
Enterprise Networks: Managing Identity and Access

October 2004

Executive summary.....	3
Introduction	5
Research methodology	5
Respondent demographics	5
Key findings	6
Current practices in identity and access management	6
End-user management.....	9
Rating identity and access management performance	13
Identity and access management and Security: Vendors and vendor ratings.....	14
Appendix	19

Executive summary

October 2004

Users' identities and their access to enterprise information networks and systems provide the foundation of business operations today. The rapid growth in access points, multiplied by the increase in the number and types of users inside and outside the enterprise, has resulted in a proliferation of user types and identities. The key challenge then becomes knowing exactly who is supposed to have access to what, and making sure each user has secure access to only the resources they are entitled to, while logging and reporting what they've done while connected. This latter function is especially important in light of increasingly stringent security and privacy regulations. This critical aspect of IT is referred to as identity and access management.

TechRepublic conducted a study among nearly 300 US IT and business professionals from organizations with 500 or more employees to examine best practices and key issues surrounding identity and access management. The key insights from the study are:

- *Enterprises manage an increasing variety and number of end-user types.* One-third of respondent organizations have 4 or more end-user types for which they provide identity and access management to the firm's networks and systems. Coupled with this is the challenge of providing more complex and sophisticated services as part of identity and access management.
- *IT security and identity and access management are best delivered by internal teams.* More than half of the firms interviewed provide information and systems security through internal teams that are either fully deployed against security and identity and access management or have part-time responsibility for these key services. Only a small number are using external resources for IT security.
- *Most organizations are still managing identity and access management with manual and non-integrated point solutions.* Two-thirds of participants report their business manages identity and access management through manual or non-integrated point solutions, either as stand alone solutions or in combination. Only about 30 percent use an integrated identity and access management solution at this time.
- *There is still room to improve.* Identity and access management vendors can boost customer satisfaction by offering products and solutions that integrate more easily and fully with current systems and processes, which are also easier to use, with lower initial and operating costs. Technology decision-makers also seek solutions that offer better access management and administration features.

These data suggest that although the diversity and number of end-user types are multiplying, as are the number of locations at end-users reside multiply, most organizations are running today's business with yesterday's identity and access management solutions. Around one-third of those surveyed have some form of integrated identity and access management solutions in place but the same number still require one or more weeks to add a new user to the network. In today's fast paced environments, tools that may have worked well in the "one-location one-network" model cannot support a business that thrives on fast IT service delivery from secure and reliable interactions with customers, suppliers, and partners in real-time.

To further substantiate that traditional means of managing network identity and access are increasingly inadequate for today's businesses models, Gartner reports that integrated, product-suite solutions are quickly becoming the mainstream approach to identity and access management.¹ And our respondents

¹ Gartner, October 2, 2002; October 2003.

already understand the need for change. Between 50 and 70 percent named three companies as the leading vendors in identity and access management solutions: Computer Associates, RSA, and Novell. Each of these industry leaders offers their version of a next-generation, integrated identity and access management solution:

- Computer Associates' (CA) eTrust Identity and Access Management Suite is the first standards-based set of fully integrated solutions, with a common portal-based user interface. Our solution enables organizations to streamline management while protecting investments in existing systems, reduces overall costs, and facilitates compliance with regulations. Key features of eTrust solutions include:
 - Role based provisioning and de-provisioning of user accounts using business logic represented in workflow
 - Enforcement of consistent policies across all managed systems, irrespective of the underlying technology (file, URL, web services)
 - Complete single sign-on capabilities from desktop and Web-based applications. In addition, Web Services-based identity assertion provided to combine partners and intranet Web services applications.
 - Robust auditing capability that tracks all identity and access change and usage activity throughout the enterprise.
 - Support for the adoption and deployment of new technologies while fully leveraging and protecting existing infrastructure and resources.
- RSA Security Identity and Access Management products also provide an integrated, efficient, and cost-effective way of centrally managing users and access rights to enterprise networks. Key components of RSA's solutions include:
 - User management that provides authentication and access management along with delegated administration, approval of workflow, and user self-service.
 - Provisioning to activate and de-activate user accounts or profiles across the network quickly, accurately, and efficiently.
 - Robust and reliable authentication of user identities through single sign-on that also allows authorized individuals to navigate seamlessly across those applications and systems they have permission to access.
 - Access management to assign and enforce user access privileges across enterprise networks and systems, for remote or on-site end-users.
- Novell NSure Identity Manager automates and streamlines the secure management of user access rights, passwords and profiles, improving efficiency and reducing IT costs. NSure delivers timely, secure identity management through:
 - User provisioning that provides timely access to the new and existing employees, manages user groups, and administers access based on job roles (including revoking access in real-time).
 - Password management through single sign-on with self-service capabilities, and the ability to create and enforce system-wide password policies.
 - Automation of routine user management and a self-service tool that allows users to update their own profiles.
 - Automated System-wide auditing and reporting to verify users' access and usage histories.

