such. Policies on how data should be classified are generally non-existent or poorly communicated. Also, data is often difficult to classify because of its inherently dynamic nature. Information resources often get misclassified upon creation for either of these reasons. As a result, potentially very sensitive information might not be correctly classified, and is therefore subject to improper use.

- **Information security is usually not identity-based** When policies to enforce information usage are developed, it is important that violations of these policies can be associated with specific identities. It is insufficient to simply be notified that an information usage policy was violated—it must be not only prevented before it occurs, but also must be traceable to a specific individual.
 - **The focus is often on controlling access, rather than on facilitating appropriate access quickly and efficiently** “Keeping the bad guys out” is essential for effective security. But, allowing appropriate people to share information easily and dynamically is also essential for enabling the efficient operation and growth of the business.
-

Section 2:

Content-Aware IAM

Expanding the scope of IAM: Content-Aware IAM

At its most basic, identity and access management should help you answer the most important questions relating to your users:

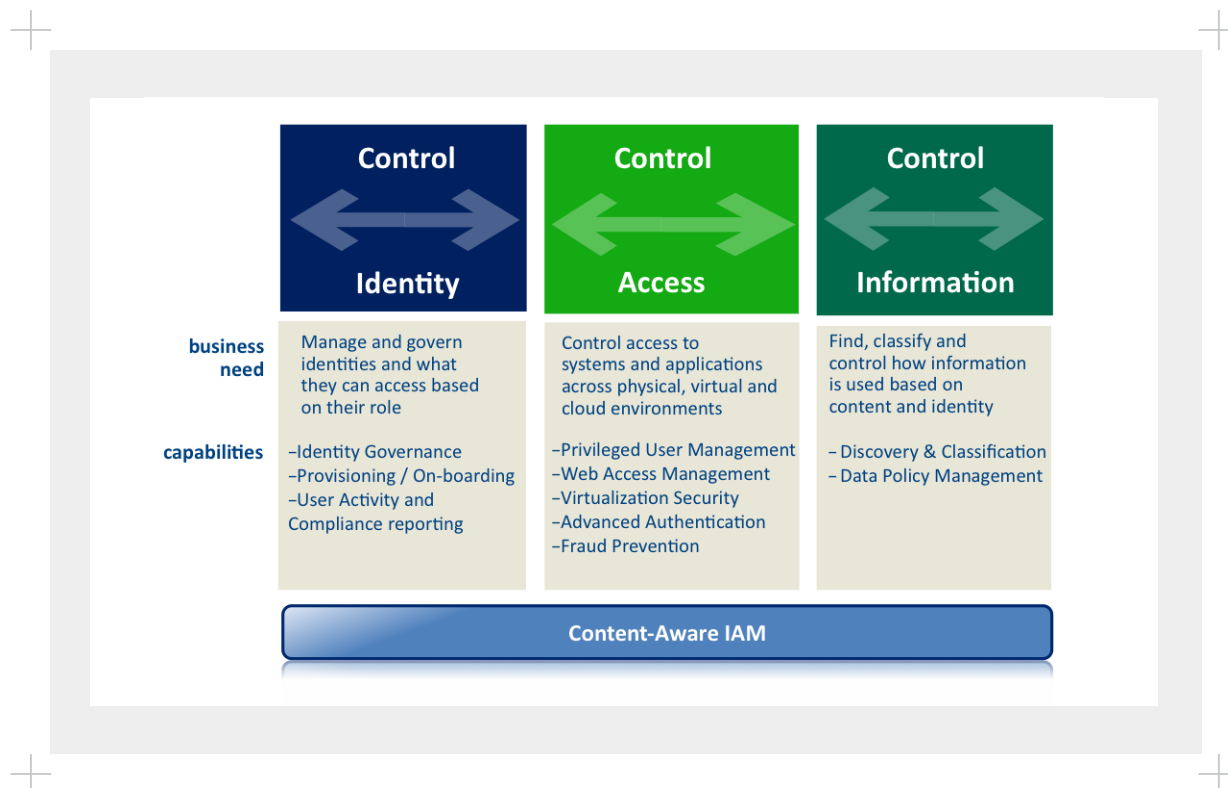
- Who has access to what?
- What can they do with that access?
- What can they do with the information they obtained?
- And, what did they do?

