TRANSFORMING AGENCY SECURITY WITH IDENTITY & ACCESS MANAGEMENT

EXECUTIVE RESEARCH BRIEF

DELL Software

FOUR POINTS TECHNOLOGY
A Service Disabled Veteran Owned Small Business


USER LOGIN

TRANSFORMING AGENCY SECURITY WITH IDENTITY & ACCESS MANAGEMENT

The rampant increase in cyberattacks, mounting regulatory requirements, and the constant concern over insider threats mean that securing your agency's resources is more important than ever. Yet at the same time, agencies face budgetary constraints, staff shortages, and a host of conflicting priorities that result in basic security protocols—things like ensuring users have appropriate access privileges and verifying that passwords are regulatory compliant—being neglected.

In a recent GovLoop survey of more than 250 federal, state, and local government employees **(figure 1)**, we found that the inability to create an effective identity and access management (IAM) system was a major challenge to many public sector organizations' security efforts.

To discuss how agencies might tackle this dual challenge of security and fiscal restraints, we spoke with Dan Conrad, Identity and Access Management (IAM) Specialist at Dell. He explained how creating a holistic, automated, and centralized IAM system could actually save costs while increasing security at government agencies. He also offered guidance on how to create such a system in the face of other agency challenges.

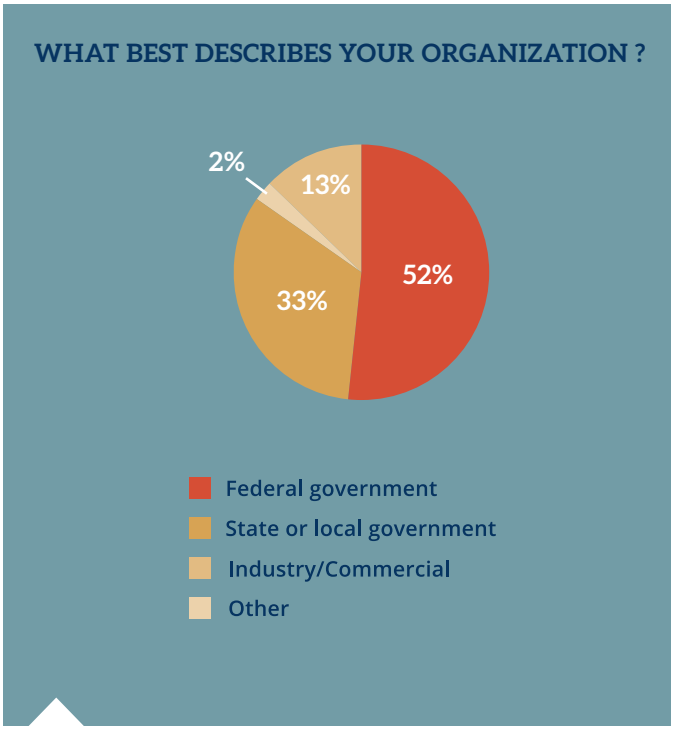


FIGURE 1

BARRIERS TO ROBUST IDENTITY & ACCESS MANAGEMENT

The risks associated with an ineffective IAM system are severe. Among survey respondents, decreased security was a major concern, as was the potential of unknowingly breaking regulatory compliance **(figure 2)**. However, many agencies continue to struggle with building a robust and comprehensive system of access controls. A lack of effective governance, inconsistent methodologies, IT staff constraints, and weak management buy-in were common challenges. We discuss these challenges in-depth below **(figure 3)**.

Challenge #1: Lack of Central Governance

In many agencies, user accounts, access privileges, and protections are managed in disparate settings by a variety of departments and platforms. One survey respondent, when asked what data source informed their IAM system, replied, "I don't know. We have a dozen systems that are all handled differently." That answer was unsurprising – and quite common.

Less than 20 percent of survey respondents' organizations use a single IAM system to regulate access across their agency. Additionally, 30 percent of respondents reported having to maintain more than five different user names or passwords to accomplish their daily tasks.

This scattered governance of multiple accounts and privileges can be extremely detrimental to agency security. First, maintaining various systems with different access protocols often leads to employees creating shortcuts or workarounds in order to simplify their access. "If you don't make [a log-in system] easier for the users to use, they're going to find a way to make it easy, and you won't like how they do it," said Conrad. Tactics like creating linked or easily recallable passwords compromise agency security as well as regulatory compliance.

Additionally, the lack of central oversight makes it difficult to ensure each account and its related privileges are consistently appropriate. One survey respondent described the way user privileges are removed following an employee departure from their agency: "HR and, honestly, word of mouth. In other words, 'Oh man, they left six months ago? Take them out of the system now!'"

Without a central governance structure to oversee employee accounts, the risk of accounts becoming inflated with unnecessary privileges or defunct following a departure is high. Even worse, insufficient oversight can lead to indicators of inappropriate user behavior—even possible insider threats—being missed.

Challenge #2: Inconsistent Methodology

This lack of central oversight is often linked to an inconsistent and often insecure methodology for prescribing and changing access privileges. One survey respondent described the way access privileges are granted at his organization: "It's dependent on the system. Some by the user roles, some by department memberships, some by user request, some by individual basis as determined by administrative folks."

Because there is no overarching strategy for managing and consolidating these disparate accounts, changes to accounts are often done on an ad hoc basis with little consideration for how one change may impact other accounts and privileges for that user. Conrad said, "In the best case scenario, you would call the help desk, the help desk would figure out what you needed access to, retract your old access, and then contact the resource owner to determine if you should actually have access to that."

WHAT ARE THE TOP CONCERNS ASSOCIATED WITH AN INEFFECTIVE IAM SYSTEM AT YOUR ORGANIZATION? (PLEASE RANK)

	OVERALL RANK
Risks agency security	1
Risks breaking regulatory compliance	2
Prevents users from accessing necessary information	3
Increases network complexity	4
Consumes unnecessary IT staff time and resources	5

Total respondents: 212

FIGURE 2

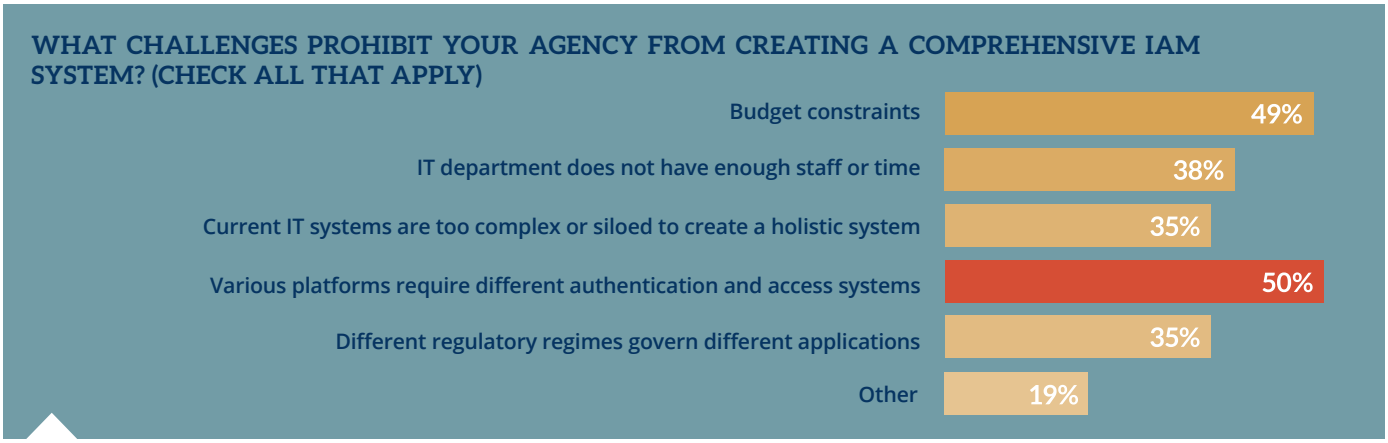


FIGURE 3

Unfortunately, that rarely happens. "Nine times out of ten, [IT administrators] grant access, without really knowing that access to the resource is even necessary. And then you change departments, you open another ticket to get different access, so you get more and more access," said Conrad.

The problems with this inconsistent methodology are two-fold. Granting unnecessary access privileges to users is an obvious security and regulatory risk. Moreover, because different departments and managers grant these privileges inconsistently, there is no audit trail. In the event that a department wants to perform due diligence on a user account and audit access privileges, they would find it nearly impossible to do so given the ad hoc nature with which those requests were logged and granted.

Challenge #3: Burden on IT Staff

To compound management barriers, agencies without a comprehensive IAM system are likely to face resource constraints. When there is no central governance structure or automated request systems, the burden of maintaining user privileges and access most often falls to IT staff. In fact, 38 percent of survey respondents said that their IT department did not have enough staff or time to create and maintain a comprehensive IAM system.

This stress on a constrained department is likely to lead to oversights in access privileges, lags in request processing, and increased burden on individual users to track their accounts. What's more, the time IT staff will relegate to basic IAM maintenance is time lost on monitoring more pressing and high-level organizational needs. As a result, other security risks may be overlooked.

Challenge #4: Budgetary Constraints

Yet even as inappropriate governance, inconsistent methodologies, and unsupported IT departments continue to degrade the effectiveness of IAM systems, many agencies have not taken strides to improve their processes. Why? The lack of progress is largely the result of budgetary constraints coupled with a lack of internal support for improvement.

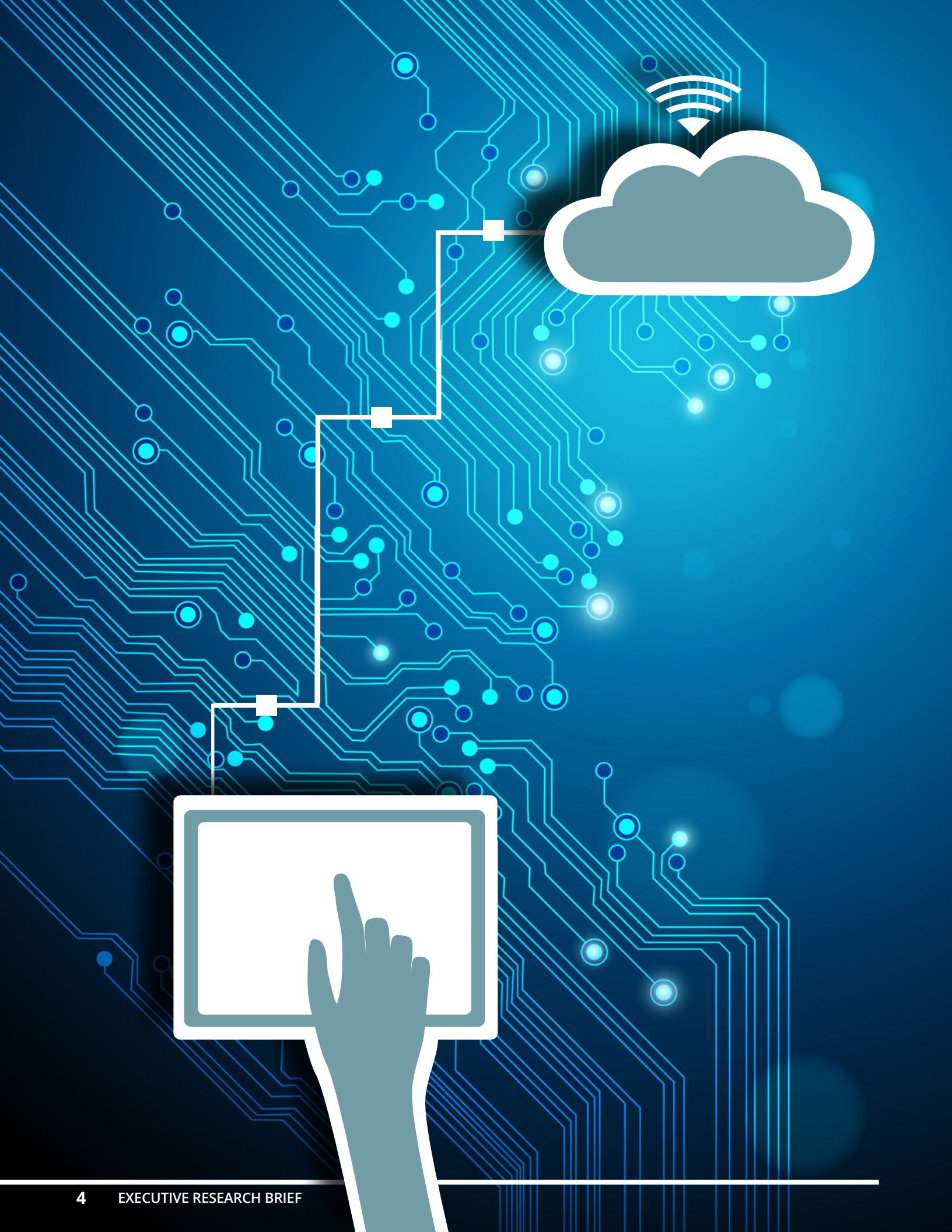
Nearly half of survey respondents said that budgetary limitations prohibited their agency from creating a comprehensive IAM strategy. Conrad said this is unsurprising. Not only are agencies grappling with reduced funding, many personnel find it difficult to get financial support for a project whose cost-savings are not obvious.

"It's really hard to put a dollar value on it unless it happens to you and then you have to go back and figure out what it cost," said Conrad. "Being proactive can definitely save money, but it's fairly hard to justify allotments."

In many cases, it takes the agency being the victim of an internal breach for managers to take IAM needs seriously. "Past experience is always a big one. That changes the game quite a bit, when something is actually exploited," said Conrad. "Budget follows incident. You hate to see it work that way. We always like to be proactive, but that's not always the case."

In order to avoid security breaches, agencies must proactively assess, modify, and centralize their IAM systems. In the next sections, we explain how to accomplish this task by overcoming the challenges of buy-in, decentralized governance, and IT staff overstretch.

> "If you don't make [a log-in system] easier for the users to use, they're going to find a way to make it easy, and you won't like how they do it,"
>
> *- Dan Conrad, IAM Specialist at Dell*



THREE STEPS TO CREATING AN AGENCY IAM STRATEGY

The first step to securing your agency is to revise your overarching IAM strategy to ensure that it meets your agency's needs. Conrad suggested starting any revisions by examining your current status: "Identity and access management is an evolving term that means different things to different people. You really have to consider what it means to your organization and what is currently covered under that umbrella."

For example, an agency primarily concerned with national security will unquestionably consider user account security a top priority and will require robust credentialing and authentication mechanisms. Alternatively, an agency whose information is primarily public may be more interested in streamlining the user experience across applications.

Then, consider if the current state of your IAM system is effectively serving your mission and securing your organization. If it's not, you'll want to develop a new strategy that consolidates and enhances your IAM functionality. This is a daunting task, but Conrad laid out steps to determine your IAM priorities and begin to revise your strategy for access management.

Step #1: Secure Management Buy-In

First and foremost, Conrad said that it's crucial to secure buy-in from managers before revising your IAM strategy. "We get calls from architects and project managers who want to do identity management, but when we really get involved with the process, we find that they have partial management buy in, but they don't have 100% management buy in," said Conrad. "So the project may get off the ground and moving slightly, but then it never really follows through to complete fruition."

To avoid this pitfall, it's important to discuss IAM priorities with administrators and create a strategy that is compatible with organizational goals. "You really have to determine where identity and access management as a strategy lies within the priorities of your organization," said Conrad. "Of course, with most government organizations, that's a dynamic list; things are always moving up and down."

Therefore, you should create a strategy that is going to fit short and long-term agency goals. Cost savings and increased security from insider threats are two benefits that can be expected from a central, automated IAM system and both of these will continue to be priorities for agencies in the future.

Step #2: Start Small

Of course, those benefits will not come overnight. To secure necessary buy-in early in the IAM installation process, Conrad suggested starting with smaller projects that show immediate benefits. "The best practice for moving forward is to take the low-hanging fruit and start to enroll things under central governance, so that users get used to governance and finding better and easier ways to request access," said Conrad.

For instance, rather than consolidating all user accounts immediately, Conrad suggested to start by merging and reexamining privileges for shared drives within an organization. This reorganization will make data governance easier for both users and administrators, and it can be executed with little impediment to current processes. This seamless transition is key. "Anytime you're changing technology in your environment, you always want to give your users the same or better experience," said Conrad.

Step #3: Follow Regulatory Directives

As you begin to revise your IAM procedures, keep in mind that many regulatory bodies have established guidelines that can help steer your strategy. Conrad acknowledged, "Everyone has different needs. They have different priorities, they have different regulations, they have different authentication and even architecture of their organization." That being the case, it might be tempting to dismiss regulatory suggestions in favor of IAM configurations that suit your agency's current technology and processes.

However, Conrad advised against homegrown solutions. "Don't just take those directives and assume that people don't really understand your environment," he said. "Find a way to do what those directives tell you to do, because the technology exists to do it today." What's more, following those directives ensures that your resultant IAM system will be regulatory compliant.

THE NEED FOR CONSOLIDATED AND CENTRALIZED GOVERNANCE

Once an IAM solution is adopted at your agency, it should be placed at the center of the organization and applied to all user accounts and processes. This centralized governance is central to reaping the full benefits of IAM tactics from a cost perspective because it minimizes technology investment by applying one system across processes.

More importantly, an effective IAM technology can protect agencies from the costs of a potential breach because it maximizes user account security. The three features of a centralized system that ensure accounts are managed appropriately – personalized access control, audit trails, and streamlined user access – are detailed below.

Personalized Access Control

According to survey respondents, the business, security, and regulatory rationales for access management tasks are inconsistently relayed to IT staff before those tasks are performed. This is problematic from a security perspective because it means that any access requests handled by IT can't be executed with enough information to ensure security is maintained. Yet only about half of our respondents said that department or business administrators—employees with better knowledge of the processes in question—executed users requests for additional access privileges at their agency.

Conrad explained how this discrepancy can be easily resolved through central IAM governance: "With today's modern technology—with solutions from Dell—we could put that access to resources into the hands of the business process owner through complete automation without having to give the IT help desk any special permissions to grant those resources."

When a user sends a new privilege request, it creates a ticket that is stored and eventually executed by the central IAM system. For a user, this is helpful because any request for access can be submitted to one location. However, the request itself is pushed to the administrator most closely associated to that user and the privileges in question. That administrator then evaluates the request for appropriateness and accepts or rejects it without assistance from the IT department.

While the system that governs IAM is centralized, it allows requests to be managed throughout the organization. "With a centralized system, that access could be evaluated by the person that actually knows if you should have that access," said Conrad.

User Audit Trail

Once that request is granted, it is logged in the IAM system. Over time, an audit trail—a searchable, chronological record of executed events—is created for each user that highlights which privileges are assigned to their account, how those access rights have changed, and who authorized those changes. "Formerly, you didn't have any way to know how someone got access to certain portals or information, who gave it to them or even why they have it," said Conrad. "But you need that auditing capacity, so that you can look at what the person has access to today, and what they had access to six months ago, and give you that full access control picture."

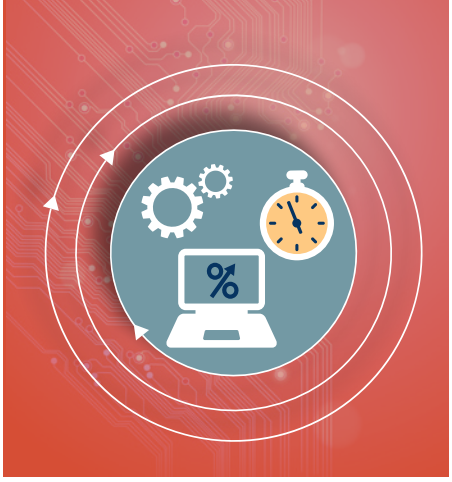
This audit trail provides a holistic picture of how privileges are apportioned at an organization, allowing security personnel to know who has access to what at any given time. It can also alert administrators to changes in user behavior.

For instance, an audit trail may show that a user has submitted multiple denied requests for increased access. This could indicate a potential security threat if the user in question is consistently requesting access to information outside the parameters of their job. Conversely, it may be a sign that the user's current role should be re-evaluated. They may need a higher clearance level in order to execute the tasks required of their job. In either scenario, a centralized system that shows the user's entire access history is key to understanding the context of specific requests.

Streamlined User Access

Finally, a centralized portal for all IAM functions increases the likelihood that users will appropriately request and maintain their user privileges. 70 percent of respondents said users maintained separate credentials for various platforms used at their organization, rather than leveraging a single identity across platforms. As Conrad noted, this creates a security risk because users are likely to create workarounds to avoid diligently maintaining multiple sets of complex access credentials.

A centralized system, connected to all agency portals, consolidates these user logins into a single identity. This not only allows users to submit any privilege change requests to a single system, it also allows them to seamlessly execute their daily tasks without having to recall numerous credentials and login processes. As a result, users will find it easier to securely maintain their online identity.



THE BENEFITS OF AN AUTOMATED IAM SYSTEM

Once you've formed a long-term IAM strategy and created a centralized system, daily maintenance of accounts and privileges will become a substantially easier burden for your agency. Conrad admitted, "When you present an entirely new system to a customer—especially to a person who is new to access control—it can be an overwhelming concept." In fact, a robust IAM system should automate many of the processes currently performed by IT staff.

For instance, 70 percent of respondents said changes to user privileges were executed by IT staff at their organization. Furthermore, 57 percent of respondents said user requests for additional access privileges were processed by IT staff. Yet these tasks can be executed autonomously, if the roles and relevant privileges for requesting individuals are already defined within the IAM system.

"When you can automate and take the person out of the picture, then that would be the best practice," said Conrad. Not only does automation of IAM reduce the probability of human error, it also reduces IT department workload, increases end user productivity, and ensures ongoing compliance of user accounts.

These three benefits, as well as their impact on organizational efficacy, are described in greater depth below.

Alleviates IT Staff Burden

The most obvious advantage of reducing manual maintenance of accounts is the positive impact on IT staff workload. "Take something like password management. Sometimes up to 70 percent of the calls that come into help desks are simple password resets," explained Conrad. "When you give the users the capabilities to reset their own passwords, you can free those help desk people up to do other things and you can get a lot more done with that same amount of money."

With automation, IT labor constraints no longer dictate the efficacy of your IAM processes. And because staff no longer have to dedicate time to routine maintenance of accounts, they are able to dedicate more time to high-level IT tasks like architecture planning and proactive cybersecurity.

Increases End User Productivity

What's more, IT are not the only agency personnel who can expect to become productive as a result of automation. We noted earlier that a central IAM system allows end users to seamlessly transition between processes without having to use disparate logins and credentials. This results in higher productivity, as employees can focus on their responsibility rather than account management.

Automation compounds these productivity benefits. Because maintenance functions like password resets and privilege changes are executed automatically, end users no longer have to wait for IT personnel approval before performing routine tasks. Lag times are eliminated so employees are able to focus on their primary responsibilities, rather than identity upkeep.

Ensures Ongoing Compliance

Automated maintenance also guarantees that accounts, login credentials, and access privileges remain updated and compliant.

Currently, only 26 percent of respondents said that individual permissions were reviewed at least once a year for appropriateness. This is likely because 64 percent of respondents said their IT staff were charged with monitoring user activity for policy violations and 58 percent said the IT department maintained user password compliance. The labor and cost required to review so many records is untenable. However, an automated central IAM system ensures review occurs on a routine basis, without burdening security personnel or costing more for the agency.

For those tasks that are still best assessed by department personnel, this automated function can actually push administrators throughout the organization to periodically scrutinize access privileges, so that exceptions to standard role assignments are thoroughly reviewed. Conrad said, "You can set it up so that person has to actually evaluate that access on a scheduled interval, whether it's once a year or once a week. So that when this person moves around throughout the organization, they don't get what we call 'access bloat.'" This also ensures that access levels remain regulatory compliant, even as users transition to new roles or depart the organization.

To compound these benefits, automation can also be leveraged to gain buy-in for IAM projects-at-large. "When you can show that cost savings on that time for a completely automated solution that actually enhances the security and enhances the administrator experience, the ROI just follows," said Conrad.

THE ADVANTAGES OF SEEKING EXTERNAL SUPPORT

Admittedly, determining just how to use existing technology and regulatory directives is no small feat and many agencies will find it necessary to seek external support to effectively revamp your IAM strategy. "There are third parties that will come in and evaluate your identity and access management system and give you advice and direction. They can guide you to know what's actually possible before you engage your plan," said Conrad.

Conrad also noted that seeking external support could minimize the money and labor required to revise systems by simplifying plans. "Many of our customers come to us with a massive drawing or a whiteboard of what they want to happen. In reality, they're doing a ten step process, when six of the steps are unnecessary due to emerging technology," said Conrad.

Four Points Technology, a Dell partner, provides this sort of evaluation support. Conrad explained how their advisors assist in structuring a strategy and securing buy-in: "They can come in and do an overall evaluation of identity and access management and give you a score. The scores will also be compared to other organizations of similar structure so that you can see where you're doing better in some areas or worse in others. And then they can show you where you can get the most bang for your buck to improve that score. It also gives you something to shoot for instead of just throwing arrows in the dark and hoping that things get better."

"As a Premiere Partner with Dell and working with many of our customers' system security challenges over several years, we recognize that each customer is unique. Some agencies already have good tools, systems, and controls," said Denise Harrison, CIO of Four Points Technology. "But as Dan mentioned, a holistic and architected approach is the only way to ensure user experience improvements as well as security compliance."

ABOUT DELL SOFTWARE

Dell Software helps government agencies unlock greater potential through the power of technology — delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. Dell Software solutions for security, information management and systems management enhance your on-premises, remote, cloud-based, and mobile infrastructure and endpoints. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate results.

www.dellsoftware.com

ABOUT FOUR POINTS

A Service Disabled Veteran Owned Small Business

Four Points Technology, LLC is a CVE-verified Service Disabled Veteran Owned Small Business (SDVOSB) delivering technology solutions to our Government customers around the world. We partner with top manufacturers and software companies to provide our customers with leading edge information technology solutions. As a Federally-focused prime contractor, Four Points Technology offers a strong contract portfolio that includes Government-wide contracts such as GSA Schedule 70 and SEWP IV as well as multiple agency-specific IDIQs and BPAs. Our disciplined approach to the management of product delivery and ancillary services provides access to the latest technology in an environment that supports rapid implementation, clear productivity gains, and short ROIs.

www.4points.com
dell@4points.com

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 150,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington D.C. with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to Hannah Moss, Research Analyst, GovLoop, at hannah@govloop.com.

www.govloop.com
Twitter: @GovLoop

1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421
Fax: (202) 407-7501

www.govloop.com
Twitter: @GovLoop