Introduction

In order to understand in more detail how IT organizations are meeting the challenges of identity and access management, TechRepublic conducted a survey to examine best practices and key issues regarding identity and access management. Specifically, we asked respondents about:

- Current practices in identify and access management;
- Types of end-users and approaches to end-user management;
- Overall organizational performance of key components of identity and access management; and
- Identity and access management and security vendors and vendor performance.

The results of the study are highlighted in the following sections.

Research methodology

A survey invitation was sent to registered TechRepublic members between May 1 and May 26, 2004. The Web-based survey was designed to explore and identify the key issues surrounding identity and access management. The results reported here are based on 268 completed surveys collected during the study.

Respondent demographics

Survey respondents were selected from among TechRepublic members who met certain selection criteria, specifically those who:

- Are from a cross-section of industries conducting business in the United States.
- Are affiliated with organizations with 500 employees or more.
- Are primarily IT and business managers and directors, and other technical professionals.

Summary tables of these data are provided in the Appendix.

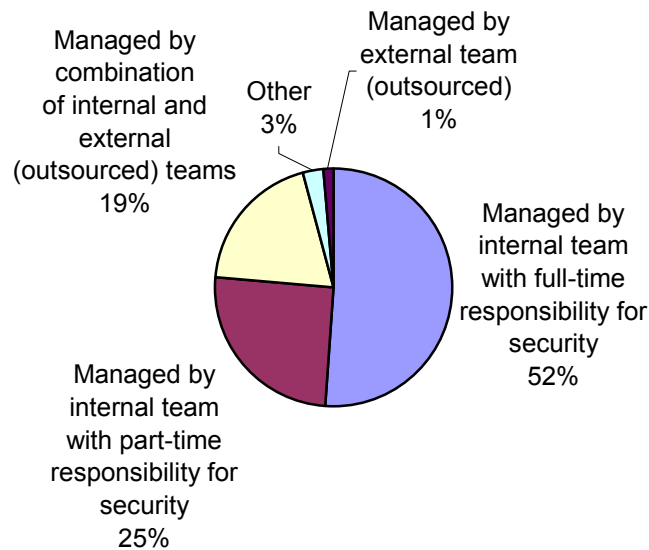
Key findings

Current practices in identity and access management

One objective of the study was identifying current practices with respect to identity and access management. We first asked participants to describe how their organizations currently manage information and systems security.

According to respondents their organizations most frequently handle identity and access management with an internal team with full-time responsibility for systems security (51 percent of responses). Another 25 percent use an internal team that has only part-time responsibility for systems security. It appears that outsourcing is not as common, less than 20 percent of organizations manage identity and access using a combination of internal and external teams.

Which statement best represents how your organization manages information and systems security?

