

SOLUTION BRIEF

Content-Aware Identity and Access Management | February 2012

how can Content-Aware Identity and Access Management give me the control I need to confidently move my business forward?

agility
made possible™





Content-Aware Identity and Access Management (IAM) solutions from CA Technologies enable you to control user identities, access, and information use. You can achieve more effective compliance, reduce IT risk, and expand your customer and partner relationships to help grow your business.



executive summary

Challenge

Managing the identities and access rights of those inside and outside the enterprise has become a primary concern for IT organizations today. Reducing IT risk, meeting regulatory requirements, and increasing efficiencies are all central to your business. At the same time, you need to develop new and innovative ways of expanding your business, as well as leverage new service models such as cloud computing.

Opportunity

Content-Aware IAM from CA Technologies is a comprehensive and scalable solution for managing user identities, access, and information use. It protects your critical IT resources, from the Web to the mainframe, including virtualized and cloud environments. It also provides automation of security and compliance controls, increasing efficiency and simplifying compliance audits.

Benefits

Continuous and sustainable regulatory compliance—through automation of security controls and more effective proof of controls—is a primary benefit of the Content-Aware IAM suite from CA Technologies. But equally important are business benefits such as reducing cost and improving efficiencies by automating and centralizing identity management, reducing risk by improving security for critical IT resources and information, and enabling greater business performance by improving competitive responsiveness, customer online experiences, and partner ecosystems.

Section 1: Challenge

Reduce risk, improve compliance, and grow your business

Your organization faces significant security challenges in today's world, where protecting vital business data can be an expensive and daunting proposition. For example, you must proactively protect your critical applications, server-based resources, and information from unauthorized access. You must also ensure that your data does not get communicated inappropriately, either internally or externally. You must comply with governmental and industry regulations as well as internal security or business policies. Most importantly, you must ensure continuous business operations by mitigating risk at virtually every level of your organization—all while maintaining budgets and achieving operational efficiencies.

In case this isn't enough of a challenge, you need to also be able to develop and introduce new online services quickly and securely, as well as extend the reach and effectiveness of your partner ecosystem. Only by doing this will you be able to meet the growth objectives for your business.

Further, you must continue to evaluate and adopt promising new service models or technologies, such as cloud computing or virtualization. So, the security solutions that you might choose must offer comprehensive capabilities that enable you to leverage these new technology approaches.

Sound identity and access management (IAM) provides the foundation for effective security by ensuring all users have only the appropriate level of access rights to all protected resources, and that those rights are enforced. It helps lower administration costs by automating many system administration functions, as well as the provisioning and deprovisioning of accounts and access rights. IAM also greatly enhances regulatory compliance by automating your security controls and simplifying your compliance audits. Finally, it can enable business growth and help you solidify existing customer and partner relationships, as well as more effectively develop expanded relationships.

The key questions that must be answered by any identity and access management solution are:

- Who has access to what?
- Are they who they claim to be?
- What can they do with that access?
- What can they do with the information they obtained?
- What did they do?

By answering these questions, you can identify and remediate inappropriate access rights, as well as ensure that your IT assets are protected.

This solution brief will present the innovative solutions that CA Technologies provides for IAM, and highlight how these solutions can greatly simplify your compliance efforts, reduce your IT risk, and help you reduce your total IT costs.

