

WHITE PAPER: IT SECURITY COSTS

# Reducing the Costs of IT Security Management

MARCH 2009

Sumner Blount

CA SECURITY MANAGEMENT

---

## Table of Contents

---

<b>Executive Summary</b>	<b>1</b>
<b>SECTION 1: CHALLENGE</b>	<b>2</b>
<b>The Challenge to Do More with Less</b>	
The Increasing Demands on IT	
The Need for Increased Operational Efficiencies	
<b>SECTION 2: OPPORTUNITY</b>	<b>3</b>
<b>Identity and Access Management (IAM)</b>	
<b>Reducing IT Security Costs</b>	
Help Desk Costs	
Security Administration Costs	
Application Development Costs	
Deprovisioning of Physical Resources	
<b>Productivity Considerations</b>	
<b>SECTION 3: BENEFITS</b>	<b>9</b>
<b>Quantifying Reduced Costs and Increased Productivity</b>	
Help Desk Costs — Password and Profile Management	
Security Administration Costs	
<b>SECTION 4: CONCLUSIONS</b>	<b>12</b>
<b>SECTION 5: ABOUT THE AUTHOR</b>	<b>13</b>
<b>ABOUT CA</b>	<b>Back Cover</b>

# Executive Summary

## Challenge

---

IT managers today face a dizzying array of pressures. On one hand, they must ensure a secure environment to protect the company's assets and reputation. But on the other hand, they're being asked to do it at a lower cost than in the past. The pressure to "do more with less" is strong and unlikely to change. This pressure to increase efficiency and manage costs exists in the face of increasing demands for more and better applications and services for the user community (internal and external) as a whole. The competing requirements to reduce costs and increase services present huge challenges.

## Opportunity

---

This paper discusses ways of streamlining the management of IT security in order to improve the overall operational efficiency of the enterprise. The focus is on the cost reductions that can be gained through the use of an integrated Identity and Access Management (IAM) capability. IAM is a set of processes and systems that determine who should have access to what applications, databases and platforms, the conditions under which that access should be granted, and how that access should be monitored.

## Benefits

---

Sound IAM practices and solutions can not only significantly lower security administration costs and increase productivity, but can also provide a foundation for security management by:

- AUTOMATING** IT process to reduce overall IT costs
- ADDRESSING** Identity-related system exposures
- ENFORCING** Consistent security policy across your enterprise
- DELEGATING** Administrative access power

## The Challenge to Do More with Less

### The Increasing Demands on IT

IT managers have been living with the requirement that their organizations “do more with less” for years. At first, this was an exercise in taking costs out of IT operations. But today, the requirement calls for providing services that are more tightly aligned with business goals, as well as focusing strongly on the increasing challenges and costs surrounding IT security. The demands for increased security capabilities and services spring from several trends. Among the most important 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. 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 security 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 efficiency of IT and other associated organizations (such as the Help Desk).

These factors, among others, are driving IT groups to search for solutions to streamline the management and “secure-ability” of their operation.

### The Need for Increased Operational Efficiencies

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

“Do more” relates to actually producing more tangible results by increasing the productivity of each employee. More is required because of the trends mentioned above. At the same time, 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.

Before considering areas of IT security management that are ripe for cost reductions, let’s first look at the key capabilities offered by an Identity and Access Management solution.

## Identity and Access Management (IAM)

An IAM capability can be used to significantly reduce the costs associated with IT security management, thereby improving the overall operational efficiency of the enterprise.

**PERFECTING IDENTITY MANAGEMENT** In almost all companies, users' identities and their access privileges are a core element of the business strategy. Behind those identities are the employees, contractors, partners, customers and others who drive every aspect of operations.

*IAM is a set of processes and systems that determines who should have access to what applications, databases and platforms, the conditions under which that access should be granted, and how that access should be monitored.*

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** To enable the creation and administration of user identities and profile information

**PROVISIONING** To allocate to each user the appropriate accounts and access rights to corporate resources, as well as deprovisioning them at the appropriate time (for example, when they leave the company)