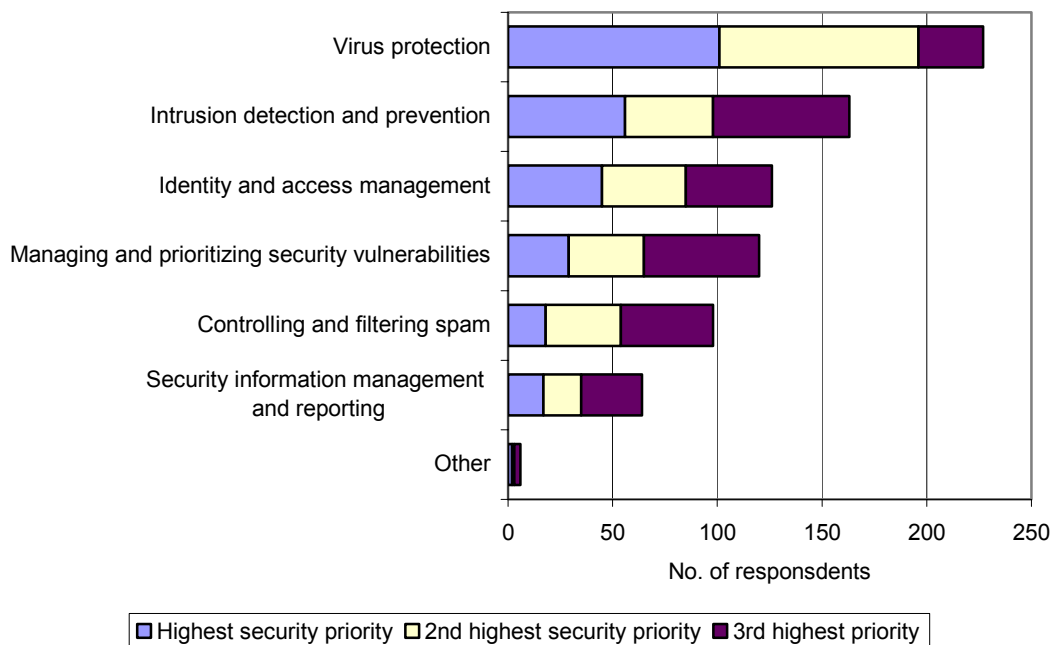


In an effort to understand specific IT security challenges, we asked study participants to identify their top three security issues. Security priorities were ranked on a 3-point scale where 1 = highest priority, 2 = second highest priority, and 3 = third highest priority.

Over 70 percent of respondents ranked virus protection as their first or second highest security priority. Other highly ranked security priorities include (ranked first or second in priority):

- *Intrusion detection and prevention* (37 percent of respondents)
- *Identity and access management* (32 percent)
- *Managing and prioritizing security vulnerabilities* (24 percent)
- *Controlling and filtering spam* (20 percent).

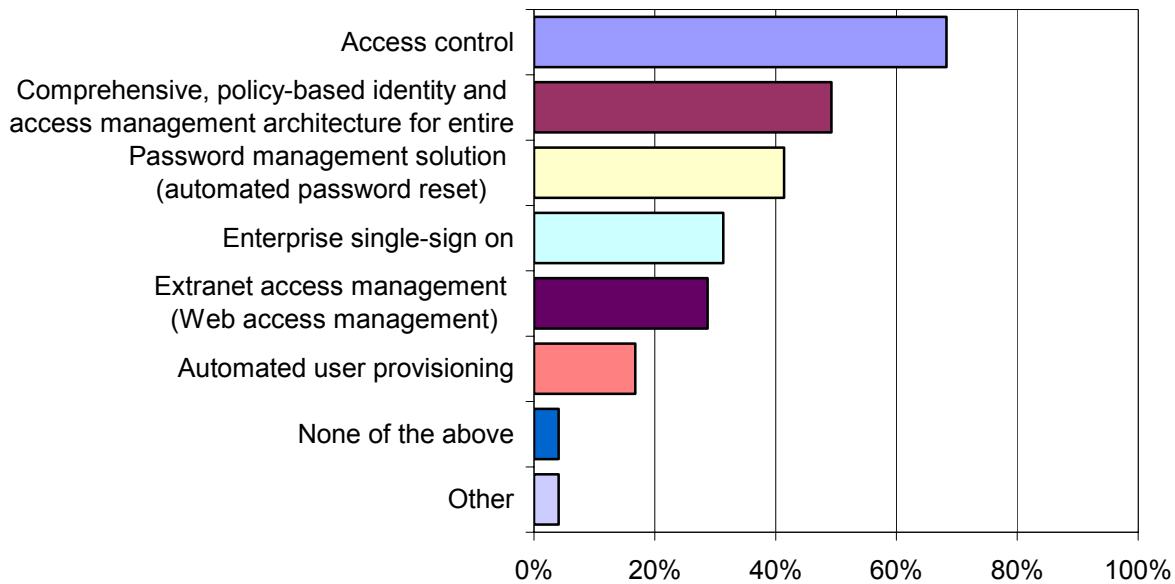
Please choose the top 3 IT security priorities for your organization.



