Five Things the CISO Would Like their Organization to Know About the Importance of Entitlement Management

ECHELON ONE, LLC
Executive Security Intelligence

August 1, 2007

Five Things the CISO Would Like their Organization to Know About the Importance of Entitlement Management

"Most of our clients have met compliance standards in regard to having good external protection in place. It's the internal controls – who is entitled to access what – that will remain the Achilles Heel faced by large enterprises in 2007"
– Bob West, Echelon One

"Send the entire C-Staff to 'Scared Straight Bootcamp.' Until we do, stockholders, the business itself and our careers are at risk." – IT Manager Global Financial Institution[1]

"If you don't have an effective way to change a user's entitlements your business is exposed. Often, the person with the most entitlements is the new employee or the employee who has just rotated through different departments. It is easy to overlook these employees." - CISO of Global Financial Institution

Of the 700 people in a top five U.S. bank's information security team, 500 alone are allocated to managing entitlements for its employee applications and many are busy hard coding who is authorized to access what directly into each application. As soon as the changes are made, many entitlements are already outdated meaning the valuable assets fueling the bank's business are dangerously exposed. Despite the best of intentions, they are no closer to the adherence of financial and compliance controls. Their risk level has not decreased.

Does this sound similar to your organization? With employees, contractors, customers, vendors, suppliers and partners all accessing the applications and data that fuel your business from all around the world, there can easily be thousands and even millions all entitled to access a different part of the same valuable application or view a different part of the same data. And, through it all, you are only one outdated entitlement away from a significant business risk.

Echelon One, a leading research and consulting company, has observed that organizations can spend 100-500 hours writing entitlement rules into each of their applications as they update applications to fit new compliance standards. Line-of-business managers may spend as many as 60 hours per year performing entitlement reviews, in order to sign off on compliance documentation required by auditors. We believe the challenge for most organizations in 2007 is deciding how they plan to manage user entitlements effectively. Why? Because even the most robust identity and access management products being used today are *incapable* of providing the flexibility, visibility, control and accountability needed to manage the entitlements effectively in today's compliance era. That is why so many enterprises, including three of the top five banks worldwide, have already deployed Entitlement Management tools specifically designed to manage the changing entitlements needed for today's compliance

[1] "Thwarting Data Loss: Best in Class Strategies for Protecting Sensitive Data". Aberdeen Group, May 2007

requirements and built with real-time audits in mind. This whitepaper discusses the importance of "Entitlement Management" – two words your Chief Compliance Officer has probably never heard of but needs to know about – and the role it plays in meeting compliance with corporate and governmental regulations.

After conducting many security reviews in a variety of industries, we've compiled our experience and summarized the five things every CISO would like their organization to know about Entitlement Management. They are:

1. What is Entitlement Management and why should my organization care?
2. Why is Entitlement Management a leading compliance concern for corporations today?
3. How have enterprises managed Entitlements historically?
4. What is the best way to address Entitlement Management and meet compliance requirements?
5. What are the expected compliance and security benefits of deploying Entitlement Management tools?

We've written this whitepaper with the senior level information technology or security executive in mind and hope they find it useful enough to share with other decision makers in the audit or compliance departments so more effective decisions about managing entitlements can be made.

What is Entitlement Management and why should my organization care?

Lack of good Entitlement Management practices leads to unnecessary business risks everyday. For example, consider the following scenario:

The head of a brokerage trading department is transferred to a different department, but her application and data access entitlements remain unchanged. Taking all her entitlements intact to her new job allows the former head of brokerage to improperly transfer millions of dollars at the click of a button – an entitlement she should no longer have. No one in the auditing department even thinks to look for this sort of problem. It goes undetected for half a year. No one can see the problem unless they are looking specifically at this one individual in a bank of tens of thousands of employees thus leaving the business at an unnecessary, and potentially huge, risk.

"Entitlements" are the granting and enforcement of privileges in business applications and data that may be based on an employee's role in an organization, their geographic location, the type of transaction requested for execution, and other situational context needed in order to grant access or authorization and carry out specific actions within the enterprise. "Entitlement Management" is the more daunting task of keeping entitlements up-to-date. The act of auditing the accuracy of entitlements can be a complex task because for most organizations this is a manual process meaning entitlements stay out-of-date – no matter how many bodies an organization throws at the problem.