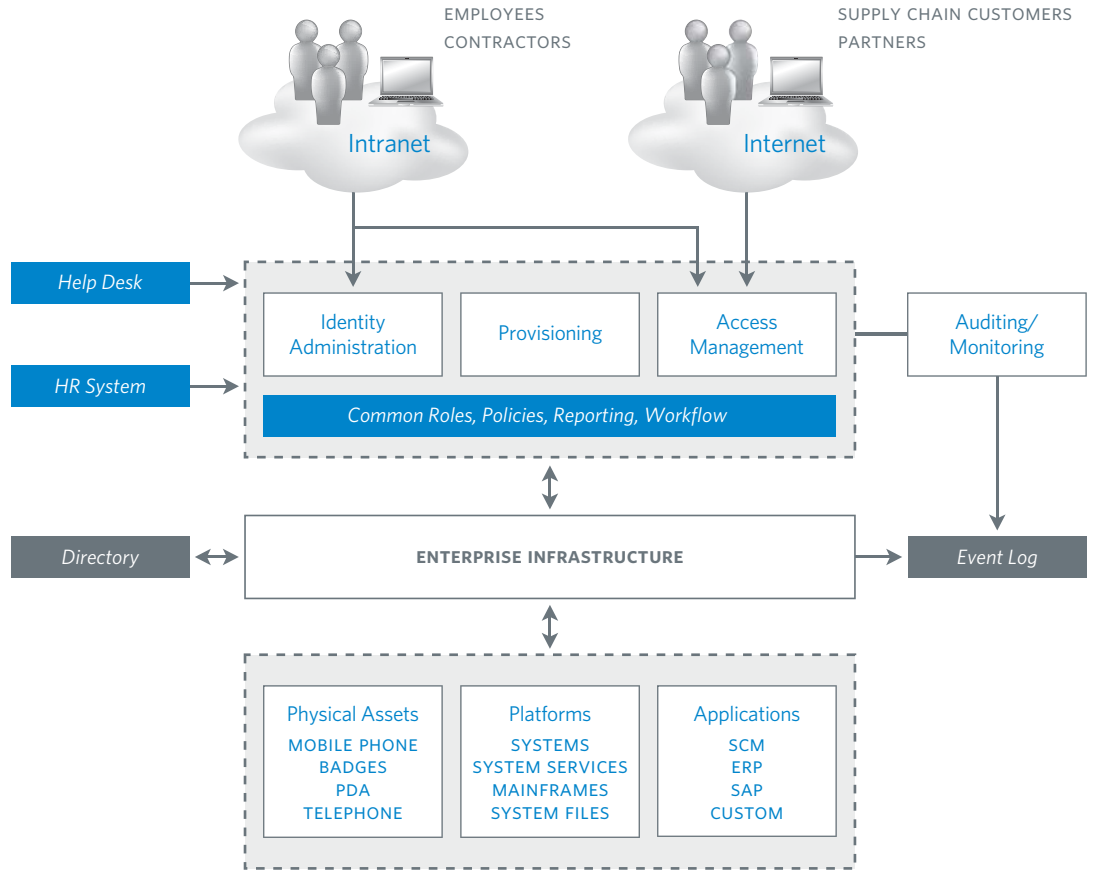
**ACCESS MANAGEMENT** To help ensure that your organization maintains the integrity of its information and applications by preventing unauthorized access. Includes controlling access to all critical resources, including web applications, enterprise applications, systems, critical system services, databases and repositories

**MONITORING/AUDITING** To provide aggregation, filtering, analysis and correlation of security events across all components within the environment. Also provides visualization tools to facilitate analysis of this information by system administrators.

FIGURE A

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

## AN INTEGRATED IAM PLATFORM



## Reducing IT Security Costs

Let's look at specific ways to reduce expenses and increase efficiency through the use of an integrated IAM platform.

### Help Desk Costs

If you're going to reduce the costs of the Help Desk, you need to empower users to manage more of their own profile information. Since a significant amount of Help Desk resource is spent on password and profile management tasks, this is an area ripe for cost reduction.

No area is more illustrative of this than password management. Many users are forced to authenticate to each of the applications that they regularly use, requiring them to maintain a set of application passwords, that 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 manage.

There are two important approaches to this problem. First, an application "single sign-on" solution can virtually eliminate the problem of having to remember many different application passwords. Second, a comprehensive password services capability can provide significant cost savings by empowering users to manage their own passwords. Password services should

also provide capabilities for ensuring that user passwords meet defined standards for length, format, content and frequency of change.

### Security Administration Costs

Security administration is another important area where cost reduction is possible. Many security administrators find themselves performing tasks that either are 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:

- Creating identities (profiles) for new users and the access rights (entitlements) for each user based on his/her role or group membership
- Allocating resources to new users and de-allocating resources when users (typically employees) are removed from the system
- Managing the identities and entitlements of external (typically partner) users
- Collecting and analyzing 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. The rest of this section will highlight how these tasks and some related areas of security administration are particularly suitable for significant cost reductions.

**MANAGEMENT OF USER PROFILE AND ENTITLEMENT INFORMATION** 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 users' attributes (such as their roles) and entitlements change.