Respondents only ranked the 3 highest security priorities.

Next, we inquired about the current status with respect to identity and access management solutions. Among those interviewed, many organizations are focused on access control (nearly 70 percent). Almost 50 percent of respondents reported they have a comprehensive, policy-based identity and access management architecture for their entire enterprise, followed by solutions for password management (slightly over 40 percent). Enterprise single-sign on (31 percent) and extranet access management (29 percent) garners equal attention among respondents. Less than 20 percent appear to have implemented automated user provisioning.

Which of the following best describe your organization's current status with respect to "Identity and Access Management" solutions?



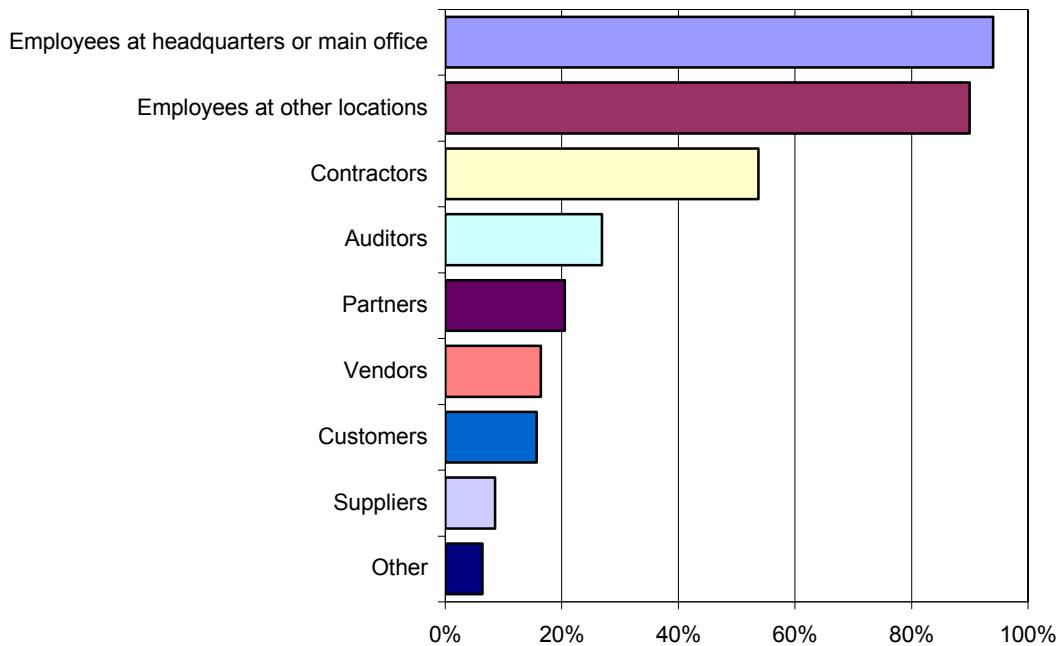
Respondents could select more than one answer.

End-user management

This section of the study provides information about managing end-users. We began by asking study participants about the types of end-users routinely granted access to enterprise networks and systems.

