IDENTITY MANAGEMENT

Executive Summary

Among the biggest challenges federal users face in deployment and downsizing their IT environment are budget constraints, knowledge transfer and maintaining adequate staffing levels, according to respondents to an online survey conducted by Federal Computer Week (FCW) last month.

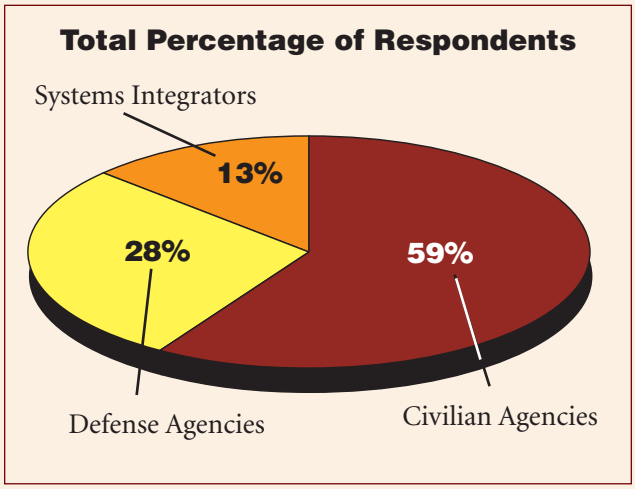
Of the 120 government and industry officials surveyed, the largest percentage, 70%, said security is their biggest concern in trying to securely manage the design, implementation and support of operational servers. Of least concern, according to 38% of respondents, is managing commercial off-the-shelf (COTS) applications.

Interestingly, many survey respondents had no estimate for how long it will take for their organizations to meet security compliance guidelines. On average, 2/3rds of respondents couldn't estimate the phase at which their organization is currently positioned in meeting those regulatory requirements.

The survey created by Microsoft Corp., and Quest Software, and conducted by FCW Research Online was designed to gain understanding about federal sector knowledge and acceptance of Active Directory and identity management practices.

Of those practices, most said they were not aware of a timeframe for having reduced or single sign on for identity management. Given the choice of investing in additional staff, using existing resources, outsourcing using COTS products or doing nothing, the largest number of respondents reported they are using COTS products or working with existing resources to reduce the cost, complexity and operational challenges associated with account management and provisioning.

The results of this survey indicate that government IT professionals could use more education on the importance of Active Directory and identity management in meeting compliance deadlines, and consolidating sign on access to systems.



In this survey, 59% percent of respondents were from civilian agencies and 28% worked in defense agencies, and the remaining 13% were systems integrators. In terms of job function, the largest percentage, 33%, worked in computer, communications or network management, followed by 29% who worked in executive or command positions. In all, 37% had purchasing power greater than $1 million (with more than 3/4ths of those with budget responsibilities exceeding $10 million). In some survey questions, the total number of responses exceeded 120, because executives were asked to check all that apply.

Other interesting findings include:

- Security, cost and lack of resources were cited by many respondents to explain the lack of progress on compliance with regulations that mandate single sign on. Most want systems integrators to assist in reducing costs.

- Many respondents seemed unsure of the link between Active Directory and other operating systems, nor the breadth of operating systems their organizations are currently using.

Using Active Directory to Achieve Critical Identity Management Goals

Despite directives and regulations such as HSPD-12/FIPS 201 and FISMA, and the ongoing climate of heightened security throughout the federal government, most defense and civilian agencies are still struggling with how best to resolve the identity management challenge.

While many have started rolling out smart cards to identify who is accessing buildings and information, most organizations haven't yet tied smart cards into human resources and logical access systems. A chronic need for integration has led to confusion. Clearly, Federal Computer Week's survey results demonstrate that many agencies are torn about whether to invest in additional systems, software and services, which will add more moving parts, rather than simplifying or streamlining identity management processes. Perhaps this is why so many respondents didn't have an answer as to when they will fully comply with identity management mandates.

What federal leaders need to understand, is that much like Dorothy in the Wizard of Oz, government entities can use what they already possess to resolve the identity management challenge. While it may not be as simple as clicking their heels, most agencies can use current resources, rather than investing in point solutions that may add complexity and lead to integration problems down the road.

Optimize What's There

This is precisely why Microsoft Corp., and Quest Software Inc., have joined forces to promote Active Directory as the primary component of a strong, yet simplified identity management solution. Because Active Directory (AD) is already available in approximately 90% of government IT environments, and many organizations are also already using identity management solutions from Quest Software as well, it's critical to investigate using AD to streamline processes for stronger authentication and identity management. Quest Software tools, for example, can integrate non-Windows platforms into Microsoft's widely used AD environment. "Federal customers will not only save time and lower their total cost of ownership, but by leveraging AD, they will also dramatically strengthen the security of both their physical and IT infrastructures," said Jeff Stratyner, Director of Identity Management Solutions, Quest Software Public Sector Group.

Infrastructure Optimization Benefits

Quest Software and Microsoft can help government accomplish more with Active Directory and Identity Management solutions, enabling agencies to:

- Simplify and optimize the identity management infrastructure;
- Automate provisioning and de-provisioning;
- Ease the burden on helpdesks with automated password management;
- Audit changes made to Active Directory and MIIS;
- Extend Active Directory, MOM and SMS to non-Windows environments; and
- Utilize existing technologies and skill sets to get the job done.

Via the new Infrastructure Optimization Initiative (IOI), Microsoft and Quest will work with customers to create a roadmap that will help each agency get a better handle on identity management. Each roadmap will show how to meet federal mandates, and based on current security requirements, will define how much security is needed to satisfy specific agency goals. "Optimizing what's already in place, and filling the gaps with solutions from partners such as Quest Software can help any agency find the best path to process optimization, along with stronger security," said Curt Kolcun, Vice President, Microsoft Federal.

As a Microsoft Gold certified partner, Quest Software can assist government agencies to overcome just about any integration hurdle. This is because Quest Software provides not only authentication to non-Windows environments, but also lifecycle asset management and advanced security services as well. Together, Microsoft and Quest Software can provide federal defense and civilian agencies with the roadmap to guide them on the journey down that yellow brick road to streamlined processes and more secured operations.

MARK YOUR CALENDARS:

April 19, 2007 - ***Managing Your Multiple Identity Disorder***
www.quest.com/public_sector/

June 6, 2007 - ***Attaining the Active Directory & Identity Management Solutions for Your Agency Webinar***
www.microsoft.com/federal/webcasts

Microsoft®

QUEST SOFTWARE® PUBLIC SECTOR GROUP
Government and Education Solutions