Anyone in the information technology department will tell you creating an identity with associated privileges is not difficult. The challenge for the organization is the act of managing the multiple entitlements associated with one identity, when applied to different resources when accessed in multiple contexts. Without the right tools, auditors and line of business managers often find themselves knee deep in a manual process examining and reviewing each employee's identity and all of their associated

entitlements (which are changing dramatically with a rapidly evolving business climate). This daunting task is exactly why organizations are at a tremendous risk for potentially costly and damaging mistakes.

Why is Entitlement Management a leading compliance concern for corporations today?

Entitlement Management is a leading compliance concern because without it managing, enforcing, and auditing controls over access to information outlined in Sarbanes-Oxley, the Health Information Portability and Accountability Act (HIPAA), the Gramm-Leach Bliley Act, Payment Card Industry Data Security Standard (PCI DSS), Senate Bill California 1386, the European Union (EU) Privacy Directive and Basel II is not only extremely difficult – it is also a monumentally complex and costly task.

Take for example, the EU Privacy Directive. It mandates that personal information cannot leave their EU country of residence. If your corporation operates on a multinational scale you might find yourself needing to define specific entitlements around when employees can and cannot access personal information. For example, an application that uses a UK resident's personal information may be acceptable to access while employees are accessing it from the UK. But, once the employee leaves the UK and tries to access the same application from Hong Kong or France, this is not permissible. Many organizations complying with the EU Privacy Directive are finding they can greatly benefit from Entitlement Management tools because for the first time, they can manage, enforce, and control location-specific and context-sensitive policies. Defining these types of entitlements works not only for those complying with the EU Privacy Directive, but also for other businesses that want to confine what their employees are doing from where, when, and in what context. For example, is it acceptable to allow the same level of authorization if employees are accessing applications from home? How about from a partner's network? What information can a user change? When? From where and under what context? In today's business climate, organizations need to define much more precise, fine-grain entitlements that lock down control over applications and information.

The risk from a compliance perspective is that, without a good understanding of who has privileges to certain applications, information, and processes, a corporation cannot validate its compliance with regulations like Sarbanes-Oxley or PCI DSS. There must be a very good understanding of entitlements to answer the questions most commonly posed by auditors.

How have enterprises managed Entitlements historically?

Entitlements are not new. Traditionally, entitlements are stored in a wide variety of Identity and Access Management tools that allow the creation, modification, disabling, and deletion of credentials for people, devices, applications and processes. The different classes of tools used for identity and access management include directories that store credentials, provisioning tools to manage the creation of unique IDs, web access management tools for consolidating the number of user IDs for web applications, self-service tools such as self-service password reset tools, authentication tools, virtual directory products to manage multiple information stores, and federation tools to pass credentials from one domain to another.

There are two significant gaps when using these tools to manage entitlements. First, Identity and Access Management tools take a strictly user-centric view of entitlements, typically granting access to applications based on a user's group memberships or role assignments. These products do not take into account resource or context-specific attributes that are important for making entitlement decisions. For example, what is the classification level of the document being accessed and does that match the clearance level of the user? The second major gap is the Identity and Access Management products operate in a binary fashion – you either can access the application or you cannot. This level of control is inadequate when you consider a certain application may have many fine-grained resources within a single application. For example, a portal will have multiple portlets, tabs, pages, buttons, and functions, each of which may have different entitlement policies.

To address these gaps, applications have historically maintained their own internal databases to manage entitlements or tightly coupled entitlements with policies and business logic of specific applications. This becomes unmanageable for the corporations that have many applications and many users. Maintaining these separate databases or hard-coding policies into applications has made it difficult for a corporation to consistently provide the appropriate access and associated entitlements to its employees and business partners across the entire enterprise Each application that ends up with a different silo of entitlement policies exposes the corporation to potential system misuse, financial losses, and unnecessary regulatory scrutiny. And to make matters worse, it impedes the ability of the enterprise to react to changing business conditions because any change requires custom development in multiple applications.

What is the best way to address Entitlement Management and meet compliance requirements?

Specifically designed Entitlement Management tools like those from Securent can help organizations achieve their compliance and audit concerns by creating a consistent, standards-based infrastructure for managing and enforcing the appropriate access and entitlements across the enterprise. For example, three of the top five banks worldwide, the largest investment management broker in the world and the second largest pension provider in Canada have all standardized on Securent. Securent's Entitlement Management Solution (EMS) externalizes entitlement policy resolution, management, and audit from applications—giving total visibility and control over the entire security landscape of your organization with as much or as little control over specific policies as needed.