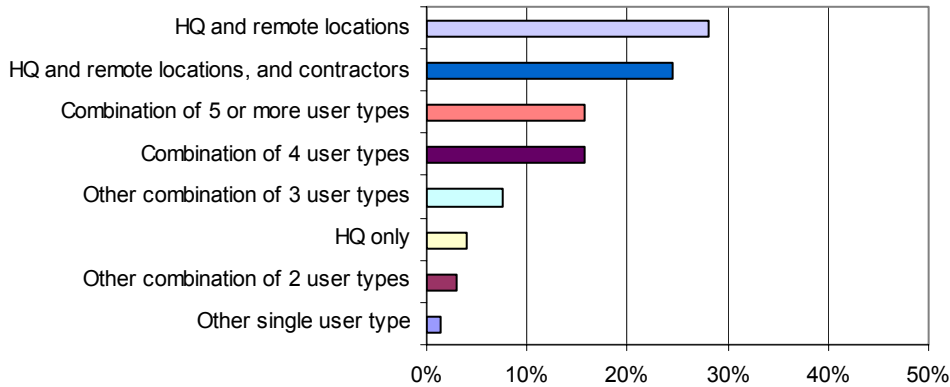
Close to 95 percent of respondent organizations grant access to their enterprise networks and systems to employees at their headquarters or main offices. The next most frequent user group granted access is employees at other locations (90 percent). Slightly more than half give contractors access. Approximately 27 percent of organizations allow access for auditors and 21 percent to their partners. Other less common types of users are granted access less than 20 percent of the time.

Which of the following types of end-users are routinely granted access to your enterprise networks and systems?



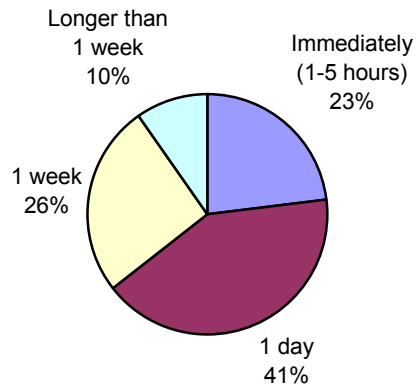
Respondents could select more than one answer.

We delved a bit deeper into the various types of end-users that enterprise support concurrently. We discovered that almost 30 percent routinely grant access to only two user types, namely employees at the main office and remote corporate locations, while another 25 percent issue access for three user types—employees at headquarters and remote sites, and contractors. Nearly one-third of the firms we interviewed have more complex and varied end-user base, providing access to 4 or more end-user types.



Next, we asked respondents to estimate how long it takes to give a new user access to all of the appropriate IT systems. Surprisingly, less than 25 percent can issue access to new users within 5 hours. Less than half can grant access within 24 hours. The remaining third of organizations require 1 week or longer to provide access to new users.

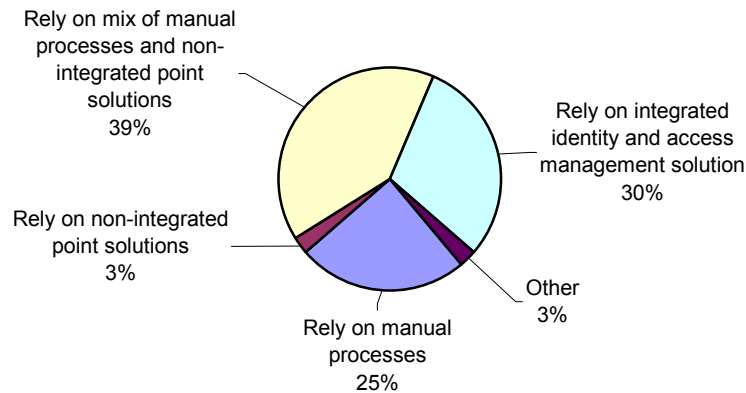
On average, how long does it take before a new user has access to all of the appropriate IT systems?



We also asked survey participants how they manage the identities of various end-users. Their responses are provided below.

Almost 40 percent of respondents rely on a mixture of manual processes and non-integrated point solutions, while only 25 percent report using only manual processes. Thirty percent rely on an integrated identity and access management solution. For a few respondents (3 percent), identities are managed using non-integrated point solutions, and a similar number reported other solutions such as a mixture of integrated and manual processes and in-house software.

