

White Paper



# Reducing the Costs of IT Security Management

Sumner Blount, eTrust® Solutions  
January 2006

## Table of Contents

The IT Security Management Challenge .....	3
Introduction to Identity and Access Management .....	3
Achieving Increased Operational Efficiencies.....	4
Reduced IT Security Costs.....	4
Help Desk Costs .....	4
Password and Profile Management.....	4
Security Administration Costs.....	5
Creation and Management of User Profile and Entitlement Information.....	5
User Access Provisioning.....	6
Management of Security Events .....	6
Partner Management .....	7
Application Development and Maintenance Costs .....	7
De-provisioning of Physical Resources.....	8
Management of Potential System Vulnerabilities .....	8
Increased Productivity .....	9
Problem: Lack of immediate system and application access for new users .....	9
Problem: Excessive management overhead in handling access request approvals .....	9
Problem: Wasted time spent in multiple application logons.....	9
Summary .....	10

## The IT Security Management Challenge

IT Managers today face a dizzying array of pressures. They must not only ensure a secure environment to protect the company's assets and industry reputation, but they often are being asked to do it at a lower cost than in the past. The pressure on IT to "do more with less" is strong and is unlikely to change significantly.

This pressure to increase IT efficiency and to manage costs exists in the face of increasing demands for more and better applications and services for the user and management populations as a whole. The demands for increased capabilities and services spring from several emerging trends. Among the most important of these trends are:

**Increased Need for Regulatory Compliance.** The burdens of compliance with current laws and regulations such as Sarbanes-Oxley and HIPAA often fall heavily on the IT security group. Creating effective internal security controls for compliance often places enormous strains on this group.

**Increased Merger and Acquisition Activity.** As companies grow through acquisition or mergers, the complexity of the IT security challenge increases with each acquisition. Entire new user populations and applications as well as many heterogeneous legacy systems must be integrated into an existing IT infrastructure. The complexity of the resulting infrastructure can increase significantly.

**Steadily Increasing User Populations.** As companies extend their business applications to their partners, and to increasing numbers of online customers, the demands on IT expand significantly. Managing ever-increasing numbers of users, their profiles, and their access rights to protected applications puts a strain on budgets, and increases the need for an effective way of improving the overall effectiveness and efficiency of IT and other associated organizations (such as Help Desk).

These factors, among others, are driving IT groups to search for solutions to streamline the management of their operation. The competing requirements to reduce costs and increase services present huge challenges. This paper discusses ways of streamlining the management of IT security in order to improve the overall operational efficiency of the enterprise. The focus of this paper is on the cost reductions that can be gained through the use of an integrated Identity and Access Management (IAM) solution.

## Introduction to Identity and Access Management

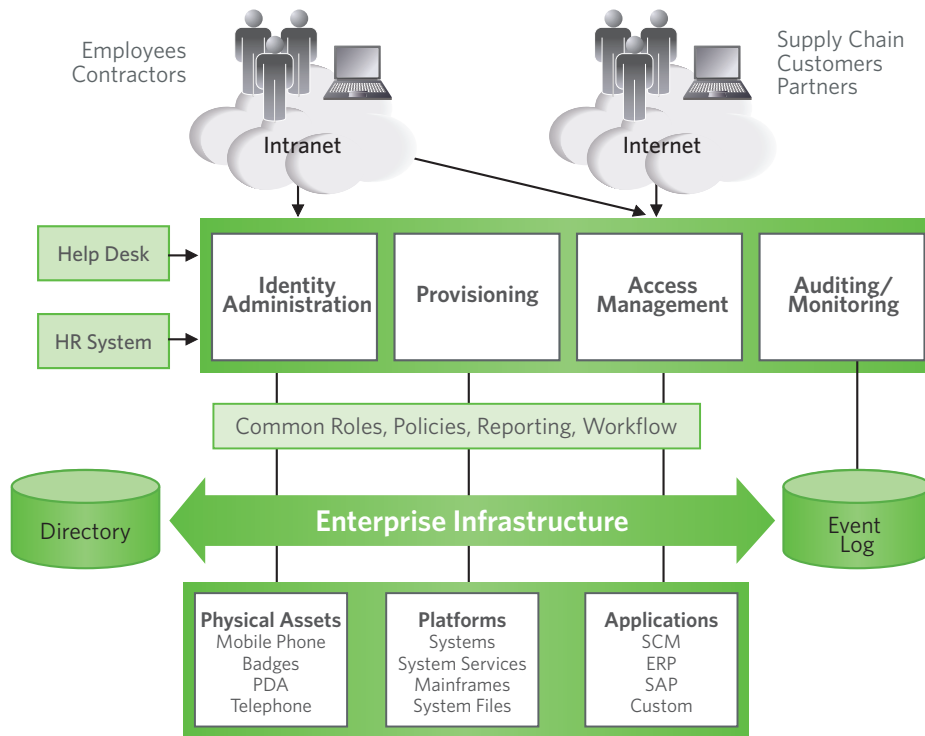
In almost all companies, users' identities and their access privileges are a core element of the e-business strategy. Behind those identities are the employees, contractors, partners, customers and others who drive every aspect of operations. Identity management is a set of processes and systems that determines who should have access to what applications, databases and platforms, and the conditions under which that access should be granted. The key questions that must be answered by the identity and access component of security management are:

