Gartner Research

Publication Date: 18 December 2008 ID Number: G00164175

Cutting IT Costs Within IAM and With IAM

Earl Perkins, Perry Carpenter, Ant Allan

This research describes identity and access management's (IAM's) role in reducing costs in enterprises, and what enterprises can do to reduce costs of IAM operations and projects. Customers should implement near-term and long-term cost-cutting opportunities in both situations.

Key Findings

- Cost savings in IAM initiatives can occur simultaneously with cost savings in IT operations if IAM is leveraged effectively.
- Both near-term and long-term actions can be done to and with IAM to reduce costs. It isn't necessary to sacrifice strategic planning when cutting costs.

Recommendations

To realize savings, enterprises can:

- Reduce the scope of IAM initiatives.
- Renegotiate the terms of the service provider agreement.
- Audit for existing IAM assets to leverage efficiencies in their use.
- Optimize the existing IAM operations organization.

ANALYSIS

With the current economic challenges, enterprises are seeking opportunities to reduce costs. Although repeatable, established operational activities are certainly the first target of opportunity, cost savings throughout enterprise activities are also needed.

There are two dimensions of cost reduction experiences:

- Immediate, opportunistic and quickly implemented actions for immediate return on those actions
- Paced, longer-term and selective actions that become part of the enterprise business life cycle

Of course, immediate actions can also yield long-term contributions, but that is not their primary aim.

How can IAM be implemented to improve identity-relevant security efficiency and otherwise reduce costs? Depending on the IAM deployment scope, the cost reduction motivation can be for immediate return and/or for long-term strategic return.

A distinct advantage of IAM initiatives over other infrastructure or application initiatives is the ability of IAM to contribute significantly to cost reductions in the enterprise. Unfortunately, IAM deployments and operations have a history of being expensive to implement and maintain. This research sets out cost-saving opportunities from both perspectives: cutting costs within IAM programs and operations, and using IAM to cut costs in IT and the wider enterprise.

How Can You Cut the Costs of IAM Programs?

IAM deployments have near-term as well as longer-term cost-cutting opportunities.

Near-Term Cost-Cutting Opportunities

Inventory your current IAM assets for potential leverage. Prior to evaluating, selecting or purchasing new products, inventory what the enterprise already owns. The enterprise may already own IAM products that perform some of the functions required, but has not implemented them fully. Using "what you already have" reduces implementation time frames (that is, no vendor selection or negotiation is needed) and reduces overall software spending (that is, with the exception of any new per-seat or per-processor licenses required, no new software is necessary).

Reduce the scope of IAM initiatives. Costs can be reduced by focusing on only one or a few aspects of the initiative. This could be organizational (for example, complete the initiative for a particular division or department as a credibility opportunity as well as an alliance-building experience), geographic or functional (for example, deliver only Web access or password management as a first phase). A key decision factor is in getting the most value from the reduced scope performed, whether technical or political. In addition, some vendor products are especially well-suited to reduced-scope implementations (that is, many of these come from more "pure play" IAM vendors).

Increase the time scale for IAM initiatives. Year-over-year costs can be reduced by increasing the time taken to complete the initiative, thus spreading costs more thinly over time. In essence, the enterprise is reducing the scope of what will be done this year, and putting off the rest for subsequent years, incurring only labor costs. A key decision factor here is in ensuring that the IAM initiative can still meet business deadlines, whether operational or regulatory.

Review and audit your IAM plan and its execution. In IAM implementation or operations, cost and schedule overruns are often the result of bad planning or a failure to plan. Proper planning for IAM programs and operations help you to determine effective deployment strategy and priorities. For instance, many companies inadvertently slow down their IAM projects — and eat up expensive resources — by trying to integrate so-called "difficult systems" first. These difficult systems (such as user provisioning) may not be of the highest priority to deliver business value. In fact, they prevent enterprises from developing a "credibility experience," instead of focusing on a less-complex solution and thereby gaining a valuable customer ally in the program by delivering solutions for them.