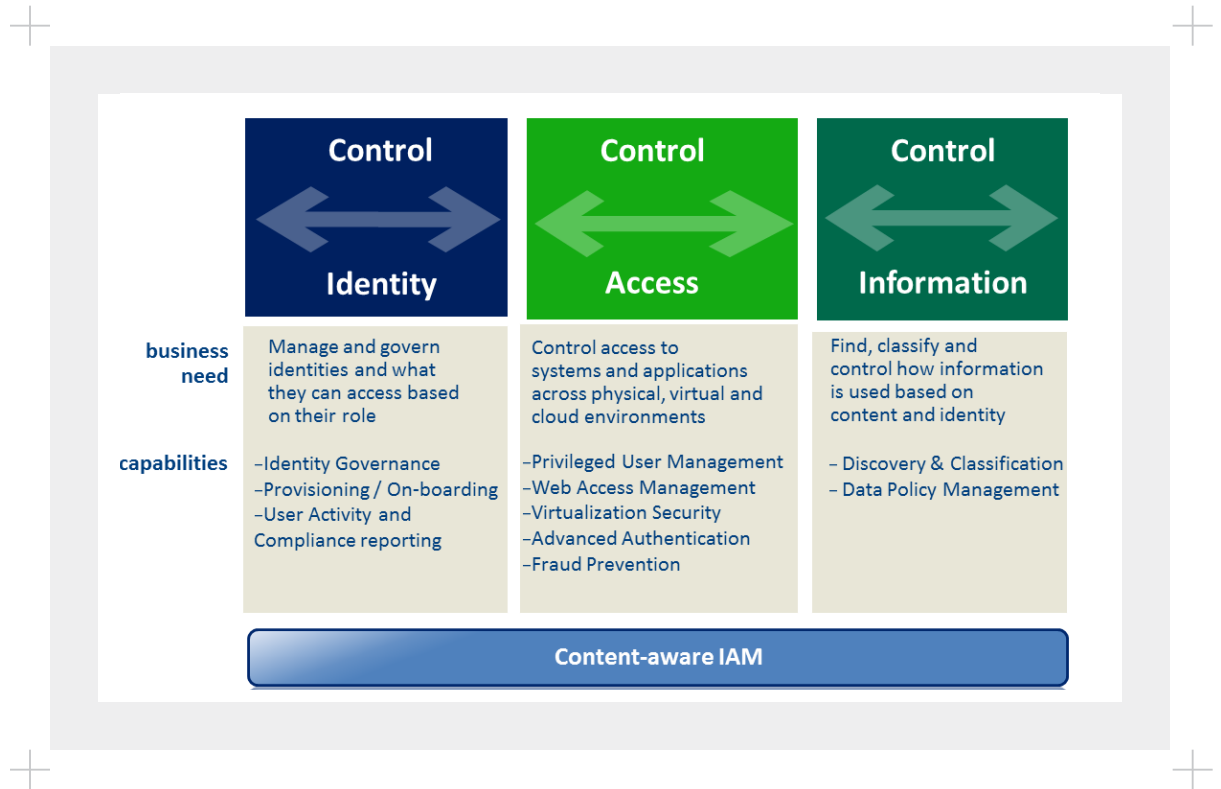
Section 2: Solution

Meeting your critical identity and access management challenges with Content-Aware IAM from CA Technologies

Effective identity and access management cannot exist in isolation. It should be viewed as part of an overall strategy that can serve to reduce overall IT security risk, as well as improve efficiencies and productivity across the environment. The strategy of CA Technologies is to provide all the key capabilities to enable enterprises to meet their IT security needs, as well as to integrate these capabilities with other management functions such as operations, storage, and service management.

There are three key issues that need to be addressed when planning a strategy for identity management, as represented in the following graphic:

Figure A.



To ensure effective security, you must:

Control identities Manage user identities and their roles, provision users for access to resources, ensure compliance with identity and access policies, and monitor user and compliance activity.

Control access Verify user identities and enforce policies relating to access to web applications, systems, system services, and key information. Also, provide management of privileged users to avoid improper actions.

Control information Discover, classify, and prevent leakage of confidential corporate and customer information.

These three elements are essential for a comprehensive approach to IAM security. Unfortunately, most IAM vendors provide some elements of only the first two categories—but they don't enable you to provide control down to the data level. CA Technologies uniquely provides the complete solution for all these critical areas. The following sections describe the broad and integrated capabilities that Content-Aware IAM from CA Technologies provides.

Control identities

Most IT organizations struggle to keep up with the explosion in the number of users of various types, the complexity of managing access rights for all these users, and the need to prove to auditors that each user has only the appropriate level of access. Unfortunately, many approaches to these problems amount to poorly coordinated manual processes that expose organizations to higher costs and risks. Poor management of user identities also negatively impacts users, as inefficient processes reduce user satisfaction and productivity.

To eliminate these inefficiencies, the entire identity lifecycle of users needs to be automated. Through capabilities such as automated provisioning and workflow processes, enterprises can gain significant efficiencies, because users become more productive, and administrators are freed up to focus more on activities that will meet the needs of the business.

CA Technologies provides a comprehensive and integrated approach to identity lifecycle management. The CA Technologies solution includes capabilities for identity governance, role management and mining, and user provisioning. This end-to-end approach includes the initial creation of user identities, the allocation of accounts and access entitlements that they require, the ongoing modification of these entitlements as the user's role changes, and timely removal of these rights and accounts upon termination.

Another key problem in managing users relates to user activity and compliance reporting. Many organizations are drowning under excessive amounts of system log information. Manual processing of this information not only wastes huge amounts of time, but hinders effective identification of significant security events. In addition, many regulations have requirements for collection, storage, and reviewing of system log data that are almost impossible to meet with a purely manual approach. To effectively comply with these requirements, you must have an automated and repeatable process for identifying and addressing policy and controls violations.

The CA Technologies solution for user activity and compliance reporting (User Activity Reporting Module) automates the collection, normalization, and filtering of user activity log data across your IT environment. This capability alone can greatly increase your administrative efficiency, reduce IT costs, and free up your team for more business growth-oriented activities.

Unlike other products that focus purely on building up the speed of log data collection, this module is designed to help you answer the key questions that matters to your PCI, SOX, or HIPAA auditors—accurately and fast. It simplifies and speeds compliance with over 400 reports that are already mapped to privacy and compliance regulations, and IT control frameworks and standards. It also uniquely allows you to keep up with constantly changing regulatory reporting requirements with regular, automatic compliance report updates.

The products from CA Technologies that enable you to effectively control user identities include:

- **CA IdentityMinder™** Provides identity administration, provisioning/de-provisioning, user self-service, and compliance auditing and reporting. It helps you establish consistent identity security policies, simplify compliance, and automate key identity management processes.
- **CA GovernanceMinder™** A business-oriented solution that leverages analytics and workflow to automate identity governance processes, including entitlements cleanup, certification, segregation of duties, and role management. By automating these processes and controls, it helps you reduce risk, improve compliance, and increase operational efficiency.
- **CA User Activity Reporting** Provides user activity and compliance reporting usage across physical, virtual, and cloud environments.

Control access

Controlling access to critical enterprise IT resources is required not only for effective compliance, but also to protect shareholder value, customer information, and intellectual property. Without effective user authentication and access policy enforcement, improper access (either intentional or inadvertent) can have disastrous effects. There are three important areas to consider:

- Controlling access to web-based applications and services
- Controlling access of privileged users to information, applications, and services
- Advanced authentication

Web access management Organizations today face two seemingly contradictory imperatives. In order to boost performance and revenues, they must expand their reliance on the Internet and web applications that connect them with their customers, partners, and employees. On the other hand, an organization that opens up its systems to potentially millions of users inside and outside the enterprise also exposes its applications, networks, and data to significant risks, which can jeopardize the whole organization. Many organizations are reluctant to take advantage of the business growth benefits that can accrue from such approaches as identity federation and service-oriented identity because of security concerns.

CA SiteMinder®, the industry-leading web access management product for over fifteen years, provides an essential foundation for user authentication, single sign-on, authorization, and reporting. It enables you to create granular access policies that can control access to critical applications based on a flexible set of static or dynamic criteria. This flexibility makes it much easier to control user access to your applications, and helps eliminate the need for security-related code within each application itself. The result is faster application development and greatly reduced maintenance and administrative costs.

CA SiteMinder has been successfully deployed in some of the largest and most complex IT environments in the world. It has been proven to scale to millions of users with very high performance and reliability.

IAM from CA Technologies also includes capabilities for secure identity federation, to enable business growth through the expansion of comprehensive partner ecosystems. By allowing partners to securely access your applications, and vice versa, you can streamline value chains, but more importantly take advantage of growth opportunities available through integrated online partnerships. In addition, comprehensive security for SOA-based architectures is provided so that both web applications and web services can be protected in a common security infrastructure.

The CA Technologies products that enable you to effectively control access to web applications and web services include:

- **CA SiteMinder®** Provides centralized management and enforcement of user authentication, authorization, single sign-on, and reporting. It enables you to easily secure your key applications, improve your user experience, and simplify your compliance audits.
- **CA FedMinder™** Extends the capabilities of CA SiteMinder to federated partner relationships, which enables your organization to rapidly implement and manage partner ecosystems to help grow your business.
- **CA SiteMinder Web Services Security** Provides core authentication and authorization services and protects access to XML-based web services.

Privileged user management One of the most important areas of IT risk relates to privileged users (IT and security administrators). Whether inadvertent or malicious, improper actions by privileged users can have disastrous effects on IT operations and on the overall security and privacy of corporate assets and information. Therefore, it is essential that admins be allowed to perform only those actions that they are authorized for, and only on the appropriate assets.

In addition, admins often share (and sometimes lose) their system passwords, leading to an even larger risk of policy violations. And, when these users all log in as “Root” or “Admin,” their actions, as reported in the log file, are essentially anonymous. These conditions not only pose a significant security risk, but make compliance extremely difficult because improper actions cannot be prevented nor associated with the offending person.

What is needed is very granular access control on admin users. Unfortunately, native server operating system security does not provide sufficient control over who can access what resources, nor does it provide the granular auditing needed to meet compliance requirements.

The CA Technologies solution for privileged user management, CA ControlMinder™, secures servers by providing more granular entitlements for administrators across platforms than are offered by native operating systems. This facilitates easier compliance through unmatched granularity of policy-based access control and enforcement that includes segregation of duties. The solution controls who has access to specific systems, resources on those systems, and critical system services (for example, it is important that administrators not have the ability to turn off the system logging process in order to hide an inappropriate activity). It also simplifies management through a single user interface to manage all your server platforms.

The solution also supports extensive privileged user password management (PUPM), which helps provide the accountability of privileged access through the issuance of passwords on a temporary, one-time-use basis, or as necessary while providing user accountability of users’ actions through secure auditing. PUPM is also designed to allow applications to programmatically access system passwords and, in so doing, remove hard-coded passwords from scripts.

Advanced authentication User passwords are a source of great inconvenience for users and high costs for IT groups. In addition, they don’t provide adequate security for today’s critical applications and information. Two-factor authentication provides stronger security than passwords, but when implemented as hardware tokens, create significant cost and inconvenience issues themselves. CA AuthMinder is a versatile multi-factor authentication solution that eliminates these problems and helps provide increased security for your critical assets. It is integrated with CA SiteMinder so that it can transparently protect and verify Web users’ identities and help protect them from identity

theft and fraud without changing their familiar sign-on experience, nor requiring the possession of hardware tokens.

Another concern for all IT groups is the prevention of fraud or identity theft. Criminals have expanded their reach far beyond traditional targets of consumer banking and credit cards, looking to harvest valuable data that is accessible online. The challenge you face is how to instantaneously detect and block fraudulent activity before fraud losses occur, without affecting legitimate users. CA RiskMinder is a fraud detection and risk-based security system that helps prevent fraud in both consumer and enterprise online services. It also provides organizations the ability to determine and enforce different levels of authentication based on the acceptable amount of risk for the given transaction. Based on a risk score and company policies, organizations can enforce other forms of strong authentication, including the use of CA AuthMinder, depending on the user and the type of desired transaction.

The combination of CA AuthMinder and CA RiskMinder, in conjunction with the extensive authentication capabilities of CA SiteMinder, provide flexible and strong authentication for all users.

Control information

Enforcement of access control over sensitive information is only the first step in a comprehensive approach to information security. Once users have gained legitimate access to this data, many organizations have little or no control over what those users can do with it. These organizations often are not fully aware of all the places their sensitive information is stored, and have no protection against this information being exposed or disclosed to unauthorized people, either internally or externally. Something as simple as a social security number can have significant negative impact if disclosed inappropriately. For this reason, many organizations believe that their own employees pose a more serious data security threat, via either inadvertent or malicious behavior, than do outsiders.

CA DataMinder helps you get control of your massive amount of information, and most importantly, protect sensitive data from inappropriate disclosure or misuse. It protects data-in-motion on the network, data-in-use at the endpoint, and data-at-rest on servers and repositories. It enables you to define policies that define which data should be checked, what type of data item should be monitored, and the action to be taken if inappropriate activity is detected. It also includes a collection of prebuilt policies based on real business use cases that make quick deployment much simpler. It significantly reduces information security risk and makes it easier to prove compliance with certain security-related regulations and best practices.

On-premise or cloud – your choice

Some organizations like the “hands-on” benefits of a fully on-premise IAM deployment. Others understandably want to take advantage of the significant efficiency and agility benefits that cloud services can provide. But, most organizations tend to prefer a hybrid approach, outsourcing many services to the cloud while keeping more critical applications or information on-premise.

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 (named “CA CloudMinder™”), hosted in large and secure data centers and managed by CA Technologies experts. Other cloud identity services will be offered over the next twelve months. 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 CA Technologies difference: Content-Aware IAM

Identity and access management is not a new area of technology. It has already been reducing risk and improving efficiencies for thousands of enterprises around the world. There are many IAM vendors, and many of the large IAM suite vendors claim to offer essentially the same capabilities. So, how can someone decide which IAM vendor to choose?

The primary difference between IAM suite providers lies in the functional breadth of their offering, their support for a variety of deployment models and environments (including mainframe, cloud, and virtual), and the innovation that they bring to their product offering.

CA Technologies is unmatched in these areas. But, more importantly, IAM from CA Technologies provides capabilities that other IAM solutions do not. Traditional IAM 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 or fully 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 much more control over what users can do with your critical information. This integrated solution also helps reduce your IT risk, automates key security processes for increased efficiencies, and enhances your overall compliance posture. And finally, it enables you to confidently adapt new and emerging computing models such as virtualization and cloud computing.

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

Section 3: Benefits

Reducing IT security risk while improving operational efficiencies and enabling compliance

The Identity and Access Management solution from CA Technologies provides a complete and proven solution for protecting your critical IT assets across your entire environment, delivering these important benefits to IT organizations of all sizes:

Reduced security risk

Content-Aware IAM from CA Technologies helps ensure that your critical IT resources are protected, and that only properly authorized users can access them, and only in approved ways. It also allows you to manage and analyze security event information to quickly identify and remediate potential security issues, including improper disclosure or use of sensitive corporate or customer information.

Improved regulatory compliance

IAM products from CA Technologies provide your organization with the tools necessary to support continuous compliance with automated and centrally managed capabilities that help reduce costs while strengthening IT security controls. With comprehensive auditing, your compliance challenges become much simpler because you can provide the proof of controls and validate to auditors the effective operation of your established security controls. It also helps you automate your security compliance

processes, so as to help ensure compliance with your corporate or regulatory policies and to provide proof of compliance for easier and more efficient audits.

Reduced administrative expense and improved efficiency

IAM products from CA Technologies can help automate many of your key IT administrative processes, especially those related to managing user identities and access rights. Along with automated filtering and analysis of security log information, these capabilities can bring significant administrative efficiencies, thereby reducing your overall IT costs. They can also help to improve user and management productivity, since less time has to be spent in manual processes.

Improved secure business enablement

Customers and partners will only do business with your organization if they believe that you can provide a secure environment for their personal information. IAM products from CA Technologies can help your organization secure their applications, as well as deliver new applications and services more quickly to your customers and partners. These applications can provide a personalized and positive user experience, thereby strengthening your customer and partner satisfaction and helping you grow your business and partner ecosystem.

Section 4:

The CA Technologies advantage

Content-Aware IAM from CA Technologies enables you to control not only user identities and access, but also information usage. This important capability increases your overall security, and helps prevent inappropriate use of your corporate or customer information.

IAM from CA Technologies also offers a unique combination of advantages, including comprehensive reach across applications, platforms, and services; modular design based on common services and user interfaces; centralized and automated provisioning, workflow, and entitlement; and global scalability.

IAM from CA Technologies is also supported on the widest variety of platforms (from distributed to mainframe) and deployment models (including cloud and virtualized environments). You can deploy it on-premise, as cloud services, or in a hybrid environment, providing you with flexibility and agility in your use of IAM solutions. This enables our IAM solutions to provide a consistent and secure platform across your entire IT environment, including emerging technologies that you might adopt in the near future.

CA Technologies has been a leader in IT management for over 30 years, has over 1000 security customers, and is committed to continuing to bring innovative security capabilities to them. We have a very large and dedicated group of security experts who know how to make security deployments successful, and help our customers achieve very quick time-to-value.

Section 5:

Next steps

If you're finding that:

- You need more flexible capabilities in how you control and enforce policies on user access to your IT resources...
- You are concerned about fraudulent users gaining access to critical business information...
- You are struggling with the costs and effort required for compliance with relevant industry and regulatory requirements...
- Budgetary pressures are demanding greater efficiencies in your administrative functions...
- You are concerned about potential risks from excessive entitlements of your admins...
- You are interested in expanding your adoption of virtualized or cloud environments, but are concerned about the security or compliance impact...

...then take a look at Content-Aware IAM from CA Technologies. It's the most comprehensive and integrated IAM solution addressing security for web applications and web services, legacy systems, virtualized environments, and emerging cloud-based models.

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.