In addition, it becomes very inefficient when the access rights to each application or resource are managed individually for each user. 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.

An IAM platform allows all user identities and entitlements to be created and managed centrally, thereby reducing administrative expense. Such a platform can also allow users to manage some 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. These include 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 its own authorized users.

**USER PROVISIONING** One of the most time-consuming tasks required of administrators is granting access to systems or applications, especially in the case of new users who need 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.

An automated provisioning service allows that process to be completed 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 related to granting or terminating 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.

**MANAGEMENT OF SECURITY EVENTS** 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, antivirus, 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 three million log entries per day. The amount of administrator time it would take to perform any reasonable analysis on that massive amount of information is unimaginable.

In the chaos that can result from security information overload, it is essential to restore order and be able to focus the administrator's attention on the events that really matter. This requires a comprehensive security management approach 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 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 reader with the relevant information tailored to his/her unique needs
- Forensic analysis tools to help identify the cause of certain security events
- Integration with enterprise network management and service desk solutions

**PARTNER MANAGEMENT** 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 its workload.

The solution is 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 to delegate management of those users 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.

**MANAGEMENT OF SYSTEM VULNERABILITIES** Most analysts agree that a major problem, in terms of both 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.

Management of diverse system vulnerabilities requires a robust vulnerability management approach. The system must integrate the entire process of computer asset identification, 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.

### **Application Development Costs**

When access rights security is enforced within each application, application development and maintenance costs soar. Management 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.

By separating security enforcement from applications and moving it to a centralized access management service, the costs of developing and maintaining these components in the application are essentially eliminated. Applications become much simpler, maintenance becomes much less costly, and the testing effort is reduced because rigorous testing of large amounts of security code does not have to be done for each application.

### Deprovisioning of Physical Resources

Often, when these employees leave a company, they have acquired access to a number of physical resources. These often include 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 deactivate them to save service subscription fees upon the employee's termination.

If physical resources are allocated using an automated provisioning system, they can be de-allocated immediately with the deprovisioning capabilities of that system. This will terminate the service fees immediately without requiring manual intervention.

### Productivity Considerations

Along with these significant cost reductions, an IAM platform 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 are reduced because of the lack of an automated way of managing user identities.

Many IT environments are struggling under infrastructures that were not designed to handle current numbers of protected applications, or the size of their user populations. These internal processes are typically manual, and drain significant time and energy from managers and users alike. Listed below are some of the problems associated with managing user identities, their profile information and their access rights to protected resources.

**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 they will need to perform their job duties.

Consider the following example to illustrate the potential impact of this delay:

Assuming a 40-hour delay for allocation of accounts and access to resources and \$31.25 hourly pay for the employee (translating to a \$65K annual salary), the resulting productivity loss will be \$1,250 for each new employee hired.

The answer is a comprehensive user provisioning solution, that automates user access requests or the initial allocation of resources to users.

**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. This process can be automated using a workflow capability. 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.

**WASTED TIME SPENT IN MULTIPLE APPLICATION LOGONS** Burton Group has estimated that the average user in many environments might spend 15 minutes a day in application logons.

## Quantifying Reduced Costs and Increased Productivity

Pursuing the opportunities provided by a comprehensive and integrated IAM capability results not only in better security management, but in many different kinds of cost savings. Let's look at areas where these cost reductions can be most significant.

### Help Desk Costs — Password and Profile Management

Gartner estimates that in a large enterprise, each user calls the help desk 16 times per year, with 25% of those calls related to password reset. Its 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.

### Security Administration Costs

The rest of this section will highlight some of the cost reductions that can be recognized in specific areas of security administration.

**CREATION AND MANAGEMENT OF USER PROFILE AND ENTITLEMENT INFORMATION** 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 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 to be 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, when deploying a centralized IAM platform:

