

Secure By Design: Building Identity-based Security into Today's Information Systems

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for IBM

March 2010



IT MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS AND CONSULTING

Table of Contents

Executive Summary	1
Securing the Rapid Pace of IT Evolution	1
Secure By Design.....	3
Security Built-In: A Closer Look at Today’s IAM Capabilities	3
The Benefits of Security “in Real Time”.....	4
A Comprehensive Approach	5
The Long View: Identity and Policy Lifecycle Management.....	5
The Service Option: Securing “IT as a Service”	6
IBM: Enabling Security By Design.....	7
EMA Perspective.....	9
About IBM	10

Executive Summary

Businesses have long focused their IT investment on new innovation and the expansion of capability. But as an alarming—and increasing—number of IT security incidents make clear, businesses must also make a similar strategic investment in information security and IT risk management.

Most organizations have invested in tools and techniques that add security to the environment, as well as technologies that focus on the protection of data itself. But what about building security *in*? What about an approach predicated not on reacting to the most recent threat, but on building a stronger environment that integrates risk control into its very fabric?

Most organizations have invested in tools and techniques that add security to the environment. But what about building security in?

Today's technologies for identity and access management offer not only an effective answer to this question, but value beyond risk control alone. When identity can be more directly integrated with business functionality, IT can deliver services more finely tuned to the individual—enabling the business to capitalize on opportunities that may otherwise be lost. This is in addition to the dependence that other security and policy control technologies have on identity, and also adds to a comprehensive approach to security management. Few other domains offer such a combination of business optimization and risk management integrated directly into the environment.

In this paper, ENTERPRISE MANAGEMENT ASSOCIATES® (EMATM) analysts examine today's security challenges in light of the opportunity to build security directly into information systems, and the role of today's finely grained technologies for identity and access management that make this more proactive approach possible. IBM is highlighted as an example of a leading vendor that offers a comprehensive range of capability in Identity and Access Management as part of a broad security portfolio for integrating security throughout modern IT systems. Business professionals will gain a new appreciation for how today's access management capabilities not only strengthen the environment against today's more serious threats, but build business value directly into IT as well.

Securing the Rapid Pace of IT Evolution

Recent years have seen nothing short of a revolution in IT. In little more than a decade, the Web has gone from an innovation to a critical vehicle for business. The Web itself has become vastly more powerful and enabling, with concepts such as Web Services transforming the implementation and integration of IT in Service Oriented Architecture (SOA). The explosion in virtualization technology has made the delivery of IT capability even more flexible, freeing information systems from many of their traditional physical constraints and optimizing the utilization of IT resources. This, in turn, has created new opportunities to further extend the value of IT, with concepts such as cloud computing enabling service providers—both outside and inside the enterprise—to deliver IT functionality on demand to large numbers of customers simultaneously.

But what happens when innovation outpaces the management of IT security risk? Organizations often embrace new capability in order to capitalize on new opportunities and expand horizons. But with new capability often comes new risks—and if those risks are not addressed effectively, they can have a significant impact when potential threats become real.

Evidence for this state of affairs has been mounting—and it is hardly trivial. According to the Privacy Rights Clearinghouse¹, more than 345 million personal records have been involved in data breaches reported in the US alone since early 2005, part of a global total that may be considerably higher. This has led to high interest among organizations worldwide in technologies such as data entitlement management and Data Loss Prevention (DLP) for stanching the loss of sensitive information due to security exploits.

But is this where businesses should begin in addressing this problem? Consider this: In the 2009 Verizon Business Data Breach Investigations Report², weaknesses and exploits of authentication and access controls represented 3 of the top 5 categories of breaches resulting from hacking. Consider as well that when the Open Web Application Security Project (OWASP) updated its Top 10 Most Critical Web Application Security Risks³ in 2007, “broken authentication and session management” appeared in seventh place. In the first “release candidate” for the 2010 update of the OWASP Top 10⁴, this category had moved up to third place.

Businesses must recognize anew that the front line of enterprise defense is Identity and Access Management (IAM). It is the fundamental technology for determining who has authorized access to what, without which tactics such as data entitlement management may have little or no point of reference for enforcing policy.