- Who has access to what?
- What did they do?
- When did they do it?
- How can we prove it?

By answering these questions, you can effectively align security with business goals, protect vital business assets, streamline business operations and achieve regulatory compliance. The key capabilities, which must be integrated together for successful identity and access management, are:

- **Identity Administration** — Enables the creation and administration of user identities and profile information.
- **Provisioning** — Allocates to each user the appropriate accounts and access rights to corporate resources, as well as de-provisioning them at the appropriate time (e.g., when they leave the company).
- **Access Management** — Helps to ensure that your organization maintains the integrity of its information and applications by preventing unauthorized access. This includes controlling access to all critical resources, including web applications, enterprise applications, systems, critical system services, databases, and repositories.
- **Monitoring/Auditing** — Provides aggregation, filtering, analysis, and correlation of security events across all components within the environment. Also, it provides visualization tools to facilitate analysis of this information by system administrators.

The following illustrates the major components of a comprehensive IAM platform, and illustrates their relationship to the rest of the IT infrastructure.



**Figure 1. An integrated IAM Platform**

Note (at the bottom of the graphic) that access to a wide range of resources must be protected. This includes not only applications, but physical devices, systems, and critical system services and databases.

In summary, sound identity and access management practices and systems provide a foundation for security management by addressing identity-related system exposures, enforcing consistent security policy across your enterprise and delegating administrative access power. It also helps lower administration costs through integrated auditing and automated management.

Let's now look at specific ways to increase efficiency through the use of an IAM platform.

## Achieving Increased Operational Efficiencies

The challenge to “do more with less” has two important components, each one of which should be part of any effort to increase overall operational efficiency of the IT infrastructure.

“Do more” relates to actually producing more tangible results by increasing the productivity of each employee. Productivity has been sapped in many cases by inefficient internal processes, excessive manual procedures, and the requirement to deal with issues unrelated to one’s actual job function.

“...with less” relates to reducing the overall costs of IT security management. This can be done by eliminating needless processes, making users more self-sufficient, and automating a number of the IT administrative tasks that now require excessive amounts of time to perform manually.

There are several areas of IT security management that are ripe for substantial cost reductions.

## Reduced IT Security Costs

Many companies have struggled with the high costs of managing security, often due to outmoded, manual processes. Surprisingly, this is an area where cost reductions are quite easy to achieve, especially in the area of managing user identities and their entitlements. Let’s look at areas where these cost reductions can be the most significant.

### Help Desk Costs

The goal of any attempt to reduce the costs of the Help Desk needs to involve empowering the user to manage more of their own profile information. Since a significant amount of Help Desk resource is spent on these types of tasks, this is an area ripe for cost reduction.

## Password and Profile Management

**The Problem:** Many Help Desk teams spend much of their time helping resolve problems that the users potentially could solve themselves. No area is more illustrative of this than in password management. In addition, many users are forced to authenticate to each of the applications that they regularly use, requiring them to maintain a set of application passwords which are usually different from each other. The two ways to combat this problem are to empower the users to manage their own passwords, and to reduce the number of passwords that users are required to know.