Securent's entitlement management product is novel because it has been specifically designed to enable enterprises to consolidate the configuration of entitlement policies in one place with a simple-to-use administrative console that allows administrators to manage all of the organization's fine-grain entitlement policies for easy changes and audits. This is a big advantage over turning to developers to change entitlements within each individual application silo. This is a much more costly, ineffective way to manage entitlements. With Securent EMS, administration of some polices can be delegated to the appropriate business analysts or line-of-business managers to quickly and easily create or change policies on the fly without having to rely on developers to hard-code policies into the application, while other policies, for example those pertaining to cross-application compliance, can be retained by central compliance teams. This is a much more cost-effective and secure way to manage entitlements.

What are the expected benefits of deploying Entitlement Management tools?

Benefits include persistent compliance, enhanced visibility, better security, easier audits, and dramatic savings in time and cost of development and maintenance. Key capabilities and benefits of the solution include:

- **Easier Audits and Persistent Compliance**: Securent gives you centralized, on-demand, and automated policy review capability within applications and across the enterprise. Real-time reports and alerts on who can access what, who accessed what, and who made what administrative change are easily available from a single management console for the entire enterprise. Securent enables companies to enforce and audit segregation of duties and other compliance policies for the entire organization with ease. Furthermore, Securent significantly reduces the cost of remediation by providing clear views of who has access to which resources under which conditions and how that user acquired access – addressing all of the key questions an auditor would ask. Once the precise source of the failure is identified, Securent EMS allows for quick updating and immediate enforcement of the new policy.

- **Savings on Redundant Programming:** In most organizations, most applications have their security permissions hard coded or configured separately. Likewise, when polices change, every application needs to be changed one by one. Securent transforms this process by allowing you to set or change your permissions across multiple applications from a single management interface. This results in a huge savings both in the initial build or configuration of a new application, even more over time as you configure new policy changes as opposed to having to recode them, and yet more as each additional application leverages the deployed entitlement management infrastructure. Customers have reported that total man hours required for the initial development and deployment of projects have fallen by as much as a third, and when adding in decreased maintenance, audit, and support costs they're seeing Return on Investment (ROI) of 300 to 400% in the first year alone.

- **Enhanced Visibility and Security:** By enabling standardized distributed policy resolution, Securent EMS helps organizations eliminate the significant complexity and risk associated with redundant, stove-piped, development and maintenance of policies across heterogeneous environments. Securent EMS provides policy consistency, which leads to enhanced visibility and overall security.

- **Speed to Market:** By untangling security from your core business logic, Securent can dramatically decrease the time it takes you to make a new application or service available to your customers. Securent streamlines your planning and prototyping by providing built-in, ready to use, fine-grained security controls that can be reused across application. By enabling you to be responsive Securent makes you a welcome partner to the Lines of Business. Our customers report that EMS has enabled them to decrease 18-month project cycles to 12 months.

Conclusion

Entitlement management provides visibility and ease of control around who has access to applications and information and what they can do with it. As a result, organizations must begin to turn more toward the use of entitlement policies to comply with increasingly complex compliance regulations. The key challenge for most IT departments in 2007 will be deciding how they plan to manage user entitlements

effectively. To achieve compliance, audit and security goals, enterprises must resist the urge to build entitlements into applications and deploy purpose-built Entitlement Management tools like Securent EMS.

About this report

This report is sponsored by Securent, the leading provider of entitlement management solutions. Securent's Entitlement Management Solution (EMS) enables organizations to secure sensitive applications and data with ease and precision. Securent EMS is the first proven XACML standard-based solution that allows organizations to create, enforce, review, and audit fine-grained access policies across heterogeneous application and IT environments distributed throughout the enterprise, all with centralized management and visibility. The significant cost, time to market, and compliance benefits of EMS have been proven at many Fortune 500 customers. Securent's product and market leadership have been recognized by leading industry analyst firms such as Gartner, Burton Group, and Forrester. To learn more about Securent's award-winning solution, visit www.securent.com or call +1.650.625.9400.

About Echelon One

Echelon One is an information security research company that specializes in helping executives develop the right combination of people, processes, and tools in order to maximize the impact and effectiveness of their security investments. Echelon One is comprised of a group of the most respected thought leaders in the information security community and helps executives to become efficient and effective providers of information security services for their employees, customers and business partners.