Many organizations apparently do not recognize the security exposures they face from poorly implemented identity and access controls, or are simply not taking the risk seriously enough.

And yet, many organizations apparently do not recognize the security exposures they face from poorly implemented identity and access controls, or are simply not taking the risk seriously enough. Cases such as the 2009 breach of over 30 million passwords sustained by photo sharing site RockYou.com reveal not only where many need to do a better job of protecting user credentials, but also that simple, easy-to-guess passwords remain in common use—indicating a failure to implement even the most basic access control policies.

Businesses must wake up to these facts. The pace of technology innovation continues to accelerate, and with increased momentum of IT deployment and delivery alternatives such as Service Oriented Architectures and cloud computing, the need for more effective access control is becoming paramount. No longer can the business think that security can be “added on” through accumulating more and more defenses alone. Today it must be “built-in,” and strategic approaches to identity and access management are primary enablers of this philosophy.

But their value does not end there. Linking identity to information technology also opens entirely new opportunities for the business. Business information systems can be made even more responsive to the user, providing them with information of highest appeal and opportunities most likely to see success when they are tailored to a specific individual. Few other domains of technology can provide this combination of risk management with business optimization, making today’s technologies of identity and access management one of the best IT investments an organization can make.

1 <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

2 W. H. Baker et al, 2009 *Data Breach Investigations Report*, Verizon Business, 2009

3 http://www.owasp.org/index.php/OWASP_Top_Ten_Project

4 http://www.owasp.org/index.php/File:OWASP_T10_-_2010_rc1.pdf

Secure By Design

The idea of building security into information systems may not be new—but it may require a shift in thinking about how IT can be secured in ways that can help the business perform better. Many organizations have a range of defensive tools and technologies that have accumulated over time as security has been “added on” to the environment. These tools continue to have their place, in both monitoring the environment for potential risks as well as for defense. But this is more the “responsive” side of security management.

The idea of building security into information systems may not be new—but it may require a shift in thinking.

Building-in security by design, on the other hand, represents more than the “proactive” side of the security equation. It requires not only a recognition of the risks in today’s emerging approaches to IT and information protection, but the ways in which these risks can be mitigated and managed directly in IT systems.

Today’s identity and access control technologies substantially expand past approaches to building security directly into IT, assuring a more consistent enforcement of policy throughout the various components of modern information architectures. Access management is vital for any business transformation, but it is essential for defining policy for *who* can access *what* information under *which* circumstances. New technologies that provide monitoring and enforcement of fine-grained policy governing who and how individuals and groups can access or block sensitive information are thus complementary to IAM, but identity and access controls must be established before DLP tools can match policy to appropriate information access and use.

Security Built-In: A Closer Look at Today’s IAM Capabilities

The complementary relationships of DLP to identity offers just one example of how today’s IAM technologies elevate the basic concept of access control into access assurance that can be deployed throughout modern information architectures. To illustrate this range of capability, consider a typical modern application:

A session requiring authentication often begins with the establishment of a Secure Sockets Layer or Trusted Layer Security (SSL/TLS) connection that provides confidentiality for the information exchanged between the endpoint and the application. (This connection-level security may be extended to other components of the application as well.)

Authentication, which typically takes place when a user supplies their login name and identifying credentials (a password is typically the simplest case), establishes the identity of the user. Once validated, information that the user has been verified can be provided to each component of an application as needed, as a transaction progresses throughout an integrated system. For example, identity federation techniques communicate the authentication information necessary to each component—but no more than is necessary at each step. Information such as username or any other personally identifiable information can be abstracted, which helps to assure greater security and privacy for personal data. These techniques often call on Web Services to uncouple dependencies on underlying systems and enable this authentication information to move more freely.

While authentication and federation identify the user, access control technologies protect access targets by evaluating authenticated access requests against policy. This means that access controls may be tailored to specific environments, such as individual OS platforms, applications, servers or mainframes, or to specific requirements, such as more finely grained control over highly sensitive root or administrator access.

Just as federation abstracts identity information, access policy controls can also be abstracted to better fit system requirements, translating access control into fine-grained entitlements that are complementary to Web Services for authentication, or linking access control with “single sign-on” technologies for unifying authentication processes. This provides significantly greater flexibility in tailoring access controls to the needs of a specific environment.

Today's techniques uncouple dependencies on underlying systems and enable authentication information to move more freely.

As transactions progress, their state changes. Transaction state information may be communicated through an application system through session management techniques that, together with identity and authorization information, supply the data needed at each step as transactions unfold. This information may also be communicated via Web Services.

The flexibility of Web Services in weaving together today's information systems suggests the role of systems purpose-built for SOA security and policy management. SOA security technologies can also validate the content of Web transactions, which may be critical to assuring transaction integrity. Validation may include such factors as verifying the structure and format of SOAP messages in Web Services. It may go even farther, however, to include techniques such as the cryptographic validation of message signatures, the encryption and decryption of sensitive content, or the enforcement of other aspects of policy appropriate at a certain transaction point. Systems that perform these important functions can also deliver high performance that improves the responsiveness of modern application systems.

The Benefits of Security “in Real Time”

Given the central importance of identity to assuring policy, the establishment of identity is critical. This speaks to the need to enroll users and validate identity credentials so that users can be properly authenticated when accessing authorized services. The technologies of user provisioning can embrace a wide range of policy requirements and provide workflows that smooth these vital processes within the enterprise.

But what about the application that faces the public or a potentially large and varied customer base? Here, “on demand” enrollment—often of previously unknown customers, for example—must take place in real time in order for the application to serve its business purpose. The responsiveness of this capability is critical to enabling a business-to-consumer (“B2C”) application to fulfill customer expectations, here and now. The sensitivity of online customers to application performance measured in seconds is well known, and applications cannot risk losing them to cumbersome enrollment processes. This is particularly true during peak utilization periods or seasonal variations in application load, when *all* application components must be optimized to respond to demand.

Responsive real-time enrollment and authentication can help solve these challenges—and more. For example, a system that authenticates a user once—but does not revalidate authentication throughout the remaining steps of a transaction—can become an attack target. Attackers that can interpose themselves into such transactions after a one-time validation may be able to take advantage of the user's credentials, if the application does not re-validate the user later in the process. Real-time authentication can re-validate the user throughout a transaction, helping to close these security gaps. This re-validation can be transparent to the user, and need not risk customer goodwill by complicating security management.

Real-time user enrollment and authentication offers business benefits beyond security as well. It can bring greater personalization to applications, customizing the presentation of portals and serving information of greatest interest to the user once identified. By linking identity to information such as buying preferences, it can also help business applications better serve customers by fine-tuning what the user sees, such as buying suggestions optimized by business analytics. This suggests how identity technologies can also help increase an application's business performance.

A Comprehensive Approach

Data and application security is a field in a constant state of flux. Organizations must therefore recognize the role of technologies that help defend against a changing threat landscape such as intrusion prevention and vulnerability assessment. These technologies can help protect the network, data and application environments as well, and for assessing IT environments for known vulnerabilities. Intrusion detection and prevention for applications can be further enhanced by network defenses designed for Web environments, while database monitoring and security systems help assure control over resources that house data itself.

It is worth noting that appliances that provide security and performance for SOA environments can also defend against the exploitation of Web Services. This directly complements system- and application-level defenses in the network, by providing message-level assurance for SOA transactions.

Constant change in the threat landscape means that application systems must also be assessed for vulnerabilities in light of current threats. Vulnerability management for applications is the objective of Web security assessment tools that help organizations understand their risk exposures in deployed applications, while source code security analysis tools help identify and remediate application security issues in development and maintenance.

The Long View: Identity and Policy Lifecycle Management

All these capabilities give architects and developers a powerful set of tools for building confidence into IT systems from the outset. Just as important, however, is the need to maintain this confidence over time.

Consider, for example, how the roles of individuals change. Within the organization, personnel may change job functions that require a different set of privileges in accessing information systems. Resources of higher sensitivity may be appropriate for access in one role, but not in another. A customer or a contractor may become an employee at some point, which would necessitate a change in access privileges in IT.