In order to answer these questions, you need to be able to effectively manage and control three areas, as follows:

- **Control identities** Manage user identities and their roles, provision users for access to resources, maintain compliance with identity and access policies, and monitor user and compliance activity.
- **Control access** Enforce policies relating to access to systems, web applications, and information. Provide management of privileged users to avoid improper administrator actions. Provide flexible, strong, and risk-based authentication capabilities so as to help identify and prevent fraudulent activities.
- **Control information** Discover and classify sensitive corporate information, and enforce usage policies relating to this information.

The following graphic highlights these key areas and indicates the capabilities that are essential for each one.

Figure A.



What is Content-Aware IAM?

The essence of Content-Aware IAM is the ability to manage all of the areas defined above: identities, access, and information usage. Controlling identities lets you efficiently manage your users, their roles, and their access rights across the enterprise. Controlling access allows only properly authorized individuals to gain access to your critical systems and applications. But, this is not enough for a unified approach to security and compliance. Controlling information usage is critical because it helps to prevent the inappropriate theft or disclosure of confidential enterprise or customer information. This capability enables you to create policies that define certain classifications of data and the operations or actions that will not be permitted on that data.

Content-Aware IAM is not a stand-alone technology, but an integrated set of IAM components that create a unified solution. This implies that entitlement management, role management, provisioning, and even access management are all “content-aware” in the sense that their functionality is integrated with, and impacted by, the classification and usage of the information. We’ll see in a later section how this works, and the benefits it provides.

Many traditional vendors tout that their solutions are “context aware,” which some people confuse with the concept of content-aware. “Context aware” implies that certain contextual attributes are used to enhance the granularity of the enforcement of access policies. For example, contextual attributes could

be: the location of the user, the authentication method used, the user's recent activity, or the time of day. Example: access to an enterprise application might be denied if the user is using their home computer, or attempting the access on a weekend. Content-Aware IAM goes farther, and uses not only context but the information content to determine if the operation should be allowed. Example: you might have rights to access a specific customer record but not their financial information (content), and you can email that record to Finance, but not to anyone else. Content-Aware IAM, coupled with contextual enforcement, provides a very powerful and innovation approach to protecting your critical assets.

Data loss prevention and information control solutions should be identity-centric so that a common model of roles and entitlements exists across the IAM environment. This implies, for example, that when a user changes roles, their information usage rights (in addition to their access entitlements) will also immediately change, and any rights associated with their previous role will be terminated.

The benefits of Content-Aware IAM

The benefits of IAM are well-known and significant: reduced risk, improved efficiencies, simplified compliance, and improved business enablement. Content-Aware IAM is a natural progression of the evolution of IAM technology. But, it provides some important benefits over a traditional IAM approach, including:

- It provides additional protection by protecting information from misuse or disclosure—information of many types (customer information, intellectual property, nonpublic information, etc.) can be protected against communication outside the enterprise boundaries, or transmittal to an unauthorized device (e.g., a USB drive).
- It enables expansion of the business in a secure fashion—moving security closer to the data dynamically increases security. For example, certain data might be classified as “Secret,” so only those people with “Secret” clearance can access that data. Even if someone was given inappropriate access to a system, they could still not access the data. This enables the business to grow without sacrificing security.
- It provides auto-classification of data—data can be automatically classified through the use of generic descriptions that define both the characteristics of sensitive data and its level of sensitivity. For example, data such as source files, SSNs, health records, etc. can be described so that this type of data can be found and classified across the enterprise.
- It enables information content and usage to play a role in the other key IAM processes, such as provisioning, identity certification, user activity reporting, and access management. If you know how a person has used sensitive information in the past, it can help you more appropriately determine the roles and entitlements that this person should have. Or, you can use the classification of the data to determine whether an access request for it should be granted. Content-Aware IAM can provide improved policy enforcement and therefore reduced IT risk.
- Information use policy enforcement is identity-based, so that all actions are associated with an individual. This supports compliance and allows quick remediation action.