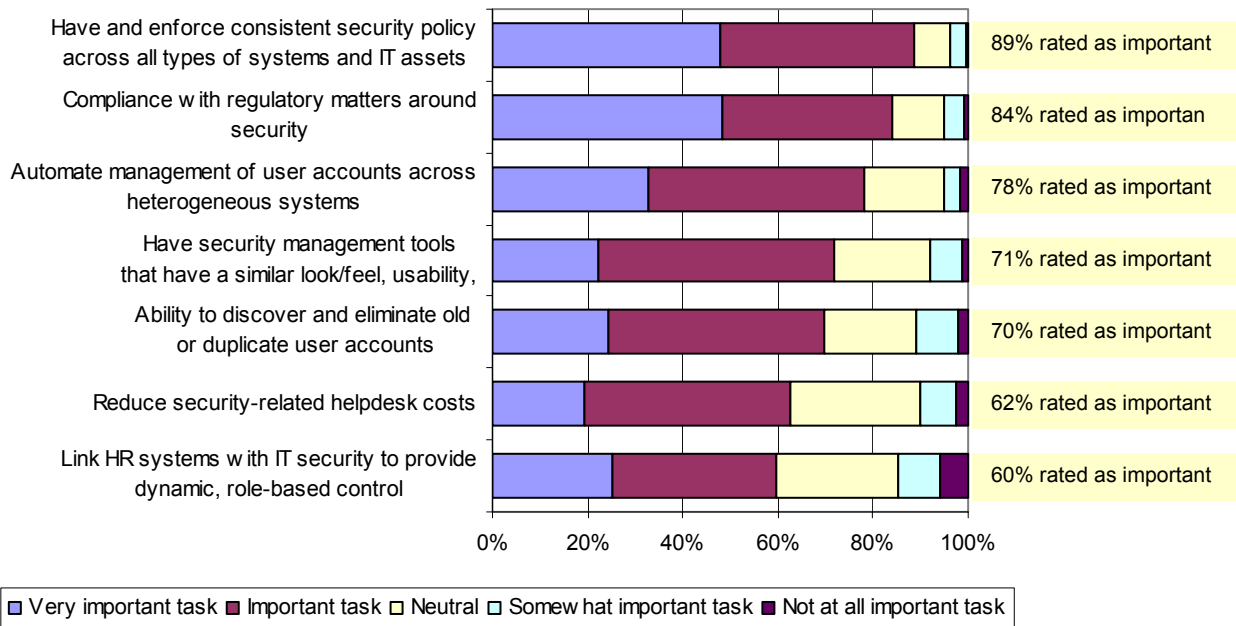
How do you currently manage the identities of your various end-users?



Rating identity and access management performance

In this section of the study, we asked participants to rate various identity and access management tasks and rate how well their organizations currently perform these tasks. We began by having them rate the importance of identity and access management tasks. Ratings were scored on a 5-point scale where 1 = very important, 2 = important, 3 = neutral, 4 = somewhat important and 5 = not at all important. These ratings are shown below.

For each of the following identity and access management tasks, please indicate the IMPORTANCE to your organization.

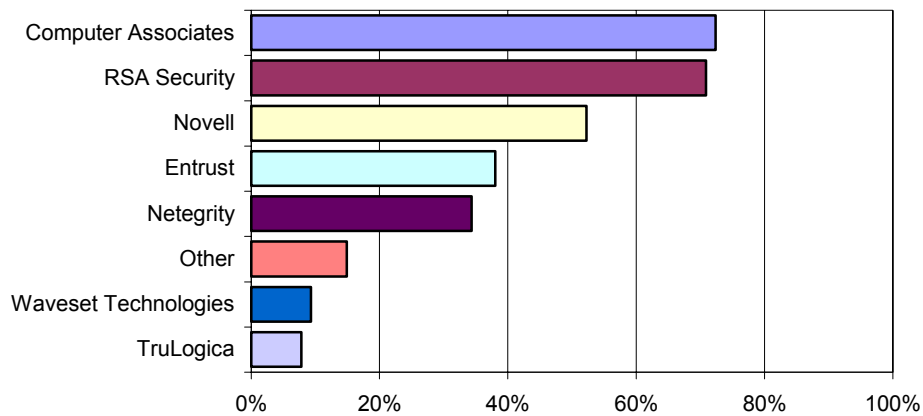


Respondents rated each task.

Identity and access management and Security: Vendors and vendor ratings

In this section of the study, we asked participants several questions relating to the organizations future requirements for identity and access management. First, we asked them to identified the identity and access management market leaders. Current opinion holds that Computer Associates, RSA Security and Novell are the top three market leaders in this space.

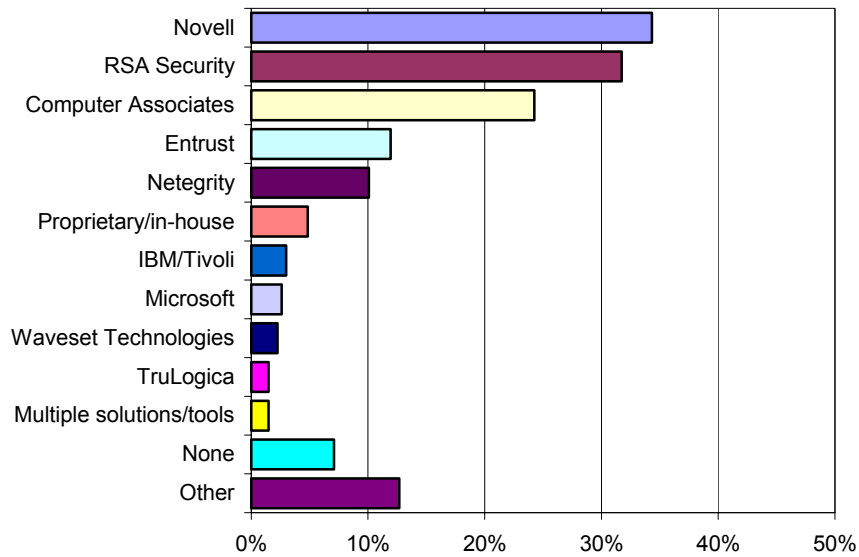
Which vendors do you believe are the top 3 market leaders in identity and access management solutions?



Respondents chose the top 3 market leaders.

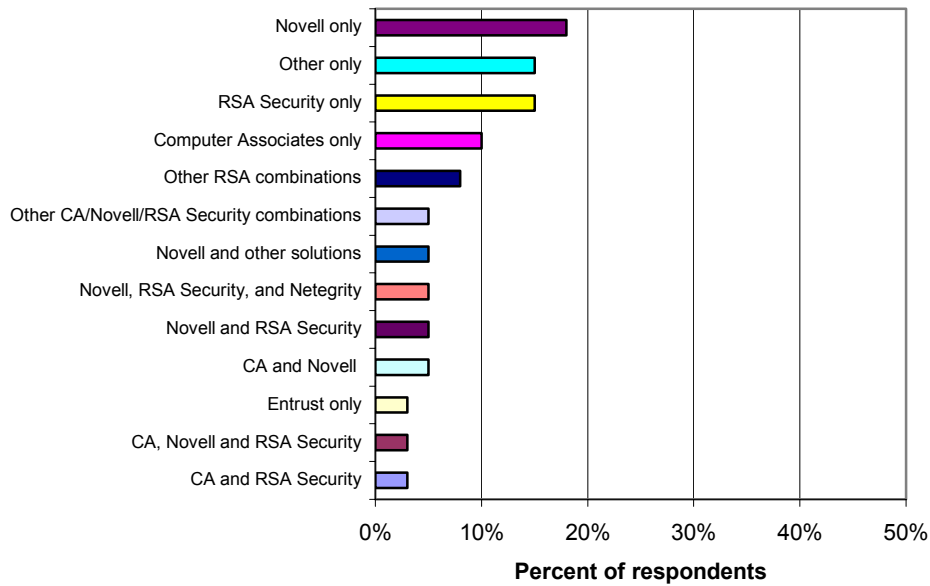
Next, we invited respondents to identify their current identity and access management solution provider(s). Amongst our sample, over 30 percent of organizations are using Novell and RSA Security, while about one-fourth are using Computer Associates identity and access management solutions. The other vendors are used by much less than 20 percent of those surveyed.

Which vendor(s) are you currently using for identity and access management solutions?



Respondents could select more than one answer.

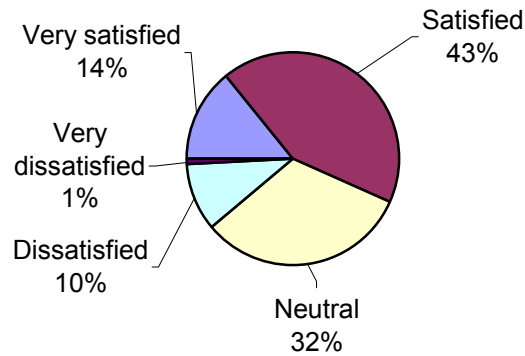
While this chart tells us the overall distribution of these solutions among our sample, we wanted to know the specific stand-alone identity and access management solutions as well as the particular solution combinations that are being used by our respondent organizations. Approximately 70 percent of our sample uses a single solution for identity and access management, either Novell, RSA, Computer Associates, Entrust or another identified solution (the “other only category”). The remainder report using a combination of solutions for identity and access management, namely combinations of well-know products and home-grown tools.



N=239, includes only those who reported a specific solution.

We also expanded our inquiry to touch on the overall level of satisfaction respondents have with their enterprise security solution. Only about 15 percent of our respondents are very satisfied with their current security solution, while around 43 percent report they are at least satisfied. The remaining 43 percent of our sample are not very impressed with their solutions(s) or are actually dissatisfied.

How would you rate your overall satisfaction with your current security solution?



As a follow-up to the security solution rating question, we asked participants what their vendor(s) could do to improve customer satisfaction. Their open-text responses were classified and the results are highlighted in the table below.

Suggested improvements	Percentage of respondents
Better integration	21%
Ease of use	17%
Reduce costs	14%
Better access management/administration	9%
Improved/more features/tools	6%
Better reporting/communications/alerts	6%
Better support/service/training	6%
Better flexibility/compliance/compatibility/stability/security	6%
More customization/in-house influence/control	5%
More speed	3%
Better policies/directories	3%
Other improvements	4%

For this analysis n=145 and includes the open-text responses of those who had specific suggestions for improvements.

Appendix

The following tables contain the breakdown of the respondents by key demographics: organizational size, job role, and primary industry.

Organizational Size

Number of employees (all locations combined)	Percentage of respondents
500 – 999	15%
1,000 – 4,999	36%
5,000 – 9,999	18%
10,000 or more	31%

Primary job role

Job role	Percentage of respondents
IT director and manager	26%
Network or systems technologist	17%
Technical service and support	16%
Business management	15%
Developer	9%
Other technical professionals	8%
IT executive	6%
Security IT director and manager	3%

Primary industry

Industry category	Percentage of respondents
Government (Federal, state, local, including military)	20%
Manufacturing	15%
Education	13%
Health care, life sciences, and pharmaceutical	12%
Finance, banking, and accounting	9%
Business services (computer-related)	7%
Technical/Basic R&D	6%
Real estate, legal, insurance	5%
Transportation, communication, and utilities	3%
Architecture, construction, engineering, and mining	3%
Business services (noncomputer-related)	2%
Retail	2%
Other	3%

Other industries include non-profits, hospitality, and human services.

CNET Network's TechRepublic Community Research Programs

CNET Networks TechRepublic Community Research team conducts surveys of the CNET and TechRepublic membership on a project basis. Projects are funded by CNET Networks and in some cases by vendors who have particular interests in topical areas. In cases where the project has been sponsored by a third party, the Community Research team leads the effort in developing survey questions and has final approval of all questions. The Community Research team conducts all analyses and writes the final report that is subject to CNET Networks' editorial review. Funding for this project was provided by Computer Associates International, Inc. If you have a topic of interest for either editorial or sponsored research, please e-mail us at research@techrepublic.com.