Renegotiate the terms of the service agreement. During challenging economic periods, consulting and system integration partners are more open to renegotiating costs and services with customers rather than lose the entire initiative. Review service costs and terms to reflect the reduced scope, moving where possible more-expensive activities (such as connector development and workflow) to a later period in the initiative.

Modify the selection process for vendors and services. This is a critical part of the "review and audit" step above. For some customers, slowing the selection process and increasing the number of possible providers (who in turn provide a broader range of cost savings opportunities) during the review can detect previously unseen savings opportunities. Review the selection process in light of licensing and contractual agreements you may already have with vendors that also provide IAM, because this may result in considerable savings with minimal impact. Allow the contract to be reviewed by a third party that is paid only if savings are found.

Consider "incremental expansion" in existing IAM services. Enterprises with existing IAM solutions that need to expand (for example, through merger, acquisition or growth) should review "appliance style" solutions and software as a service (SaaS) options. They provide a simpler set of IAM features, but lessen the impact on mixing vendors for different needs (such as Web access management [WAM], enterprise single sign-on [SSO] and password management). The maturation of the IAM solution market for basic functions can support this, although the IAM appliance and SaaS solution market is nascent. Such incremental solutions can also address partially completed IAM implementations where funding has been substantially reduced.

Long-Term Cost-Cutting Opportunities

Assess IAM architectures for migration and services. Whether you have existing IAM solutions in your enterprise or are contemplating them, a review of basic IAM architectures is now needed. Customers with existing IAM solutions should review vendor road maps to discover vendor plans to provide a "services-centric" version of the product, whether for use within the enterprise or to be consumed as a SaaS. Increased mergers and acquisitions as a result of economic conditions will bring together disparate IAM systems from different companies — such systems will need a plan that includes architecture.

Consolidate disparate IAM technologies to streamline operations delivery. Many enterprises still struggle with basic IAM infrastructure concerns such as widely decentralized directories for authentication, rationalizing internal versus external IAM needs, and multiple access management methods. Complexity should be reduced by simplifying infrastructure design, resulting in savings opportunities over the long term and positioning the enterprise to implement other, non-IAM cost savings solutions (such as portal environments for consumers and citizens, and audit systems for better transparency).

Evaluate the potential use of open-source software (OSS) solutions. Although OSS cannot provide a full IAM software portfolio, a number of OSS tools can provide some IAM functionality rather effectively (see "Open Your Eyes to the Potential of Open-Source Identity and Access Management"). For example, if your need for a WAM tool is restricted to its Web SSO

functionality — which we see in many client implementations — consider using OSS alternatives to commercial products, such as OpenSSO, CAS or Pubcookie. Finding an OSS alternative to commercial user provisioning tools is more challenging, as connectors and workflow are lacking, but Grouper and Signet can provide some identity administration functionality, and Penrose is an OSS virtual directory.

Evaluate alternative pricing models. If you are in the contract negotiation phase, consider asking vendors about any innovative or nontraditional pricing models that are available. For instance, some vendors are now offering subscription-based pricing — which alleviates the near-term hurdle associated with a software purchase — enabling enterprises to opt for a fixed annual payment price for the term of the contract. Other examples include moving from the traditional perpetual license to a per-processor model.

How Can You Cut Costs With IAM Programs and Operations?

Deriving direct monetized benefits from IAM programs remains a heated topic. Although there are published examples on how to save money and time with core IAM functions (such as password reset/management), clear financial returns for broader, more complex solutions in administration and intelligence remain elusive. However, IAM, for enterprises that have it, plays a critical role in a challenged economy in delivering real value to cost savings initiatives.