These capabilities give architects and developers a powerful set of tools for building confidence into IT systems from the outset. Just as important, however, is the need to maintain this confidence over time.

Consider also that employees also leave the organization—for a variety of reasons. When they leave a certain role, privileges in that role must be transitioned or terminated. When they leave the organization, the sensitivity of information to which they once had access becomes a factor—again, highlighting the complementary relationship between Identity and Access Management, and Data Loss Prevention. Indeed, organizations may see the need to protect such information *before* the staff member changes their status, by monitoring and enforcing policy on what is acceptable to access under which conditions, and what is not.

In terms of IAM, these requirements speak to the need for a lifecycle approach to identity management. Role management can help organizations identify the appropriate set of privileges for a given role, while user management capabilities help organizations define policy and process for managing these changes in identity over time.

These same techniques should be applied to access targets as well. A lifecycle approach to access management means that organizations assess access privileges to information resources and refine them as needs arise. The introduction of new information systems or changes in those systems must often be accommodated by changes in access controls that protect the organization as a whole. These changes, in turn, must also be rationalized against changes in identities and roles among users, to make sure that the needs of the business are satisfied by properly tuning access control to meet both user and policy needs.

When on-demand enrollment and real time authentication are run “in the cloud,” organizations should have the ability to maintain control over security policy in-house.

Throughout these lifecycles, organizations will need to monitor access to identify issues and potential abuses as they arise. This monitoring and reporting capability may be essential to regulatory compliance, for example—but it also supports more effective security management by pointing out potential anomalies that may be early indicators of more serious issues.

Failures in taking such a comprehensive approach to access monitoring and lifecycle management have been implicated in cases such as that of Jerome Kerviel at French bank Societe Generale in early 2008, where knowledge of back office functionality and

abuse of access from a front office trading position allegedly gave Kerviel access to trading systems that enabled him to hide enormous losses due to unauthorized trading activity. The incident highlighted how Identity and Access Management can directly enforce separations of duties intended to contain such risks—and how early detection of attempts to subvert access control can be instrumental in preventing significant loss.

The Service Option: Securing “IT as a Service”

As these examples suggest, the extent of capability available for securing modern business systems is wide and varied—but this breadth of capability may also be daunting. Organizations that seek primarily to optimize their business performance also need to contain their IT development and maintenance costs, particularly when resources are constrained (and rarely has this been of higher value than in the current economic climate). As organizations have become increasingly sensitive to security concerns, they also recognize that they need reliable expertise in building security into business technology.

This is where the delivery of IT as a service has high appeal. The flexibility afforded by technologies such as virtualization and Web Services enables providers to expose functionality as readily integrated services. This makes system components more readily consumable and composable in a more flexible approach to integration. Cloud computing takes this a step further, enabling complete systems to be transferred to a service provider (regardless whether internal or external to the organization). This allows organizations to offload many of the burdens of development and maintenance while still reaping the benefits of modern technology.

These new techniques must be approached intelligently when it comes to risk management. The composition of IT from services, for example, requires direction in order to succeed—and when assuring security, this means policy. Organizations must have the capability to define security policy that guides the integration, deployment and use of services safely.

Just as important is the level of control organizations can exert and maintain over service-oriented environments. For example, when run-time elements such as on-demand enrollment and real time authentication are run “in the cloud,” organizations should have the ability to maintain control over security policy in-house. This highlights the value of on-premises tools that orchestrate policy for external or hosted services.

IBM: Enabling Security By Design

As a leading supplier of information technology to organizations of all sizes, including many of the world’s largest, IBM has become a trusted partner to many for building these security capabilities directly into modern business systems.