**The Solution:** There are two important approaches to this problem. An application single sign-on solution can virtually eliminate the problem of having to remember many different application passwords. Secondly, a comprehensive password services capability of an IAM platform can provide significant cost savings by empowering users to manage their own passwords. Password Services should also provide extensive capabilities for ensuring that user passwords meet certain defined standards for password length, format, content and frequency of change.

**Potential Savings:** Gartner estimates that in a large enterprise, each user calls the Help Desk 16 times per year, with 25% of those calls relating to password reset. Their data also suggests that each call typically costs around \$23. For a 10,000 user population, this equates to around \$920K per year in password reset costs to the Help Desk. Allowing users to manage their own passwords (according to policies defined centrally) can eliminate virtually all of this cost.

---

Single Sign-on would result in a 33% reduction in Help Desk call volume

(Meta Group)

---

## Security Administration Costs

Security administration is one of the most important areas where cost reduction is possible. Many security administrators find themselves performing tasks that are either manual, or must be performed multiple times across all relevant systems and applications, or both. If tasks such as these could be automated without sacrificing security, the cost savings would be very substantial.

Much of the time that a Security Administrator spends is devoted to such tasks as:

- Creation of identities (profiles) for new users
- Creation of the access rights (entitlements) for each user, based on their role or group membership
- Allocation of resources to new users
- De-allocation of resources when users (typically, employees) are removed from the system
- Managing the identities and entitlements of external (typically partner) users
- Ensuring that each system and its critical services, databases, and files are protected from unauthorized access
- Collection and analysis of system log and auditing information
- Managing systems to ensure that the patches for all known vulnerabilities are installed in a timely manner

In general, each of these critical tasks can be streamlined so that much of the work is automated yet fully monitored and managed by the administrator. This section will highlight some areas of security administration that are particularly suitable for significant cost reductions.

## Creation and Management of User Profile and Entitlement Information

**The Problem:** Many companies suffer high expense due to the management of multiple IDs for each user, oftentimes scattered around the company in various (and possibly unknown) places. This situation is very common, and results in significant wasted expense in creating those multiple IDs, and in updating them as a user's attributes (such as their role) and entitlements change.

In addition, when the access rights to each application or resource are managed individually for each user, great inefficiencies result. Often, those access rights are enforced by the application itself, resulting in application "security silos" that lead to wasted administrative expense, and often leading to access rights that are inconsistent across applications.

**The Solution:** An IAM solution allows all user identities and entitlements to be created and managed centrally, thereby reducing administrative expense because user entitlements don't have to be administered in multiple places. Such a platform can also allow users to manage certain of their own profile attributes, further reducing the burden on the security administration staff.

All corporate IT assets need to be protected in this way, not just web applications. This includes sensitive applications, databases, platforms, and critical system files and services. By centralizing the management and enforcement of these access rights, each application, platform, or subsystem does not have to manage the access rights of their own authorized users.

**Potential Savings:** Centralized identity administration can significantly reduce the costs of managing user profile information. For example, for each user ID that is stored separately, an administrative expense must be borne. This includes not only initially creating that ID, but also updating it as the user's profile changes. The savings from centralized ID creation and management can be calculated using the average-time to create a user ID, the expected number of new user IDs that are created per unit of time, and the average number of places that an ID must be stored. The savings for profile updates can be estimated from the expected number of updates per user, the time to perform an average update, and the number of ID storage locations requiring changing. The total savings for management of user identities is the sum of these estimates, and should make a compelling business case for an identity management solution.

The potential savings from a centralized access management solution are large. They include such expenses as:

- The time spent creating access rights for each user, and for each resource or application on an individual basis
- The time spent on updating these access rights (for each platform or application) as a user's organizational function changes
- The cost of detecting and correcting access rights anomalies or inconsistencies that arise over time since there is no central way to track them

Most enterprises should expect to see the following metrics decrease, possibly significantly, upon deployment of a centralized IAM solution:

- Average time to create or update a user profile
- Average time to process an access request
- Average time to obtain approval for those requests that require it
- Proportion of access requests that deviate from the established process for access requests
- Proportion of access requests that are exceptions to the established user role definitions
- Amount of time spent correcting access rights discrepancies across systems and applications

---

On average, ongoing management of security code for web applications cost \$13.50 per user per application annually. Small extranets with 20K users and 6 applications quickly exceed \$1M annually in security administration costs.

(Gartner)

---

## User Access Provisioning

**The Problem:** One of the most time-consuming tasks that administrators are required to do involves granting access to systems or applications, especially in the case of a new user who needs to be provisioned with all their required accounts and applications. If, for example, a user needs to access certain data on three different systems, creating accounts or access rights on those systems can be very time-consuming. This process might also include allocating physical resources such as cell phones, credit cards, etc, for a new user. This process tends to be manual and very cumbersome.

**Solution:** An automated provisioning service allows that process to be done centrally and the account access established automatically without direct system administrator intervention. Accounts on target systems, and access rights to protected applications can be set up automatically, based on the user's role or organization group membership. No direct system administrator effort is required to create these accounts or entitlements.

Another critical advantage of an automated provisioning system is that it can provide a secure audit trail of all events relating to granting or termination of users' access rights. This capability is critically important, not only in terms of tracking the history of the granting of access rights, but also in terms of meeting the requirements for regulatory compliance.

**Potential Savings:** The potential savings from automated provisioning are compelling, and depend on:

- The number and arrival rate of new users
- The number of accounts and applications that typically require access provisioning
- The time required to grant and create access to each of these accounts or applications (this depends heavily on the type of account being created and the system where the account resides)
- The time expended in requesting, tracking, and managing the management approval process for access requests.
- The cost/hour of the security administration staff

For enterprises with 20K employees, analysts have predicted that automated provisioning can save anywhere from \$350K to \$700K in security administration expenses.

(Forrester)

## Management of Security Events

**The Problem:** One of the biggest problems facing IT administrators today can be termed “security information overload.” This results when each component in large IT environments is producing audit logs of events within that subsystem. These components include Windows systems, UNIX systems, intrusion detection systems, firewalls, anti-virus, and many other components that generate log information.

The IT administrator is left to make sense of this mountain of data. Not only is this a massive drain on resources, but manual analysis leads to security holes since it is almost impossible to correlate and draw conclusions from seemingly unrelated events, even though when taken together they may indicate a serious security problem. As an example, one of CA’s large customers has an IT environment that generates around 3 million log entries per day (see graphic). One can only marvel at the amount of administrator time it would take to perform any reasonable analysis on that massive amount of information.

**The Solution:** In the chaos that can result from security information overload, it is essential to restore order, and provide a solution that can actually focus the Administrator’s attention on the events that really matter. This requires a comprehensive security management solution that provides these critical capabilities:

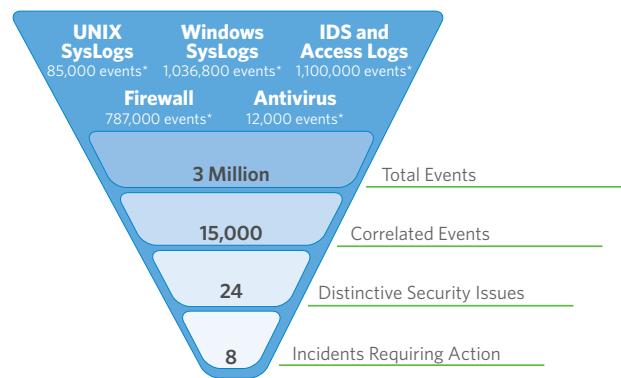
- Centralized collection and aggregation of all security event information across all components in the environment
- Normalization and filtering of all security log entries
- Correlation of apparently independent events to identify relationships between them that might indicate a potential breach attempts
- Visualization capabilities to allow easy visual analysis of the current status of all security attributes of the target systems
- Customizable reports that can provide each potential reader with the relevant information tailored to their unique needs
- Forensic analysis tools to help identify the cause of certain security events
- Integration with enterprise network management and service desk solutions.

“Pay particular attention to visualization capabilities, as the purpose of this technology is to get information to people. The visualization capabilities of the systems should be the leading criteria for evaluation”

John Hagerty, VP of Research, AMR Research

**Potential Savings:** It’s impossible to create a specific cost reduction analysis that works for each IT environment. It is reasonable to conclude, though, that a comprehensive security management system as described above makes security event management **doable**, which by itself, is a major benefit.

The following graphic illustrates the potential savings that can be achieved when security events are filtered and correlated in an automated fashion. This chart represents the log traffic from a single large user during a single one-day period:



**Figure 2. Log traffic illustrating potential savings.**

The administrative savings from going from 3 million events that need to be analyzed to 8 events requiring action makes a very compelling cost reduction business case for this type of solution. And, this does not even consider the important security advantages that such a solution provides.

## Partner Management

**The Problem:** As companies deploy their business applications online so that their partners can access them, the management of the identities and access rights of those partners becomes costly. Typically, these partners are more “trusted” than an average customer, but not so trusted as to be given the same access rights as an employee. Therefore, management of the identities of these partners often falls on the same organization that manages employee systems, adding yet another burden to their workload.

**The Solution:** An IAM platform that provides delegated administration of user identities and access. This allows the central IT group to define which sets of users and which attributes of a user the partner company can manage, and then management of their users is delegated to the partner Administrator. As a result, deployment of business applications to these partners is very scalable because the partners are managing their own users.

**Potential Savings:** The cost of managing a single user can be approximated using metrics such as:

- The initial cost and expected frequency of creating a new user identity
- The cost and expected frequency of making a single change to a user profile or access rights
- Size and expected growth of the user population

As partners take over the management of their own users, these costs can be drastically reduced. The ability to incorporate partners into your identity infrastructure is an enabling capability for creating a much more efficient and effective partner ecosystem. In particular, by making partners more of an active participant in your internal business processes (such as manufacturing planning and logistics), you can optimize these processes to increase the overall efficiency of your entire supply chain.

## Application Development and Maintenance Costs

**The Problem:** When access rights security is enforced within each application, there is a very significant cost in terms of application development and maintenance. Development of these security “silos” requires a lot of development time and expense, often simply to implement similar or identical security modules across multiple applications. This “recreating the wheel” process is inherently very inefficient.

**The Solution:** By externalizing security enforcement from applications into a separate access management service, the costs of developing and maintaining these components in the application is essentially eliminated. Applications become much simpler, maintenance becomes much less costly, and the testing effort is much less because rigorous testing of large amounts of security code does not have to be done.

**Potential Savings:** The potential savings are very specific to each environment. It depends on the amount of access enforcement code that is typically within each application, the number of applications, the approximate security testing overhead for the security modules of each application, and the ongoing maintenance that these modules require. But, the savings generally prove very significant for most companies.

---

The development savings of a centralized access management solution are approximately \$6.60 per user per applications.

(Gartner)

---

## De-Provisioning of Physical Resources

**The Problem:** Many times, when an employee leaves the company, they have acquired access to a number of physical resources supported by their company. This often includes cell phones, credit cards, PDAs, and other service-based resources such as outsourced applications. Many companies don't even track these resources closely, and often don't immediately de-activate them to save service subscription fees upon the employee's termination.

**The Solution:** If physical resources were allocated using an automated provisioning system, they can be de-allocated immediately with the de-provisioning capabilities of that solution. This will terminate the service fees immediately without requiring manual intervention.

**Potential Savings:** The potential savings depend heavily on the:

- Number of employees and the rate of turnover
- Average number of service-based physical resources per employee
- Subscription costs per user/per service
- The approximate delay in terminating these contracts using the current, manual processes

## Management of Potential System Vulnerabilities

**The Problem:** Most analysts agree that a major problem, both in terms of security and administrative expense, is the management of known system vulnerabilities. Many companies today struggle with a collection of independent and heterogeneous tools, such as vulnerability scanners and patch management systems, among others. This often results in inconsistent application of available patches, so that vulnerabilities still exist even if fixes are available for them.