Section 3:

The CA Technologies architecture for Content-Aware IAM

The Content-Aware IAM suite from CA Technologies includes a broad set of integrated solutions that help control the key aspects of your IAM environment. Full descriptions of each product are at www.security.com. The key categories, the component products, and their capabilities include:

- **Control identities (CA GovernanceMinder™, CA IdentityMinder™, CA User Activity Reporting)** Control identities by managing and governing what they can access based on their role. It also includes user activity and compliance reporting.

IAM from CA Technologies provides complete identity lifecycle management that addresses the evolving requirements associated with ensuring users have appropriate and timely access to the applications, systems, and data they need while establishing appropriate processes and controls to minimize security risk. *Identity Governance* supports controls to prevent business and regulatory policy violations (such as segregation of duties) and automates the process of validating user access to reduce security risk. *Provisioning* enables the automation of processes for on-boarding, modifying, and off-boarding users and their associated access. *Self-service* enables end users to initiate provisioning actions, password management, and related processes. *Role Management* efficiently represents users and their required access (including roles, policies, access rights, etc.) as a foundation of unified identity processes. Finally, *User Activity and Compliance Reporting* provides improved security and easier compliance through reporting on compliance and user activity events.

- **Control access (CA SiteMinder®, CA ControlMinder™, CA AuthMinder™, CARiskMinder™)** Control access to systems and applications across physical, virtual, and cloud environments.

IAM from CA Technologies provides extensive capabilities to control access to protected systems and applications, across a range of platforms and environments. *Web Access Management* provides a centralized approach to the enforcement of policies that determine who can access your critical online applications, and the conditions under which that access is allowed. Centralizing application access enforcement outside of the applications themselves helps to simplify and reduce the cost of security management, and to promote consistent security enforcement. It also provides web single sign-on for increased productivity and reduced Help Desk costs. *Federation* provides for secure access to external partner applications and data to enable partner ecosystems that support your business growth. *Privileged User Management* provides granular control over what your administrators can do on your key systems. It significantly enhances the security provided by native operating systems. It secures both physical and virtual systems, and securely tracks, logs, and reports all privileged user activities. *Virtualization Security* helps protect your systems and applications that are deployed in a virtual environment from attack or misuse, either externally or from cross-VM activities. *Advanced Authentication and Fraud Prevention* provide flexible capabilities for improving the strength of your user authentication, including risk-based authentication to help identify and prevent attempted fraudulent activities. It also enables you to avoid the high cost and reduced user convenience of hardware tokens, while improving your overall security.

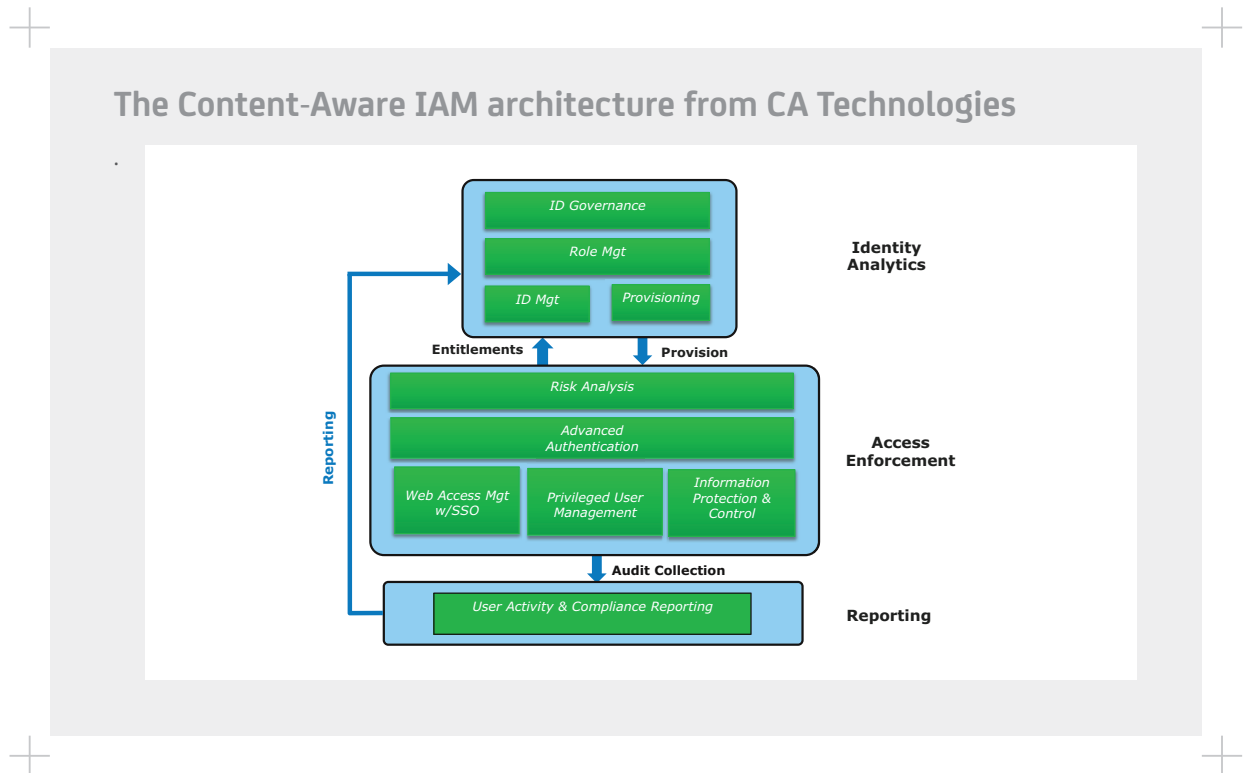
- **Control information (CA DataMinder™)** Find, classify, and control how information is used based on content and identity.

CA DataMinder identifies sensitive data across the enterprise in real time and determines whether or not end users are using that data in accordance with various security and regulatory mandates. It identifies and classifies all sensitive data; examples include personally identifiable information (PII), intellectual property (IP), and nonpublic information (NPI). It controls sensitive data at all locations: at the endpoint, on the server, on the network, or stored across the enterprise.

Many companies have faced the negative effects of sensitive information being emailed outside corporate boundaries. Sometimes this comes from malicious insiders, but often it's simply a careless but dangerous act. CA DataMinder can analyze all email to identify and prevent sensitive information from being sent to the wrong person. The result is reduced risk of improper information disclosure.

The following graphic highlights information flow between the IAM components. It also highlights how the Classification Service provides information about information content to each component, resulting in increased granularity of access and usage enforcement, as well as content-aware role management.

Figure B.



An important strength of Content-Aware IAM from CA Technologies is the level of integration among the components. This level of integration helps to simplify administration and foster consistency of interfaces across all components. And, simpler administration means lower costs.

In addition, these products can improve security for new or emerging service models, such as virtualized or cloud environments. As you take advantage of virtual computing, you will want to ensure that the physical machines that host your virtual environments are fully protected from attack or cross-VM access. In a similar way, as you move to cloud computing, you need to make this transition as easy and secure as possible. Content-Aware IAM from CA Technologies facilitates your ability to make this transition securely so that your business can take advantage of these new and important service and technology models.

Content-Aware IAM from CA Technologies provides important capabilities to leverage information content knowledge to improve overall security, including:

- **Content-Aware information classification** Data needs to be classified according to the model of data sensitivity of each organization. For example, there should be major categories of information sensitivity (examples: corporate confidential, customer private, intellectual property, nonpublic info, etc.), as well as levels of sensitivity within each category. This process today is usually manual, highly time-consuming and error-prone, and often completely omitted. CA DataMinder can analyze and classify sensitive information (using either static or dynamic analysis) and then control its usage to prevent misuse. Traditional IAM vendors do not provide this important capability, and this is the foundation on which Content-Aware IAM is based.
- **Content-Aware provisioning** The integration of CA IdentityMinder and CA DataMinder provides true identity-centric information protection. CA IdentityMinder can directly provision, de-provision, and modify users into the CA DataMinder user hierarchy. As users' roles change, CA IdentityMinder passes those changes into CA DataMinder, which ultimately changes each user's data usage entitlements.
- **Content-Aware web access management** CA SiteMinder can use information classification in its policy enforcement decisions, thereby providing you with increased granularity in how you define your access and usage policies. This enables CA SiteMinder to make the access decision based not only on whether the user is authenticated and authorized for access, but also on the sensitivity of the resource as determined by the DLP Classification Engine. So, for example, access to a document posted in a Sharepoint portal by mistake can be prevented dynamically by CA SiteMinder based on the sensitivity of the data.
- **Content-Aware role management** Information usage policies should be both identity- and role-based, because individuals who share a given role are very likely to have the same usage entitlements. The usage policies of CA DataMinder will be integrated with the role management model and associated security policies of CA GovernanceMinder, so that information usage policies can be tied directly to the business roles that are associated with these policies. This helps eliminate ad hoc approaches to business roles and results in more efficient management of users and their usage policies.
- **Content-Aware identity certification** Many regulations and best practice standards require regular management certification of user entitlements to confirm that each user has the appropriate access privileges. Many organizations don't regularly review their user entitlements, and those that do generally do it manually, resulting in increased risk and inefficient processes. Automated identity certification not only increases efficiency by automating a typically manual process, but it also helps to identify and eliminate cases of over-privilege among the user population. With the integration of CA DataMinder and CA GovernanceMinder, identity certification will include a validation of not only an employee's access rights, but also their information usage entitlements.

- **Content-Aware compliance reporting** When information access and/or policies are violated, it is essential that this becomes visible to security or compliance managers so that they can take quick remedial action, and is included in compliance reports so that the overall compliance profile of the organization is known. To provide this capability, CA User Activity Reporting (an add-on component) will capture the results of attempted usage policy violations that are prevented by CA DataMinder and include this information, correlated with other relevant access activity, in compliance reports. Content-Aware compliance reporting provides a more accurate view of the state of information usage compliance, and can be used in conjunction with other identity-related compliance information to simplify and reduce the total costs of compliance audits.

Section 4: Scenarios for Content-Aware IAM

Let's consider some very common and instructive scenarios to illustrate how an integrated approach to Content-Aware IAM can enforce security policies and help automate security processes. These cases are not exhaustive, but they are representative of some of the important security and efficiency benefits that can be gained.

Provisioning of users based on roles and policies

Bob Butler was hired as a software developer at Forward, Inc. When he was hired at his previous company, it was two weeks before he had access to all of the systems and files that he needed to do his job. During that process, all his accounts and access rights had to be manually created, but only after a paper form was signed by each system admin and sent back to the IT admin. During this time delay, Bob became frustrated because he wasn't as productive as he needed to be. In addition, during the four years Bob was there, he changed projects several times, and each time he never lost his access privileges for the previous projects and roles. As a result, when he left, he had accumulated significantly more privileges and accounts than he needed.

But, upon arrival at Forward, CA IdentityMinder and CA GovernanceMinder were used to automate the creation of his accounts and access rights and gain upper management approval through workflow processes. This process was done immediately and no paper approval forms were required. So, Bob was productive immediately, saving him much frustration and time. In addition, as his role and project responsibilities changed over the next three years, his access rights were automatically changed to reflect his new responsibilities, so that he did not have more access than he needed for his current role. Finally, CA GovernanceMinder automated the certification of his entitlements so that inadvertent over-privileges were detected and corrected quickly.

Protection of confidential records

The protection and privacy of medical records is a prime example of the importance of controlling not only access to information, but usage of that information. It is, for example, essential for HIPAA compliance.

Stan is a nurse at Metro Hospital. As such, he has the rights to see the medical records of patients for whom he is the assigned nurse. The hospital wants to allow access to these records only from approved stations within the nurses' area, and requires strong authentication when these records are accessed. Lastly, because of HIPAA concerns, the hospital requires that no online medical records be communicated outside the hospital's IT environment. Unfortunately, for his own nefarious reasons, Stan wants to

steal some of his patients' medical records from the hospital. Here's how Content-Aware IAM from CA Technologies would help protect Metro Hospital:

- Stan connects to the hospital network from his home PC and logs in. He tries to access his patients' records, but CA SiteMinder determines that he is not located at an approved PC (within the nurses' area), and denies his attempt. This failed attempt is logged, and the IT security manager is notified.
- The next day, Stan logs into the PC in the nurses' station. He attempts to access the records of a patient for whom he's not the attending nurse. CA SiteMinder passes information about Stan as context to the application, which then determines that he is not the attending nurse for this patient, and therefore denies access to this patient record.
- He then attempts to access his own patient's record. Because this requires extra security, CA SiteMinder authenticates him using his CA ArcotID™ software token, and access is allowed. He now has authorized access to this data, but he wants to use it for unauthorized purposes.
- He copies these medical records into an Excel file, and emails it to his own Gmail account. CA DataMinder analyzes the attached data that is being sent in his email, and determines that it contains patient numbers. Because there is a data usage policy that prevents this type of data from being transmitted externally, the email operation is denied, an alarm is raised to the IT security manager, and a record of the event is put into the log file. If Stan attempts to copy the information to a restricted device or email it to an unauthorized internal individual, the results would be the same. His attempt to steal this sensitive information has been defeated in every case.

Inadvertent sharing of protected information

In many cases, a violation of information usage policy is unintentional. That is, some user may transfer information to a third party that is perfectly acceptable, but which includes some data that should not be transferred.

Pierre is a finance manager at a luxury retailer in Paris. This retailer has a partnership with a few key partners in which they jointly market their products to their high-end customers. In order to develop these joint marketing campaigns, Pierre has been asked by his marketing manager to send the Paris-based customer list to the partner so they can analyze the range of customers and determine how to market to them. However, the standard customer database contains credit card information that not only cannot leave the company, but should not even be communicated to anybody internally except a select few finance employees, such as Pierre. Pierre is not aware of this, and is attempting to do an otherwise appropriate business operation.

Pierre attempts to access the Paris-based customer list and the request is allowed. He then downloads this customer information into an Excel file, and puts it on a network Share drive, to which he has given the partner access. Later, CA DataMinder performs a network scan and discovers a new file there, and a scan of the file determines that it contains protected information. When the partner accesses the Share drive and attempts to copy the data, CA DataMinder enforces the usage policy by preventing the action, and informs the compliance manager of a potential regulatory or policy violation. In this case, sensitive information was protected from disclosure outside the company.

Protection of intellectual property

Jerry is a software developer working on a strategic application for 2Big2Fail, Inc. Because he is not a Senior Developer, he can only access portions of the large set of source files. These entitlements are determined by his organizational role (CA GovernanceMinder) and enforced by CA SiteMinder.

Jerry is disgruntled and has accepted a job with a competitor. He is going to try to steal the application's source code, because he wants to bring it to his new company. He attempts to access the key source files for this application, but SiteMinder denies access based on his role entitlements. Next, he attempts to go directly to the server where these files reside by using a Root password that he has used in the past. But, the Privileged User Password Management capabilities of CA ControlMinder prevent this access, as well as logging his failed attempt.

Undaunted, Jerry copies the source files that he is authorized to use to his hard drive and tries to copy them to a USB device. But, CA DataMinder analyzes the data in the transfer, determines that it is a source file, and prevents the operation. Next, Jerry tries to email the files to his Gmail account, which CA DataMinder also prevents. Finally, he attempts to FTP the files to his home computer. CA DataMinder prevents this action also, and in all these cases generates an alarm and logs the attempt. Not surprisingly, this attempted policy breach is identified quickly and Jerry becomes an ex-employee even sooner than he expected. As he is walked out of the building, all his accounts (across many systems) and access privileges have already been automatically terminated by CA IdentityMinder.

Information protection due to improper access

Carl is a manager at Forward, Inc. and has access to an internal Sharepoint site for his group. Another employee mistakenly posts a file on this site that contains customer financial information. One day, while scanning the Sharepoint site, Carl notices this new file and attempts to open it. Before CA SiteMinder authorizes Carl's access to the file, it calls the CA DataMinder classification service to see if the file that Carl is accessing is sensitive. CA DataMinder checks the content against its policies and determines that there is confidential information on the SharePoint site that Carl shouldn't have access to, based on his role. SiteMinder then uses this classification to block Carl's access to the information. The combination of CA SiteMinder and CA DataMinder prevented another compliance violation.

The result—a potentially serious breach of confidential information is prevented.

Summary of use cases

These examples highlighted relatively common occurrences at many organizations. In these examples, we see some compelling benefits of Content-Aware IAM. In the first example, common security processes were automated, thereby not only increasing efficiency, but most importantly improving security and simplifying compliance. In the other scenarios, we see the benefits of providing fine-grained control of what each user can actually do with the information that they obtain, rather than have the policy enforcement end at the point of access. Because the damage caused by inappropriate disclosure or theft of sensitive information can be so great, and because even well-intended employees sometimes make mistakes related to the use of this information, a solution that can help prevent these situations is essential for a robust security approach.

In summary, robust security and compliance requires more than what traditional IAM can offer. Content-Aware IAM provides these enhanced capabilities that offer compelling benefits to large IT organizations.

Section 5:

Conclusions

Identity and access management has been providing compelling benefits to many organizations for several years. But, these systems generally provide control only down to the point of access, and do not allow you to control what can be done with the information once it has been obtained. This is a significant limitation of these platforms, because it does not completely prevent misuse or inappropriate disclosure of your sensitive information.

Innovative Content-Aware IAM solutions from CA Technologies extend this capability so as to provide control down to the data level, thereby providing you with more control over what users can do with your critical information. This integrated solution can also help reduce your IT risk, automate key security processes for increased efficiencies, and enhance your overall compliance posture.

IAM from CA Technologies provides you with the flexibility to choose the deployment model that fits your business and security requirements. Our core IAM capabilities are offered as cloud services (under the name CA CloudMinder), hosted in large and secure data centers and managed by CA Technologies experts. You can adopt cloud-based IAM services according to your own needs and timetables, starting with a completely on-premise solution and then migrating certain components to the cloud as your needs and security considerations dictate. This approach offers you very high flexibility and enables you to increase your overall business and IT agility.

The goal is to move your business forward, securely. Content-Aware IAM from CA Technologies provides the foundation to help you achieve this goal.

To learn more about the Content-Aware IAM architecture from CA Technologies, visit ca.com/iam.

CA Technologies is an IT management software and solutions company with expertise across all IT environments—from mainframe and distributed, to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 rely on CA Technologies to manage their evolving IT ecosystems. For additional information, visit CA Technologies at ca.com.