- 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

**USER ACCESS PROVISIONING** The potential savings from automated provisioning are compelling, and depend on:

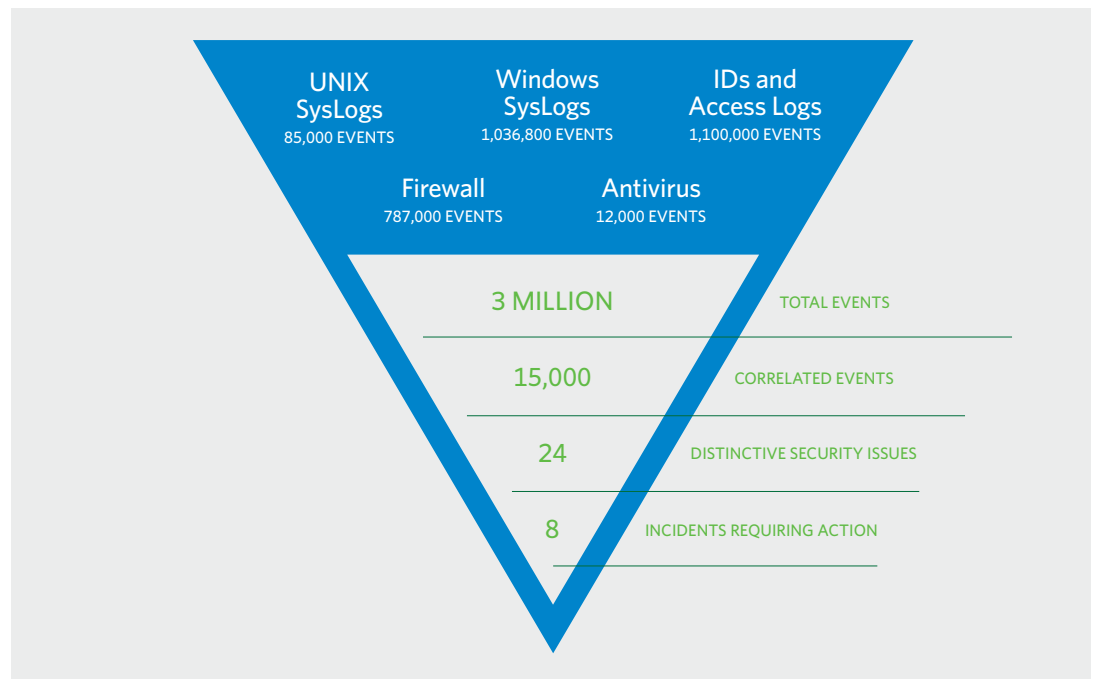
- The number and arrival rate of new users
- The number of accounts and applications that typically require access provisioning
- The time required to grant and create access to each of these accounts or applications (this depends heavily on the type of account being created and the system where the 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

**MANAGEMENT OF SECURITY EVENTS** 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 in Section 2 makes security event management doable, which, by itself, is a major benefit.

**FIGURE B**

The following graphic illustrates the 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.

**LOG TRAFFIC ILLUSTRATING POTENTIAL SAVINGS**



The administrative savings realized by going from 3 million events that need to be analyzed to eight events requiring action (in Figure B) 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 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 to 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 active participants 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.

**MANAGEMENT OF POTENTIAL SYSTEM VULNERABILITIES** The benefits of a vulnerability 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 spent determining the current patch status of all systems
- Reduced time spent actually deploying vulnerability patches to affected 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

**APPLICATION DEVELOPMENT AND MAINTENANCE COSTS** The potential development and maintenance savings are very specific to each environment. They depend 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.

**DEPROVISIONING OF PHYSICAL RESOURCES** The potential savings depend heavily on:

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

**PRODUCTIVITY CONSIDERATIONS** Here are several ways user and/or manager productivity can be increased through the use of automated management of users' identities, their profile information and their access rights to protected resources.

- Timely system and application access for new users — A comprehensive user provisioning solution 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.
- Minimal management overhead in handling access request approvals — Automated request processing frees management to focus on more important tasks, as well as providing an audit trail of the approval process for later analysis
- Reduced time spent in multiple application logons — An SSO solution can reduce the 15 minutes (estimated by Burton Group) to around three minutes, saving many thousands of dollars in productivity time when multiplied across the entire user population

SECTION 4

## Conclusions

We’ve highlighted some important operational efficiencies that can be gained by deploying an integrated IAM platform. Such a capability 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 the areas of cost reduction and increased employee productivity that can be achieved with an integrated IAM solution.

FIGURE C

An integrated IAM solution can deliver benefits both in terms of cost reduction and improved productivity.

### BENEFITS OF 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
Deprovisioning 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

SECTION 5



**Sumner Blount**  
CA Security Management

## About the Author

Sumner Blount has been associated with the development and marketing of software products for over 25 years. He has managed the large computer operating system development group at Digital Equipment and Prime Computer, and managed the Distributed Computing Product Management Group at Digital. More recently, he has held a number of Product Management positions, including Product Manager for the SiteMinder product family at Netegrity. He is currently the Director of Security Solutions at CA.

CA, one of the world's largest information technology (IT) management software companies, unifies and simplifies the management of enterprise-wide IT for greater business results. Our vision, tools and expertise help customers manage risk, improve service, manage costs and align their IT investments with their business needs.

WP05GMIAMCO0E 312910207