**The Solution:** Management of diverse system vulnerabilities requires a robust vulnerability management solution that can manage the entire process of identification of computer assets, management of patches made to each configuration, deployment of vulnerability remediation methods, and the tracking and analysis of risk for each resource, based on the vulnerabilities that might exist for it.

---

“Through 2008, 90% of successful hacker attacks will exploit well-known software vulnerabilities”.

(Gartner)

---

**Potential Savings:** The benefits of such a solution relate primarily to stronger security and therefore reduced overall risk. But, a unified, holistic approach also provides efficiency benefits, such as:

- Reduced administrative time determining the current patch status of all systems
- Reduced time spent actually deploying vulnerability patches to effected systems
- Reduced time spent manually collecting and analyzing data related to the vulnerabilities and risk associated with each system
- Reducing time spent researching and prioritizing known vulnerabilities and their solutions

## Increased Productivity

Along with these significant cost reductions, an IAM solution can also eliminate some of the “hidden costs” that plague many IT environments. In particular, there are often several areas where user and/or manager productivity is reduced because of the lack of an automated way of managing user identities.

Many IT environments are struggling under infrastructures that were designed before they experienced a significant increase in the number of their protected applications, and the size of their user populations. These internal processes are typically manual, and drain significant time and energy from managers and users alike. The most problem-laden area is often that of managing the user identities, their profile information, and their access rights to protected resources.

### **Problem: Lack of immediate system and application access for new users.**

New users are often forced to wait days (sometime even weeks) to have full access to all the system accounts, applications, physical resources, and information that they will need to perform their job duties. Consider the following example to illustrate the potential impact of this delay:

Assume:

- A 40 hour delay for allocation of accounts and access to resources
- \$31.25 hourly pay for the employee (translates to a \$65K annual salary)

The resulting productivity loss: \$1,250 for each new employee hired.

The solution to this problem is a comprehensive user provisioning solution. This is because automation of user access requests, or of the initial allocation of resources to users, can be a huge efficiency improvement in almost any IT environment. But, it also helps reduce the “hidden but painful costs” of unproductive users while these requests are being completed.

### **Problem: Excessive management overhead in handling access request approvals.**

Management approval of access requests, when done via the usual paper-based process, is a significant drag on management productivity. Automation of this process frees up management to focus on more important tasks, as well as providing an audit trail of the approval process for later analysis. A full workflow capability can also allow the Administrator to define complex approval dependencies, so that the complete corporate approval process can be replicated within the provisioning solution.

### **Problem: Wasted time spent in multiple application logons.**

A common problem in almost all IT environments is that of multiple logons for the different applications that each user must access. When each application handles its own user authentication, the result is wasted user time without any additional security. A centralized web single sign-on capability, as part of an identity and access management solution, reduces the amount of time users must spend in redundant application logons.

Burton Group has estimated that the average user in many environments might spend 15 minutes a day in application logons. A SSO solution can bring that down to around 3 minutes, saving many thousands of dollars in productivity time when multiplied across the entire user population.

## Summary

This paper has highlighted some important operational efficiencies that can be gained by deploying an integrated IAM solution. Such a solution can significantly reduce the costs of Help Desk support and system administration. It can also increase the productivity of all users, since resources are available more quickly, and long approval processes are

streamlined significantly. In addition, an IAM platform greatly simplifies and increases the security of the entire process of managing all your users and their access to protected corporate resources of all types.

The following table summarizes these areas of cost reduction and employee productivity that can be achieved with an integrated IAM solution.

Cost Reduction	Proposed Solution
Password-related Help Desk calls	Password Services component within an IAM platform
Management of user identities and entitlements	Integrated IAM platform
Provisioning of resources to users	Integrated IAM platform
Management of security events	Security Information Management solution
Management of partners	Integrated IAM platform
Application development and maintenance costs	Centralized access management
De-provisioning of physical resources	Automated provisioning solution
Management of system vulnerabilities	Vulnerability Management solution
Productivity Improvement	Proposed Solution
Faster access to resources and applications for new users	Automated provisioning solution
Reduced management overhead for access request approvals	Automated provisioning solution with workflow
Reduced application logon time	Web SSO solution