IBM technologies for defining and provisioning user identities and roles in IT are complemented by a wide range of capabilities for controlling access to sensitive information resources. Beginning with the definition of policy for SOA security and data entitlements, IBM Tivoli Security Policy Manager enables organizations to manage SOA security and fine-grained entitlement policies throughout their lifecycle, from authoring and publishing policies, to defining their enforcement in information systems, and updating policies as required. Tivoli Security Policy Manager enables the centralized coordination of policy across multiple components of complex systems, centralizing data security policy control and providing for more consistent policy definition and enforcement. It also provides a means for organizations to maintain on-premises control of distributed runtime services, which may be housed in hosted or cloud environments outside as well as inside the organization. This helps assure a higher level of control over services, regardless how or where hosted, easing a significant barrier to adoption of service-oriented approaches that reduce IT management burdens.

Complementing the definition and management of policy are IBM Tivoli Access Manager products for enforcing policy in runtime, at the access targets, such as FileNet, Cognos and Microsoft SharePoint. The wide-ranging capabilities of the Tivoli Access Manager family deliver authentication and authorization of users across a spectrum of platforms and applications as well as privileged user access to operating system environments.

IBM has become a trusted partner to many for building these security capabilities directly into modern business systems.

IBM Tivoli Access Manager for e-business provides role-based enforcement of access policy for many important enterprise business applications. It provides access control for Web environments, including Java security for IBM WebSphere and portal environments. And it extends mainframe z/OS support to WebSphere, enabling users in WebSphere environments to access vital mainframe applications, databases and resources.

Many organizations face challenges in streamlining access to a number of applications and resources, each often providing its own tools for access control. This requires individuals to remember a number of logins and passwords, which can degrade overall security. IBM Tivoli Access Manager for Enterprise Single Sign-On offers the ability to access multiple resources with a single login, while at the same time providing granular access control for each target resource under management. This provides users with more simplified, yet secure, access to a broad range of corporate applications, Web and legacy environments, desktop and network resources, through a single password.

Tivoli Access Manager for Enterprise Single Sign-On also simplifies the login process by automating common tasks typically performed on authentication, including application login, drive mapping, application launch, single sign-on, navigation to preferred screens, multi-step logins, and other typical tasks. This not only helps sign-on become more seamless, but more secure when policies are automatically enforced. It can tailor authentication and the login sequence for any user on a shared workstation. It can also log-out users automatically when workstations are left idle or unattended, satisfying compliance mandates for this functionality when required.

These capabilities complement access controls integrated with many systems. IBM mainframes, for example, are often protected by facilities such as the well-known Resource Access Control Facility (RACF). RACF has long been instrumental in securing mainframe environments by authenticating authorized system users, classifying and protecting system resources, controlling the means of access, and logging and reporting both authorized and unauthorized access attempts. Today, the Tivoli Access Manager family offers capability to integrate enterprise-wide access management with RACF, in ways that make access to mainframe resources more seamless, even when integrated with Web or other applications, while assuring comprehensive security policy enforcement.

Weaving these capabilities together are technologies such as IBM Tivoli Federated Identity Manager, which supports standards-based identity federation, which abstracts identity and authentication from dependence on any one system in a complex application or SOA environment. It enables authentication information to be leveraged in a more granular way, at each step of a transaction as needed. It can provide individual transaction processes with the information required to assure authorization without exposing personal information. This helps to assure security throughout a transaction, improving resistance to threats that seek to exploit one-time-only authentication in systems where authorization is never re-validated. It also relieves organizations of having to construct risky architectures such as those where transactions are dependent on one system “trusting” another, rather than building in today’s approaches to more reliable identity and access management. Of high value to B2C applications is Tivoli Federated Identity Manager support for user self-registration, providing on-demand enrollment that expands business reach with minimal impact on users or customers.

Building security into a modern environment means more than integrating proper authentication and access control. It also means “defense in depth.”

Once a comprehensive approach to identity and access management is built into the environment, IBM solutions support the ability to keep the posture current. Identity lifecycle management capabilities integrated into the IBM portfolio enable organizations to manage the movement and termination of personnel, partners and customers. It provides for the assessment of roles and the management of changes in roles privileges that keep access con-

trols up to date, while IBM monitoring and reporting capabilities provide the visibility and insight needed to assure that access controls are properly managed.

Building security into a modern environment means more than integrating proper authentication and access control. It also means “defense in depth,” where architects recognize that the threat landscape changes constantly. The comprehensive IBM security portfolio supports the vigilance and defensive capabilities necessary to provide this level of protection to today’s environments, with intrusion detection and prevention, SOA security, database monitoring and network Web application protection technologies that support a more comprehensive approach. IBM also provides application security technologies that strengthen applications through vulnerability assessment and more secure development, helping developers to build security into today’s environments beyond identity and access controls.

As organizations increasingly look to service-oriented options for IT delivery, IBM sees this strategic direction, and can be expected to move with its valued customers in adapting its offerings to service-based approaches. Already, the company offers its Web application vulnerability assessment capabilities as a hosted service, complementing IBM’s well-reputed Managed Security Services and giving organizations a broad set of options. When complemented by assets such as Tivoli Security Policy Manager for on-premises management of security policy for remote or hosted services, IBM gives organizations a wide range of choices in integrating service-based options with on-premises preferences, enabling customers to craft the approach that best suits business and policy requirements alike.

EMA Perspective

It is impossible to over-emphasize what a serious mistake it would be to look at this long list of capability in identity and access management and see it simply as a litany of yet more innovation. What must be understood is that today’s identity technologies can make systems far more secure than in the past, if they are implemented properly.

Far too many legacy systems still make use of antiquated techniques for verifying that users are who they claim to be, relying on simple, once-only authentication techniques and allowing “back end” systems—where sensitive data is often found—to accept connections from “front end” HTTP servers without question, simply because one machine “trusts” the other. Attackers rely on low levels of sophistication such as this to exploit the architectural weaknesses in IT systems.

Today’s more granular and distributed approaches to identity and access management help close these risk gaps and enable system

Far too many systems still make use of antiquated techniques for verifying that users are who they claim to be. Today’s more granular and distributed approaches to identity and access management help close these risk gaps.

designers to build security into every aspect of today's more sophisticated IT environments. With its long history of innovation in business technology recognized by the world's largest and most demanding organizations, IBM has demonstrated its commitment to this approach. This pedigree is evident in IBM's portfolio for identity and access management, with more than 30 years of innovation beginning with access control for the mainframe environment.

Today's identity technologies have revolutionized how identity and policy can be made granular to fit a specific purpose while preserving individual privacy. They have also revolutionized how this information can be shared reliably, unifying a more seamless and more deeply integrated approach, and extensible to many resources throughout the organization. They can deliver granularity in authentication and authorization that follows each step of a transaction, enhancing security, privacy and policy control throughout. And they can deliver this consistency transparently to users, along with techniques for enrolling users and managing access that help business applications be more responsive to business needs.

This capability is not just needed today. Trends in exploits, disclosed vulnerabilities and successful breaches alike make it clear: the adversary is more capable than ever before. Today's systems *must* build in a level of security to match the innovation they deliver, in order to mitigate today's more serious risks.

About IBM

IBM offers a comprehensive portfolio of security, risk and compliance management solutions that can help organizations meet the challenges of securing a dynamic infrastructure. These offerings deliver a full range of security capabilities that address the people, processes, and information risks in IT environments.

IBM's leadership in security is an outgrowth of its broad solution portfolio, vast network of services professionals, and dynamic Business Partner community. IBM is a strong proponent of developing and supporting open standards, and IBM's security solutions provide broad platform support. IBM is a trusted partner, having helped thousands of organizations across different industries deliver secure services while reducing risk and improving IT security and compliance across the IT domain.

IBM enables organizations to build an end to end security foundation that helps protect users, data, applications and platforms. Organizations can leverage the depth and breadth of IBM's vast experience, helping them drive service quality improvements while minimizing costs and managing risk. The IBM Security Framework forms the basis for addressing industry solution requirements across the different security focus areas of the infrastructure. IBM has solutions in each focus area that can be implemented individually, or combined into an integrated, holistic architecture designed to meet the specific needs of an organization.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that specializes in going “beyond the surface” to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals and IT vendors at www.enterprisemanagement.com or follow [EMA on Twitter](#).

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2010 Enterprise Management Associates, Inc. All Rights Reserved. EMATM, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com



2034.030110