Near-Term Cost Savings Opportunities

Leverage existing identity intelligence capabilities to achieve better transparency to access history. Some existing IAM solutions have auditing reporting and analytics capabilities that aren't used or are not fully exploited. Other products have event and information log correlation capabilities as part of an enterprise security audit/monitor/intelligence strategy. Having such solutions provides greater transparency into who has access and (where used) what resources they accessed. This transparency results in less time for auditors to audit, quicker response by IAM operations in correcting problems, and fewer mistakes made during initial provisioning, resulting in cost and time savings. This is primarily a process review issue, but IAM intelligence tools can be leveraged as a result.

Optimize your IAM operations organization with partner knowledge. The maturation of IAM has resulted in a body of knowledge regarding "success practices" for organizing to deliver IAM. These practices reside largely in consulting, integration and vendor knowledge pools. As consumers of their solutions, you have the right to aggressively pursue that knowledge, even if the IAM deployment project or program is over. Organizational structures, required skill sets and operational practices should all be reviewed in light of this interaction with your vendor and service partners. Leveraging the IAM organization more efficiently results in broader security management efficiency and a reduction in the time required for key security and identity processes.

Evaluate IAM managed services selectively. For enterprises with established IAM, this is the period to calculate the operational costs and begin comparisons with established managed services. Although some IAM infrastructure elements (such as critical identity repositories) may not be suitable for some enterprises to consider outsourcing, a significant range of IAM capabilities are eligible for consideration (such as Web access management and elements of federation). However, without a clear view of current operational costs, this evaluation is premature.

Apply streamlined identity administration to minimize per-user software licensing costs. Enterprises can use account provisioning reporting to more accurately determine how software is being accessed and used in the enterprise. Where excessive licensing is applied due to user

count ranges, they can be reduced. Administration reporting also provides protection from deprovisioned, disgruntled employees — former and current.

Longer-Term Cost-Savings Opportunities

Champion IAM's contribution to the enterprise. With the operational efficiencies that can be realized with IAM, it is critical that awareness of those efficiencies reach those responsible for funding it. This means recording the successes in IAM operations in streamlining process, focusing budget requests only on critical gaps, providing ranges of options for funding when such decisions need to be made by them, and providing examples of active participation between IAM operations, security administration and security planning. Awareness results in better, more informed budget negotiations.

Consider efficient IAM options that support SaaS applications. Customers seeking security and IAM solution technology have made very similar mistakes with each generation of IT architecture, whether mainframe, client/server or Web. Those mistakes enable the proliferation of applications or services without a means to secure and manage them effectively. IAM solutions (such as Web SSO and federation) that actually provide services for SaaS environments are receiving increasing scrutiny to offset the security costs of consuming SaaS solutions in a challenging economy, rather than installing applications and infrastructure. Review and consider them before allowing the proliferation of SaaS applications to repeat history.

Identify IAM's contribution to reducing the costs of managing operational risk. IAM intelligence solutions (such as identity auditing and analytics, and role life cycle management reporting) are contributing to the broader planning and implementation of IT governance. Existing compliance reporting and forensics capabilities using IAM information also support subscription services reporting by linking service usage with people and organizations, which is a step toward providing chargeback mechanisms in SaaS environments, as well as enhanced cost center metrics. This contributes to mitigating operational risk through cost avoidance and establishes the role of IAM with governance, risk and compliance management.

Consider IAM use for infrastructure consolidation, support of telecommuting and streamlined application development. IAM monitoring and report output provide an effective foundation for supporting consolidation of systems (and thus access to them), the means to provisioning and assigning access to employees working from home, and the capability for delivering architectural guidance in repeatable and sustainable authorization for application developers.

RECOMMENDED READING

"Identity and Access Management Technologies Defined, 2008"

"Identity Services (in) the Cloud"

"Cost Cutting in Enterprises, and Six Ways Identity and Access Management Programs Can Help"

"Tips for Negotiating Identity and Access Management Contracts"

"Developing IAM Best Practices"

"A Decision Framework for Initial Identity and Access Management Planning"

"Open Your Eyes to the Potential of Open-Source Identity and Access Management"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner