CSO

Identity Management

SURVIVAL GUIDE

3 identity management challenges | *New Brunswick conquers identity management with virtual directory* | **Identity as an attack surface** | Stop insider attacks with Privileged Identity Management | *What users love (and hate) about 4 leading identity management tools*

The identity imperative

Identity management, as Gartner defines it, is the "security discipline that enables the right individuals to access the right resources at the right times for the right reasons." It sounds like a lofty ideal, but it is at once elemental and essential and, according to Gartner, is "a crucial undertaking for any enterprise."

Password-management tools, provisioning software, security-policy enforcement applications, single sign-on, reporting and monitoring apps, and identity repositories all fall under the umbrella of identity management. Yet for all the technology behind it, Gartner notes that the practice of identity management "is increasingly business-aligned, and it requires business skills, not just technical expertise."

Yet that business alignment is one of the key challenges George V. Hulme so expertly outlines in the lead article in this guide. "IT and business leaders still underestimate what it takes to build a viable identity management program," writes Hulme.

That's where we come in.

We'll help you communicate the challenges, learn from success stories, and dive into the most valuable features of today's identity management tools.

CONTENTS

3 identity management challenges

When it comes to effective identity management, many enterprises haven't made much progress. Here's why.

BY GEORGE V. HULME

Recall the time, perhaps a decade ago, when identity and access management was a struggle. When identities were managed largely through layers of manual processes. When users were often individually provisioned to the applications and resources they needed by the appropriate application owners, or network and system management teams.

Look back to how, in those days, auditors would lug around stacks of three-ring binders crammed with lists of users and resources they could access.

Sound familiar?

Unfortunately, if you're in many large and mid-sized enterprises, these problems may not sound like those of a decade ago. They more than likely sound like problems of the here and now.

For many reasons, when it comes to effective identity management, many enterprises haven't made much progress.

While there's more automation available to provision users to the applications, systems and other resources they need, enterprises still struggle to keep digital identities aligned with the reality of their organizations. And, as the CISOs and identity managers interviewed told us, most organizations still struggle to get the basics right. They grapple with the increased number of and complexity in the applications they use. They strain to map the real-world roles employees provide with their jobs and access levels, and they fight with upper management's check-box and "project" mentality.

With all of that in mind, let's take a look at three pressing identity management challenges organizations face today.

1. Complexity

For many, this is the biggest challenge, but it doesn't always have much to do with technology or the software that vendors provide. It's that the complexity of IT has increased. There are more applications, but there are also more types of applications and resources that employees access. That includes those applications that are provided on-premise, or those, such as Software-as-a-Service, that are based on cloud architectures.

Consider the challenge to simply understand the roles and access requirements for most employees. "Organizations have a very difficult time with the very basic task of figuring out precise job roles and then being able to associate those roles with appropriate levels of access to resources," says Martin Fisher, director of information security at WellStar Health System, a not-for-profit healthcare provider based in Atlanta.

According to Fisher, WellStar is required by policy to have a job description for each of its workers. Those job descriptions must identify employees' authority, responsibilities and deliverables. "That's certainly a valuable thing to have. The problem is that the effort creates a lot — and I mean a lot — of different job descriptions," says Fisher. "For instance, consider a registered nurse who works in cardiology. She is going to have a significantly different job description than a registered nurse who works in a primary care practice. They're both nurses, but they do very different jobs. So at least within healthcare, we're trying to increasingly embrace the idea of role-based identity and move away from thinking just about positions, but it takes a lot of work and a lot of time."

2. Treating identity management as a project

Despite the fact that the complexity of identity management trips up enterprises, many IT and business leaders still underestimate what it takes to build a viable identity management program. That's why it's often a challenge to convince executives that it's necessary to invest properly in identity, not so much in the technologies and the toolsets but in the effort it will take to gain a full understanding of how workers operate and then build the IT processes to reflect that reality.

That was certainly the lesson learned by the identity manager at a mid-sized food processing company based just outside Milwaukee. The company had invested in an identity management suite with the hope of speeding the provisioning of users to the resources they needed. It was a function that had became burdensomely slow as the company began growing more quickly. "We bought and installed the software, however the initiative eventually ground to a stop after we managed to get sign-on to a few of our major enterprise applications," says the identity manager, whose company didn't permit attribution. "We have a large number of old applications. Applications that reside on the production floor and in the warehouses don't often change. Initially, we wanted to control identity for most of our applications, but management wouldn't fund the upfront work required to study employee and contractor roles and to map that to the appropriate applications," he says.

That unfortunate outcome doesn't surprise Drew Koenig, user access manager at a health services firm based in Minnesota. "When organizations get a few months into these implementations, it turns out that 90 percent of the team's efforts focus on educating the business leaders, managers and data owners," he says. "And getting the organizational mentality right that it's the data owners, not the group managers, that approve access. You need to successfully get through all of that before your initiative can progress."

Fisher agrees. "You not only need to have executive sponsorship, because your effort is futile without it, but also eager buy-in across multiple business units. If you don't have all of that support in place, you are going to have a large number of potentially insurmountable challenges," he says. "You're really working on the very fabric of the organization. And if you screw that up, the cascade of problems that generate can sap so much productivity and add so much cost to the environment."

Those costs can include everything from workers not getting access to the applications they need, to end users deciding to share credentials so they can get work done, to increased difficulty responding to valid audit requests.

It's for these reasons that many identity management professionals say that the bulk of the effort is in the enterprise's approach to adoption, and the technology and tools are the least of the focus. "I think a lot of the faulty mentality toward identity management can be blamed on the vendors," argues Koenig. "They're trying to sell software and push the notion that a multimillion-dollar identity management suite is going to get you identity management. It doesn't. Identity management is not like a service desk or a project management suite or a utility type of product where it does this one thing. Identity management, as an implementation of business processes, goes much deeper than that."

3. User authentication gone bad

One of the cornerstones of successful identity management is good authentication. Currently, most organizations still rely on username and password combinations to vet access. As we've witnessed through recent attacks, such as the breaches experienced by social networking site LinkedIn or music site Last.fm that exposed millions of usernames and passwords, passwords are not always the most secure way to control account and resource access.

Yet don't expect passwords to disappear anytime soon. Many of the stronger authentication methods — because of their own complexities and costs — have failed to gain much traction in the market.

Joe Van Overberghe, IT manager at the Otis R. Bowen Center, a behavioral healthcare services provider in Indiana with 700 employees spread across nine primary locations and additional satellite offices, knows the challenges of strong authentication all too well. Until recently, only a few of the Otis R. Bowen Center's healthcare workers would regularly access its systems remotely. However, as the center began moving in a significant way to electronic medical records, that began to change. "With electronic medical records, we suddenly had an explosion of the need for remote access," explains Overberghe.

Until recently, for remote access, the center had relied almost entirely on a hardware token that fit on a key ring. However, as a healthcare nonprofit that must watch every dollar closely, hardware tokens deployed widely throughout the organization would probably prove too expensive. "They're hardware, so they're costly. People aren't very friendly on hardware devices. They break them. The batteries run out and they're not replaceable. They are lost. So you end up constantly having to buy new tokens. We needed to figure a way to keep costs down and manage the expense," he says.

Overberghe began investigating other alternatives, such as software-based two-factor authentication provided by WiKID Systems. With WiKID, a user enters a PIN, a username and the one-time passcode into a software-based token, for access. "End users can have as many software tokens as they want within a domain and they can use any device that they have," says Overberghe. Currently, the Bowen Center has about 30 users transitioned to WiKID, and, explains Overberghe, all new users are being set up this way. "We now have people calling and asking if they can just use their phone and get rid of their old hardware token," he says.

Putting a solid identity management system in place is worth the effort, despite the challenges. Identity is the foundation of good security and solid regulatory compliance. To succeed, it requires a bit of savvy planning and work up front, but as with most things in business, success begets even more success. And the early successes in efficiency and speed of provisioning will lead to more wins and business investment down the line. "With those early victories, you can then build even more sophisticated identity management that will, hopefully, further improve how the company operates and its security," says WellStar's Fisher. ■

New Brunswick conquers identity management with virtual directory

What started as a single provincial department's effort to roll out a virtual directory now helps government employees and citizens access about 150 applications. Find out how New Brunswick solved what could have otherwise been a big federated identity management problem.

BY JOHN MOORE

The Province of New Brunswick has made federated identity services a key component of its interagency identity management service, which provides the gateway to dozens of applications.

Service New Brunswick (SNB), a provincial-owned corporation, serves as the primary identity provider for government services in the province. SNB provides more than 200 services to the public on behalf of multiple government departments. The organization provides over-the-counter services at office locations, operates a call center and offers online services.

SNB uses Radiant Logic's RadiantOne, a federated identity technology, to pull together disparate directories into a single location for application authentication and authorization. Radiant Logic includes a meta, local and virtual directory within its federated identity offering. The company refers to the virtual directory component as VDS.

The federated identity service operates within a CA Technologies identity management environment, which includes SiteMinder, for single sign-on and identity access management, and CA Directory.

Today, VDS facilitates access to about 150 applications, including 25 to 30 major line-of-business applications and gBIZ, a framework that lets citizens conduct a range of government transactions online.

"It definitely became a much bigger piece of our identity management platform than we anticipated," says Nick Bishop, technical strategist with SNB.

Identity Management Effort Starts Small, Gains Steam

Initially, SNB deployed VDS to support the New Brunswick Department of Health. The department purchased an off-the-shelf application as the foundation for its Patient Access to Quality Care system. The system lets doctors and external service providers working with patients in rehabilitation centers view patient profiles and share case notes. Patients can access the system as well.

The application involved many different user communities and different directories, but it would only accept a single Lightweight Directory Access Protocol (LDAP) source and a single authorization group. The Department of Health came to SNB for advice – and that's when the agency began looking for a virtual directory.

Bishop said SNB evaluated four or five products and selected RadiantOne. The software stood out as a purpose-built federated identity service, which included a virtual directory, Bishop says. Other product offerings required configuring different options in order to serve as just a virtual directory; the virtual directory function "was a secondary use of the other products," he notes.

RadiantOne federated identity service integrated the identity information from the various directories, so the Patient Access to Quality Care application could leverage a single source of identity data. Other Department of Health applications have since signed on for use of RadiantOne.

From its foothold in the Department of Health, the federated identity service eventually took on an extended role within SNB and the province. While SNB was evaluating virtual directory technology, the province was in the midst of an identity management system overhaul. The new system brought with it a new way of authenticating apps.

However, Bishop says, the updated method introduced backward compatibility problems with many applications. So SNB asked Radiant Logic for assistance. The vendor came back with code, which Radiant Logic calls an interception script, to rectify the problem.

The interception script executes when VDS receives an identity data request from an application. The code makes sure the identity data is translated from the original format, schema and protocol into the specific format, schema and protocol the application can understand. This process allows normally incompatible identity sources and applications to communicate without the need to create, provision, maintain, and audit another identity store just for the application, according to Radiant Logic.

The fix helped SNB avoid hours of work modifying applications to deal with the new identity management system, Bishop says. "It saved us a lot of time and effort. We didn't have to go back and rework the applications."

Even if the changes turned out to be minimal, SNB would still have faced the task of changing and testing 150 applications to work with the new authentication model. Bishop says SNB didn't estimate the resulting cost avoidance but notes that the rework job would have taken four to six months at a labor rate of between $80 to $100 an hour (Canadian) and easily run between $54,000 and $100,000 to complete.

Federated Identity Management Grows With Infrastructure Layer

Dieter Schuller, vice president of sales and business development at Radiant Logic, says identity management systems that aren't able to present user information to the applications with the right schema, structure and protocols face a huge problem. In New Brunswick, Radiant Logic's technology provided an infrastructure layer that could connect SNB's various directories.

"They needed a layer that took what they had and made it usable by all the applications that needed to access user information," he says.

Schuller says SNB is fairly typical of the federated identity technology customers he sees in the market. "A lot of our government customers ... are experiencing the same set of issues," Schuller says, adding that commercial business face similar identity integration problems, too.

Against that backdrop, the federated identity service has evolved into an intermediary software layer in SNB's identity management system. When an app requests identity data, SiteMinder points to RadiantOne and the VDS pulls together all of the directory sources. Those include Microsoft's Activity Directory, CA Directory and a SQL Server database. SNB's Active Directory deployment, for internal users, consists of one forest and 10 domains. CA Directory is for external users, while the SQL Server database contains metadata regarding user roles.

Virtual directories, in general, aim to mask the complexities of identity management. Nick Nikols, a research director at Gartner, says identity data may be stored in a format that isn't particularly user friendly. A virtual directory, he says, "can abstract away from that and generate a view that makes it easier to consume."

The role of the virtual directory is to aggregate the data stored in different identity repositories, Nikols adds. That way, an application doesn't have to go to each source to obtain the information.

SNB's RadiantOne deployment focuses on the virtual directory, joins and interception scripts, but it may move into Web services as well. SNB has been using its own Web services to provide information to applications. Bishop says SNB conducted a side-by-side comparison of its Web services with Radiant Logic's Web services and found the out-of-the-box services handled about 95 percent of what its custom services could accomplish. ■

Identity as an attack surface

One of the core challenges for information security professionals is rooted in the fact that current security models are not designed to address identity as an attack surface. Instead of treating identity as a basic access provisioning function, it should be managed and monitored as a critical resource for the organization.

BY LESLIE K. LAMBERT

Thanks to mobile computing, cloud apps and tele-working, the de-perimeterization of IT security is a "fait accompli." This has created new challenges for CSOs and new opportunities for attackers. One of the leading threats emerging from the post-perimeter IT landscape involves using identity as an attack vector. Here's why.

Historically, information security professionals have focused on mitigating vulnerabilities across traditional attack vectors, namely networks, software or physical plants within their computing environments. Despite the large investments made in preventive and detective security technologies, protecting these traditional attack surfaces continues to be a challenge. As Ponemon states in their 2014 report on Mega Breaches, many companies have failed to prevent breaches with the technology they currently have, where 65% responded that attacks evaded existing preventive security controls.

What's changed? Instead of targeting hardened networks and application infrastructures, more and more bad actors, whether outsiders or insiders, are exploiting identities to gain "legitimate" access to sensitive systems and data. Protecting this new attack surface is hard, since identities must be trusted unless there's conclusive proof that they have been comprised.

2014 will be remembered as the year of the mega security breach, many of which have been found to be directly attributable to compromised identities.

For example, in the Anthem Blue Cross data breach where cyber attackers stole millions of health insurance records, hackers reportedly obtained the identity credentials of five different employees, possibly through phishing attacks, including computer administrators, which allowed them to access the company's internal network. Data stolen included names, social security numbers, and other personal information for up to 80 million Anthem customers.

Meanwhile, Premera Blue Cross is facing five class-action lawsuits and continuing questions since it disclosed a data breach. The lawsuits, filed in U.S. District Court in Seattle on behalf of Premera customers from Washington, Nevada and Massachusetts, claim that Premera was negligent, breached its contract with customers, violated the Washington Consumer Protection Act and failed to disclose the breach in a timely manner. As well, the lawsuits argue Premera violated the Health Insurance Portability and Accountability Act (HIPAA), as well as the insurer's own privacy policies, by allowing the data to be accessed.

These lawsuits, and pending penalties, are claiming negligence due to the poor management of identities and access credentials. Clearly, the bar has been raised on what constitutes appropriate due care of identity information by organizations.

One of the core challenges for information security professionals is rooted in the fact that current security models are not designed to address identity as an attack surface. Instead of treating identity as a basic access provisioning function, it should be managed and monitored as a critical resource for the organization.

To prevent identity from being exploited as an attack surface, information security professionals must return to something "old" and engage with something "new."

The "old" is verifying how effectively traditional identity and access management systems are being managed. Is basic, good quality hygiene being rigorously applied and exercised for these critical systems? For example, how often are users required to update their passwords? Is a reasonable amount of complexity required for those passwords? Also, is security awareness being promoted among users, including the importance of strong password choices, as well as the techniques used by attackers to steal passwords like phishing and social engineering?

The "new" involves monitoring who, how, where and what identities are being used for in the organization's computing environment, including the cloud. To keep watch over the typical "flock" of identities in an enterprise, new tools and automation are required. Gartner provides a good overview of these identity analytics technologies here. ■

Stop insider attacks with Privileged Identity Management

How 6 vendors are approaching this evolving area

BY JOHN BREEDEN II

Privileged Identity Management (PIM) is based on the idea that a common element of most advanced threats involves obtaining the credentials of an administrator, super-user or even a program with local admin rights. Armed with those credentials, the attacker can turn internal systems against themselves, rewrite security policies and remain undetected.

Privileged Identity Management tools lock down those special user credentials so that even successful breaches are only done against low-level endpoints that can't do much harm. Should attackers on a compromised system attempt to elevate those privileges, not only will they be quickly detected, but any process that attempts to run will be blocked.

For this review, we looked at BeyondTrust, Lieberman Software, NetIQ, CyberArk, Centrify and Viewfinity. This is still an evolving area, and companies are approaching it from different perspectives. For that reason, this is not a head-to-head comparison, but more of an analysis of how each vendor approaches PIM.

Each vendor seemed to shine in at least one area. The Viewfinity Privilege Management suite worked well in locking down the privileges of all users, and was the best at doing so with a very light touch that is completely invisible to most users.

The Centrify Server Suite and Privilege Service products eliminated the traditional need for a password vault, giving users access to network assets as needed using their normal logins, and removing multiple passwords from the equation altogether.

The CyberArk Privileged Account Security Solution is one of the most comprehensive systems that we tested because it's made up of five distinct elements for a completely rounded security picture.

The core of the Lieberman Software solution is its Enterprise Random Password Manager which can randomize thousands of passwords in just a few minutes to ensure that even in the event of a captured password, it won't be good for long.

NetIQ's Privileged Account Manager concentrated on the often-overlooked area of non-human accounts which might be held by certain programs or processes, as well as any user who has accidentally been given greater access than needed.

And the BeyondTrust PowerBroker UNIX & Linux product takes PIM out of the Windows environment and over to Linux and Unix systems, where it's sorely needed.

Here are the individual reviews:

BeyondTrust PowerBroker UNIX & Linux

The BeyondTrust PowerBroker UNIX & Linux product only works with those operating systems, though it can tie into a management console that is able to control all systems on a network, including those protected with the BeyondTrust PowerBroker for Windows product. For this review, we only looked at Linux systems. All BeyondTrust products are perpetual and server based. PowerBroker pricing starts at $199 and volume discounts apply.

When PowerBroker is initially installed on a network, a tiny bit of code is installed on every Linux machine to act as an agent that communicates back to the central security server. Thereafter, policies for each user and every possible command can be imported from other sources or created using the main interface. Although there is a very clean GUI, BeyondTrust officials say the vast majority of their Linux users prefer the command line interface. As such, much of our testing was done using the command line.

PowerBroker takes the concept of least privilege to the extreme. Once installed, all requests by users to run a process, either remotely or on a local machine, are sent out to the authorization server. There are a lot of rules that can be set based on things like the actual command that needs to be run, the user doing the requesting, their location and even time of day. The authorization server checks the policy file and then either OKs the user to run the command or rejects them. In either case, the request and the resolution are logged.

Should a request be approved, it does not necessarily mean that the process will run as the root user. Policies can be set so that commands are run from lower-privileged accounts as an extra layer of security. So a user may want root access to run a process, but instead have that process run as some type of admin or even a normal user should doing so be possible. PowerBroker can be configured to only give out the absolute minimum permission level needed for each process.

In our testing, any attempts to circumvent the authorization server failed. By default, if the authorization server can't be contacted, such as if a network cable is disconnected, all requests are denied. Attempts to gain root or administrator access to local machines without going through the authorization server are immediately shutdown. And all communication between the local machine and the authorization server are protected using AES encryption to prevent snooping or spoofing.

The log file of every user request is stored at a central server which is not accessible from any of the client machines on a network. So even insider threats won't be able to cover their tracks. Bringing up the PowerBroker console, it's easy to spot all failed requests in the daily log file, which are highlighted red in what is likely a sea of green approvals. That way even if a user is just testing the defenses of a system or database, those attempts will get logged. Reports can be examined at any time by policy server administrators, or set to be delivered in various forms like e-mail on a schedule.

As an option, sessions from users can be recorded and played back later. This can be set so that automatic recording happens based on certain events, such as higher level commands being issued or a user remotely controlling a machine other than the local one, or whatever an administrator feels is necessary to maintain security and compliance. Because most users are making use of the Linux command line interface, much of this recording is simply capturing text and keystrokes, which makes the files relatively small. Data limits can be set however if space becomes a problem, with the program only capturing, say, the first 500k of data, which is usually enough to get an idea what a user is up to.

When using the recording component, even erased keystrokes are captured. We tried to simulate a user thinking about entering a command, like one that would erase a file, and typing it before chickening out and changing their mind. Even so, as long as we actually typed the command, that process was recorded even if it was never sent.

Many Linux administrators are likely using SUDO to enforce least privilege policies. As a nod to that, BeyondTrust has a version of PowerBroker called the PBSUDO Policy Server that integrates most of the features of PowerBroker for SUDO users, with the most important addition being that it removes SUDO command authorization from the local machines, protecting them on a remote authorization server just like the main PowerBroker version of the product.

A final component to the PowerBroker suite is the BeyondInsight tool, which uses analytics to identify anomalous behaviors and first-time events. So if a user has always logged in locally but suddenly is working remotely, that might get flagged. Or if an administrator of one part of an organization suddenly begins poking around in areas that they are not responsible for, that would also likely raise a red flag. The one negative with this tool is that it takes a very long time to become useful, with a minimum baseline of three months. Thankfully, the user interface showing all the command lines that are approved and denied works pretty well in the meantime, especially if someone takes the time to become familiar with normal network operations.

Where BeyondInsight can really help is with very large organizations, or situations where misconfigured policies are allowing some users to do things that they should not be able to accomplish. It can catch rogue trusted insiders, but also incorrectly configured policies that might accidentally be allowing unwanted processes and commands to execute.

NetIQ Privileged Account Manager 3.0

Privileged Account Manager from NetIQ, which is now under the umbrella of Micro Focus, defines privileged accounts as those that are able to access files, run programs and add or change the rights of existing users. They also concentrate on non-human accounts, which might be held by certain programs or processes, as well as any user who has been given greater access than most users. That’s a pretty huge group of people for most organizations, but Privileged Account Manager is able to manage them using automation alongside the direct monitoring of user activities.

The heart of the NetIQ product is the Enterprise Credential Vault, which stores all passwords for assets in an encrypted data safe. Users don’t need to know the passwords for the systems or assets that they need to access. Instead, they apply for access and if approved, are given a temporary password that is only valid for a certain period of time before it expires and becomes useless. These passwords can be given out automatically based on policies or may need to be approved by a policy server administrator. Almost any rule can be configured based on users and the security surrounding the requested asset. Because of the automation aspect, programs like databases and cloud services can make use of the vault as well for valid automatic processes that they need to perform on a regular basis.

Setting up the various policies is an easy process using the graphical interface. There are various categories to choose from when selecting rule groups, like Windows access and Oracle database password checkout rules. You can import an entire set of rules from Active Directory, or any other database program in the event there is already some form of user or password-based security within the organization.

Administrators can also set up rules for what happens after a session is authorized, which can be very specific. For example, users can be restricted from entering the delete command for any file, or prevented from opening notepad to copy data down to the local machine. You can also specify certain capital offenses, such as trying to run the services command on a Windows server. Going beyond just blocking, performing one of those grave offenses can automatically disconnect the user, ending their session, revoking their rights to that system and their password, and notifying administrators as to what happened and why.

We tested this by trying some sneaky ways to get around capital offenses on a protected machine and every time we were met with a session disconnected screen and revoked credentials. On the admin panel side of Privileged Account Manager, those forced disconnects glowed bright red and our clear pattern of attempted abuse was obvious. We are fairly sure that had we attempted this on a real production network, someone would be coming to have a talk with us, or probably to escort us out of the building.

Policy administrators even have control over the password checkout requests themselves, assuming the system is configured to have a human in the loop. For example, if a user requests a high level of access to a certain server and the explanation given does not justify it, the administrator can instead authorize a temporary password, but assign that person lower-level access. An explanation of why the lower level access is being granted can be sent along with the authorization so the user knows the logic behind the ruling.

Full sessions can be recorded by Privileged Account Manager. There is an excellent review program that lists all of the commands that a user entered on the left side while a full view of the desktop plays like a movie on the right. You can select any part in the video by clicking on the left-side command window, so you can see exactly when and how the user tried to open services for example, or it can be controlled like a normal video with play and fast forward buttons, or by clicking on the movie's position bar at the bottom of the screen. This can be examined any time after a session has ended as part of a forensic investigation, or in real time as the session is going on in case there is an active investigation involving a specific user.

And lest the policy administrators start to abuse their power, all of their actions are also logged, so someone can be assigned to watch the watchers for even more robust security.

The automatic features that can be programmed into Privileged Account Manager 3.0 are impressive and can really help to stop both egregious offenses and also stupid user mistakes, both of which can be very costly to an organization. But Privileged Account Manager really works best when humans are also monitoring the sessions and actively responding to user requests for access to system resources. The interface is sleek enough that a single administrator can easily manage quite a few users, with requests perhaps having to wait a few minutes for approval at peak times.

Privileged Account Manager 3.0 starts at $787 for a per-instance license. For that price, it would be a great tool for a security operations center to have with dedicated personnel actually able to take an active role in defending their network in real time. That is a lot more efficient than having SOC teams respond to the endless alerts which happen at most organizations. With all privileged accounts locked down and actively monitored, those rampant SIM alerts are going to be a lot less important, and probably a lot less frequent as well.

Lieberman Software Enterprise Random Password Manager

The core of the Lieberman solution is its Enterprise Random Password Manager (ERPM). The ERPM is an extremely powerful tool which can randomize thousands of passwords in just a few minutes as a result of an alert or simply on a set schedule to ensure that even in the event of a captured password, it won't be valid for very long.

Setting up the ERPM on a network should be a fairly seamless process for most organizations. There are no agents installed on managed systems, which makes ERPM fairly unique. Instead, trusted user accounts on protected systems are leveraged on hosted networks to hand-off all future password management to the ERPM. If Active Directory files or network maps have been kept up, this is more or less automatic. However, individual systems and devices can be added manually if needed.

Once password control of systems is given to the ERPM, an administrator can set up rules to make sure that all generated passwords conform to the restrictions of each machine on a network. For example, admins can specify if new passwords need to comply with Windows 2003, 2008 or Vista rules for number of characters or whether a password can start with a symbol. Whether or not upper and lower case letters, numbers and symbols are allowed can also be specified. It can also be designated whether a unique password for each machine is generated or if groups of machines should share a password. Given that the ERPM is managing everything, it would be kind of counterproductive and outright dangerous not to have unique passwords generated for each machine, but the option is there.

Users apply for passwords to gain access to systems managed by the ERPM. These can be granted automatically based on policy. We set up a rule where someone who was authorized to work with a certain program on a certain system during working hours would be automatically approved if they logged in during those hours within those parameters. Or everyone can be subject to manual approval, though this might require either a dedicated staff or a slight slowdown in normal daily production while people wait for authorization to use resources.

In either case, password checkouts are set to expire after a certain number of hours, whereupon the ERPM will generate a completely new password for that system. From a user perspective, approved password checkouts can come with a link for automatic logging in using the new credentials, or they can cut and paste them into the login field of the approved machine.

From the ERPM console, administrators can see all of the active threats of assigned passwords that are currently being used as well as a log of all the previous uses. Those awaiting approval are also highlighted so that they can be quickly examined and approved or denied. All sessions can be recorded and data from that can then be examined by ERPM administrators or fed into a corporate SIM system.

Should something suspicious pop up, such as an ongoing session that was somehow not approved, or even a warning from an organization's SOC that something is amiss, ERPM administrators have the option to signal for an emergency change of every password in the entire network and an expiration of every active thread, a sort of virtual panic button that can halt all previously approved network activity.

Our test environment had a few dozen systems, so this process was completed quickly, however, ERPM has a unique architecture that allows it to be deployed on networks with thousands and thousands of clients and still complete a full password refresh in a matter of minutes. That is because the central ERPM server in a large deployment is connected to several Zone Processors which each manage groups of users, mirroring the commands sent from the main host.

Resetting passwords for Windows devices can be tricky as there are loopholes that would allow existing connections to remain intact. This is the basis of the so called golden ticket type attacks where hijacked sessions remain active and renew the credentials of other users in the event of a password reset. ERPM defeats this by automatically changing all Windows passwords twice in rapid session, which is set by a single check box in the administration panel. Changing the password twice forces an urgent replication throughout the entire organization. This would expire the golden ticket's credentials since it would be two iterations behind. As a precaution, ERPM can be set to always do double password changes like that even for routine rotations on a set schedule.

Another interesting aspect of ERPM is a feature known as account pooling, which can be used to ensure that offline systems are given proper password resets. Also, it can allow administrators to detect devices that are not authorized to be on the network, but which only connect intermittently. How pooling works is that three accounts are set up in the resource pool, or more if the passwords change globally quite a lot. When initiating a change, ERPM also rotates the pool that the accounts use to authenticate. Since all accounts are monitored, when administrators see a device trying to authenticate to pool number two when the ERPM has rolled everything else over to pool number three, it means that the system in question was either offline at the time of the rollover or was recently added and is unknown to the system, or possibly not authorized to be there. Setting up account pooling is, like everything else with ERPM, extremely easy and comes down to not much more than checking a few boxes to add yet another layer of security to an already impressive system.

Lieberman Software's Enterprise Random Password Manager proves that there is more than one way to achieve good Privileged Identity Management. With prices starting at $25,000 and licensing thereafter by node, it's comparable with other Privileged Identity Management solutions, yet it offers complete support for all passwords within a network, not just the ones belonging to privileged users. It can lock down everything, and even has an emergency button to switch out every password in the event of a suspected threat.

CyberArk Privileged Account Security Solution

The CyberArk Privileged Account Security Solution is one of the most comprehensive systems that we tested for this review. It's made up of five individual elements which run under the same user interface, and which can be purchased and installed separately as needed. The five elements are the Enterprise Password Vault, SSH Key Manager, Privileged Session Manager, Application Identity Manager and the On-Demand Privileges Manager.

The heart of the system is the Enterprise Password Vault, and probably the component that everyone who uses the system is going to put in place first. The vault is a repository for storing and monitoring passwords that users need to access in order to gain permission to use system resources.

However, the CyberArk password vault is more secure than other solutions that keep every password within a single, encrypted database. Instead, each password inside the vault is stored and encrypted separately, so it's more of a series of safety deposit boxes than a single vault. This way, even if someone should somehow break down the AES encryption, as unlikely as that is, they would only gain access to a single password. Also, in our testing, securing individual passwords had no negative effects on the speed of retrieval for authorized users.

Users who need to log into an asset protected by the Privileged Account Security System are presented with an information panel that groups various servers and systems by the account types used on them. Users can see, for example, systems that they always work on under their Favorites tab, or systems that they used previously under the Recently tab. Assuming users don't currently have access to a system, they will need to select the Show Password command button. That will prompt them to fill out a small form detailing the timeframe that the password will be needed and the reason for access. They can also specify if they will only need to use the password one time during that period, or might require logging-on multiple times during the specified timeframe. The user is told what the policy is and how many people would need to approve their request before submitting it.

Back on the administrator side, we received a password access request through our Outlook e-mail. Opening up the mail gave us a link back to the administration console, which also showed all pending requests where users were waiting. If an administrator is working and has their console open they would likely see all the requests coming in that way, but the e-mail alert is a nice secondary method, especially in the event of a critical request. Looking at the request gives admins all the relevant details as to who is making the request, the exact resources needed and the time frame that the user would like the password to function. There is also a brief description provided by the user as to what they need to accomplish.

Requests can be confirmed or denied, and the administrator has the ability to send a message back to the user with their decision. Assuming authorization is given, the user can then make use of that password for the time specified. After that, the password is re-issued and the current one becomes worthless.

Not all passwords require that level of approval. Known users who need routine access to a system for a non-administrator type task, for example, can be set to be able to see a password as soon as they click on the Show Password icon. The system could still be set to record actions taken by someone who is automatically given access and the password could still expire and change each time the user is finished their work, but it would prevent any lines from forming in the approval process with users just trying to accomplish routine tasks.

In fact, the different levels of access and permissions that can be set up using the CyberArk Privileged Account Security Solution is impressive. We were even able to manage the default accounts that come with some software packages through the Application Identity Manager component. And this worked even if those default accounts didn't ever touch Active Directory and thus could otherwise become invisible loopholes within the network permissions structure.

A component called CyberArk DNA can be used to identify those hidden accounts so that they can be included in security policy. The ease of use when setting up policies is due to the fact that not only is there a very detailed master policy that can be defined, but it's also very easy to add exceptions for users, applications and specific assets using almost any criteria needed. And the nice thing is that even in the example of an exception, it does not mean that security is compromised, as monitoring and recording of that asset's use or user is still available. Any anomalous events can also be sent directly to a corporate SIM.

The recording of user sessions is very precise. The system records keystrokes and video-like screen captures of everything that is going on, but it also makes the entire pile of collected data completely searchable. We searched for any time within the archives when someone typed a specific command, and several videos recorded from within our test system quickly popped up. Not only did the videos show who typed the command we searched for, but they were also keyed up to the exact second when the user entered that command. This would be an invaluable tool for any cybersecurity officer, auditor or forensic investigator. Without such a detailed search tool, the sheer volume of data collected might make it impossible to find what is needed. But this way, searches can be increasingly narrowed until the exact users and commands, and even the exact time frames, needed for an investigation are located.

The final component to the CyberArk solution we looked at was the On-Demand Privileges Manager, which is the newest part of the suite. It is used to provide local access to certain systems such as Linux boxes where the admins are used to working with SUDU and keeping policy decisions stored locally. The On-Demand Privileges Manager allows this to still happen. In fact, we were able to run local admin commands on a test machine even when disconnected from the main privilege management server. However, sessions are still recorded for auditing purposes, encrypted and can be automatically sent back to the vault for safekeeping.

Deploying the CyberArk Privileged Account Security Solution in a series of components not only keeps the solution lightweight but allows companies to build up their Privileged Identity Management solution as needed while keeping the same basic interface. CyberArk deployments start at $35,000. Installed in components or out of the box as a whole package, CyberArk offers well-defended and defined protection for privileged identities from almost any path that a threat actor could take to compromise network security.

Centrify Server Suite and Privilege Service

While it's clear that traditional perimeter defenses fail against most modern threats, the philosophy behind the Centrify product is that a new perimeter needs to be formed around identity management. Its Server Suite and Privilege Service products first consolidate identities into one manageable area, vastly shrink the possible attack surface, then eliminate problem accounts such as network administrators and roots from having to be used except in emergencies. Instead, users are able to log in as themselves and have their privileges elevated as needed on authorized systems without having to check out a password from a vault, and without even knowing the root or administrator passwords.

Server Suite and Privilege Service can then make networks even more secure by turning mobile devices into a second authentication factor that no remote attackers would be able to access. Mobile clients do need to download an app to take advantage of this system, but on the actual network, no agents are installed on any clients, just the hosting servers.

Server Suite and Privilege Service work with Windows, Mac and mixed environments and make up one of the most economical products in this review. The standard edition of Server Suite costs $385 per server, plus a yearly maintenance fee, regardless of how many users or clients need to be managed. The Privilege Service adds remote management features to Server Suite and can be purchased for $50 per month, per each IT person who needs to access it. The Server Suite product, which was mostly the focus of this review, is delivered as installable local software as agents running on servers, while all features of the Privilege Service product are delivered as a cloud based service.

Interestingly enough, while most products in this space center around the use of some form of a data vault in order to store passwords for checking out by users, with Server Suite it's more of a secondary component. Root and administrator passwords are stored and managed within a vault and can be changed over time, however, users don't generally go to the vault unless there is some type of emergency situation, whereas it works pretty much like any other vault type of system. If needed, a user requests a root password which, if approved, is then issued for a brief period of time and then regenerated. There is also no need for an SSH key vault with Server Suite because clients and servers on the network use Kerberos to authenticate to one another with an authorization server handling the one-time key exchanges for encryption.

Instead of a vault, Server Suite administrators can set up various permissions that can be given to users on systems that they are authorized to use. Users simply log in as they normally would and work the way they always have. If something they do requires administrator or even root access, Server Suite will allow that process to run if the user is authorized to do it. Unless a typical end user tries to do something that isn't authorized, they probably won't have very much contact with Centrify Server Suite at all, though they can be given access to a user-version of the administration panel which shows them their various permissions and what assets they can access.

On the administration side, users are grouped into areas called zones. Initially much of the zone properties can be created using active directory policies. However, adding new users is a simple process once Server Suite is set up and running, as is setting up the zones themselves.

A zone is basically a type of user who shares access characteristics with others. For example, you might set up a finance group of people who are able to access computers connected with that job and run processes related to that group. Or you might set up a zone that is comprised of outside contractors who are given very limited access and only to the systems that they need in order to do their jobs. If a new finance person comes on board, they can simply be added to the finance group and the whole process takes a few seconds. Likewise if someone leaves an organization, removing them from the zone is quick and easy, and strips all credentials and permissions from them from that point forward. And there are many good options for setting up zones which can be incredibly detailed. For example, we set up a zone for helpdesk users that allowed them read-only access to log files, so they could find problems and help users, but not cause any new problems themselves.

The zone defense makes it much easier to manage large groups of users, as different administrators can divide up each zone, but it also prevents lateral movement within a network even if a user's identity is compromised. For example, when we compromised the identity of a user within our outside contractor group, that user was only able to access the very specific system allowed within the zone where they were assigned to work. Any attempt to gain access to any system or resource that was outside of that zone not only ended in failure, but with the flagging of that account as suspect and the possible revoking of all privileges depending on how the policy was configured.

New users can be given permission to access various system resources from scratch, which works if the new person is unique in some way in what they need to accomplish. However, once established, most new users will likely simply be added to existing zones to pick up those properties. Also, it's very easy to add exceptions to the zone rules when creating a new user. We created many new users for this test. For the most part, all a Server Suite admin needs to do is use a series of check boxes to define the access properties for a user, and not even that if they fit perfectly into an established zone. Possible choices include forcing a user to make use of two-factor authentication on login, the ability to access various assets in the network and even the ability to run specific commands. Users can also be given access to a user version of the Server Suite console so that they can see what is allowed and what is restricted to them, something you might want to give to internal employees so that they can avoid trying to do something outside of their purview. It's probably not something you want to share with external contractors.

On the audit side, the main tracking panel clearly shows the user and the commands they used for each session, since the two are directly tied together in the system. It's nice compared to other privileged identity management programs because you don't simply see that the root account was checked out and then have to investigate to see how it was used or by whom. Instead you see what each user specifically did, and is currently doing, right from the top level administration menu, sorted by user.

Administrators can call up recorded sessions by users which includes a real-time recording of the screen as well as a keystroke log which is completely searchable. And because nobody is normally checking out a root password or even entering it directly, there are no backdoors or holes that can be exploited to get around the monitoring process. Centrify can set up a series of Collector devices for large networks to handle the load that massive amounts of audits might generate, though our testbed didn't get anywhere close to needing even one of them.

A separate but integrated product from Centrify is their Identity Service offering, which adds an identity-focused Enterprise Mobility Management platform. Fully integrated with Server Suite, it can add two-factor authentication to any protected network using the devices that employees are likely already carrying around. Users simply download the app for their device and tie it in with their identity. Devices can be forced to conform to certain rules before making the connection too, ensuring for example that they are not already compromised or jail-broken.

Thereafter, users can be required to use those devices as a second form of authentication when accessing network services protected by Server Suite. We were even able to use a low-end device, an aging iPod Touch, as a secondary token. Once we forced a user to make use of that token, each time they logged in they were prompted to enter a four digit code on the iPod's screen. The fact that the device was being held by an actual user confirmed that they were in fact a human and not a bot, while entering the correct code proved that they were probably the authorized person. For even more security, users with devices that have fingerprint scanners can instead be prompted to use that as part of their login. Companies could then issue devices with fingerprint scanners for their employees to work with and add biometrics as yet another level of network security already built-in and managed by Centrify.

Centrify Server Suite is one of the easiest products to use in this review, and also one of the most economical with the least complicated licensing scheme. Beyond that, when coupled with Privilege Service and Identity Service, it completely removes security from the now-ineffective method of network perimeter defense, and shifts efforts to protecting identities. This allows network policies to be enforced regardless of who the users are, what devices they use or whatever network resources are ultimately being protected.

Viewfinity Privilege Management

In our testing, the Viewfinity Privilege Management suite worked well in locking down the privileges of all users and increasing overall network security. Where it really shined however was in its ability to do this with a very light touch that will probably remain invisible to most users going about their normal routines.

The first step in getting Viewfinity Privilege Management working is a silent discovery phase that takes place over several weeks on a target network. As part of this process, agents are installed on all Windows clients to help Viewfinity record that client's interactions, and eventually to enforce access policies. While many of the current access rights can be gained from importing them over from Active Directory, there are many applications, scripts, processes or even users who might connect infrequently that might get missed just by doing that. So Viewfinity watches over a network for several weeks and records who and what accesses it and what they do. All of that is then placed into a policy creation engine that gives administrators total control over how everything is allowed to access the network once the discovery phase is complete.

Viewfinity offers a free tool that puts networks through most of this discovery process to help identify who and what has administrator rights. This is likely going to be an eye-opening process for most organizations with everything from devices to scripts likely having some type of privileged access that is also likely unmanaged.

A second component to Viewfinity Privilege Management is the Application Control software, which was tested as part of the package. Though they can be purchased separately, they are so very closely related, and share the exact same user interface and management console, that it was hard to imagine a situation where an organization would want one without the other.

One of the most interesting things about Viewfinity in terms of ease of use is how trusted sources can be identified and how handling them is defined by policy. For example, we set up our Viewfinity testbed to block any previously unknown programs from accessing the network. When we downloaded a program from the outside and tried to run it, we were given the "This action is not covered by policy" warning that we had set up. However, we were also able to tell Viewfinity that anything coming from the network shared drive is part of a trusted group of programs, even if it is previously unknown to the system. Then when we downloaded the same program from the protected network share, a different policy was used to manage it instead. In that case the program was allowed to run, however, administrators were notified about what was happening.

The trusted source policy is very robust and even makes allowances for digital signatures. If your organization uses Epson printers or Cisco communications equipment for example, you can allow those devices to access the network and install updates so long as they are digitally signed. That should take a lot of the burden of false positive alerts off of administrators using over-worked corporate SIMs and still allow authorized equipment to maintain the proper drivers on the network. However, if even that level of automation is too much of a risk, it's completely optional.

Setting up policies is incredibly easy using the Viewfinity interface. There are three large buttons for policy types that administrators can fit everything into, as well as a policy to use in case something is previously unknown. At the lowest level is the Monitor tab. This is best employed with trusted applications and actions by known system administrators. Monitoring can take on many different levels all the way up to fully recording every keystroke and videoing an entire session to simply notifying someone that an action is being taken.

The Restrict Access tab is the next level up in the security hierarchy. Programs and users that fall into this category can have a variety of restrictions imposed on them. Applications for example might be allowed to run, but are blocked from accessing the Internet, or from triggering a new download of any files themselves. Monitoring and notification can also, and probably should, be used to keep an eye on things that fall into this suspect category.

At the high end is the Deny tab. Anything placed here is likely going to be known malware or at least something like a game that is unwanted on the network. It might also be a user who was previously fired or who has left an organization. Blocked programs or users can be restricted from performing any functions on the network and can even be locked down and prevented from running anything locally.

Messages to a user who runs into either a restricted access or block policy can be completely customized. Being friendly or foreboding is totally up to the network administrator. Company logos or official symbols can become part of the message too if desired. There is also a process in place, again it's completely customizable if you want this or not, for a user to explain why they want a specific program to be able to run on a network or why they need elevated access outside of the normal policy. Administrators can consider the request and have the power to keep things restricted, change the access level of the program, declare it to be trusted, or even to authorize a one-time run of the software or process in question.

Another nod to the flexibility of Viewfinity, there are already routines in place to allow unusual exceptions to every rule. For example, a network database might be locked down against remote access, but a traveling employee might need access from their hotel room. In that case, administrators can issue a one-time remote access code for a specific user to get access to a specific resource, all of which can be done over the phone.

Pricing for Viewfinity Privilege Management and Application Control is based on the number of desktops, laptops and servers being managed and is determined depending on the products and deployment licenses being purchased. Base configurations can start at around $35,000.

The two main strengths of Viewfinity Privilege Management, besides its base ability to protect networks from malicious or compromised privileged users, is its ability to remain mostly out of the way from average or even administrator-level users, and the dazzling array of easily customizable access options. We were able to create rules to handle every bizarre privilege management situation we could think up. Given that most networks probably have at least a few situations like that, it makes Viewfinity Privilege Management a great choice for unusual situations as well as day to day privileged identity protection.

This story, "Stop insider attacks with these 6 powerful tools" *was originally published by Network World.* ■

What users love (and hate) about 4 leading identity management tools

What do enterprise users really think about the identity management tools they use? There's a lot to like, but also plenty of room for improvement.

BY CSO STAFF

Four of the top identity management products on the market are Oracle Identity Manager, CA Identity Manager, IBM Tivoli Identity Manager, and SailPoint IdentityIQ, according to online reviews by enterprise users in the IT Central Station community.

But what do enterprise users really think about these tools? Here, users give a shout out for some of their favorite features, but also give the vendors a little tough love.

Oracle Identity Manager

Valuable Features:

"The most valuable features are the attestation of identities and the robust set of identity analytics."
– Mike R., Lead Solutions Architect at a media company with 1000+ employees

"I feel the Provisioning and Reconciliation Engine as well as the Adapter Factory are the most valuable, apart from the standard features which most identity management solutions provide."
– Gaurav D., Senior Infrastructure Engineer at a tech services company with 1000+ employees

"Automated User Creation and provisioning of connected resources in the case of Identity Manager, Access control to protected web resources with regards to Oracle Access Manager."
– Mwaba C., Identity and Access Management at a manufacturing company with 1000+ employees

Room for Improvement:

"With Oracle, it's always about the learning curve and the nature of how the product is integrated. It takes tons of training and getting the right experienced people involved in order to launch the initial framework. Some of the adapters also do not work very well or have limited functionality."
– Mike R.

"Connectors that are available for integrating with different products. General stability of the product needs to be improved."
– Usman J., Solution Architect at a tech services company with 1-100 employees

"The management of workflows could use some improvement as well as the overall performance of the product. Because this is such a

complex product, we find that it runs a bit slower than its competitors."
– Mwaba C.

Read more Oracle Identity Manager reviews on IT Central Station

CA Identity Manager

Valuable Features:

"I would say the most valuable feature is provisioning where we are able to provide user access to all the resources they need in a uniform way that we can audit. We don't need to spend a month going to every individual server, every individual database granting user access. We can do it from one central place."
– Boyan V., Senior IT Manager at a hospitality company with 1000+ employees

"The user interface. The synchronization with our HR system"
– Idita S., Information Security Manager at a aerospace/defense firm with 1000+ employees

"Policy Xpress makes modifications to how our user data is handled so easy."
– AppAnalyst250, Applications Analyst at a software R&D company with 1000+ employees

Room for Improvement:

"Something to help us migrate our code between environments from QA to UA to production in an easier way. That would probably be the big one."
– Boyan V.

"The GUI in CA is more complicated where a user might have to drill down more into the menu to find the real form. Also, during configuration for a new person it's a tough deal to drill into the menus to find the place to actually setup."
– Gaurav D., Senior Infrastructure Engineer at a tech services company with 1000+ employees

"An out of the box way to control when a policy executes."
– AppAnalyst250

Read more CA Identity Manager reviews on IT Central Station.

IBM Tivoli Identity Manager

Valuable Features:

"I think, the most important feature of Tivoli is "Custom Adapter Development" which allows to create agents for almost every application, so that Tivoli can communicate with those applications."
– Abhinav S., Senior Software Engineer at a tech vendor with 1000+ employees

"Flexibility, interoperability and the number of adapters/connectors that come with the product are key differentiating strengths in my opinion.

The product allows for extensive customization, particularly for things like workflow and policy configurations, which can get complex in a large IAM environment. Configuration is UI-driven, but the same can be accomplished in a more powerful and direct manner by writing scripts, which are based on JavaScript syntax. This is in contrast to products like Sun IDM, which rely on a proprietary language for product configuration."
– Sergei V., Founder & President at a consultancy with 1-100 employees

"The ability to suspend/restore user accounts across multiple products over which Tivoli controls security."
– TechCommsDir318, Director of Technical Communication at a media company with 1-100 employees

Room for Improvement:

"ITIM/ISIM pre-installation may take some time. Users need to create ITIM instances manually. IBM can bundle all the pre-installation components and make a single installation package."

– Kamala K., Security Developer at a tech services company with 1-100 employees

"1. Enable the business users to manage their permissions by themselves without the technical guys

2. Make the process of creating rules easier

3. Improve the admin GUI

4. Allow functionality to work with the cloud base services"

– Oren H., IT Management Information Security at a financial services firm with 1000+ employees

"As far as I have understood the product:

1. IBM can work on providing better options for creating custom reports, although various supporting IBM products are available. However, if the functionality is provided in the Tivoli product, then the options should be there for creating Expected Report formats.

2. It's highly dependent on the database connection, if there would be even a slight network glitch in the connection between Tivoli and, mostly DB2, databases and the system was not able to recover and re-establish the connection, it would require a complete environment restart."

– Abhinav S.

Read more IBM Tivoli Identity Manager reviews on IT Central Station.

SailPoint IdentityIQ

Valuable Features:

"User Access Review, User Access Request and SOD Policy detection. Another important feature is IdentityIQ's provisioning broker which allows us to either use its built-in provisioning engine or easily integrate with third-party provisioning and help desk/ticketing systems (such as IBM TIM/SIM, Oracle IdM, BMC IDM, BMC Service Desk, Novell IdM, Microsoft Forefront IdM, ServiceNow etc.) The back-end provisioning of IdentityIQ is lightweight and fast to implement."

– Matt C., Principal Technologist at a tech vendor

"Certification of user's access, enabling the organization to have a strict governance of what its employees are for entitled to currently."

– SecConsultant790, Security Consultant at a tech services company with 1-100 employees

"1. Very user friendly unified UI (for users and administrators)

2. An excellent out-of-the-box features (hierarchical RBAC, flexible provisioning policies, role-mining, certifications, life-cycle events, etc)

3. Modest hardware requirements

4. A large list of out-of-the-box connectors (with no additional charge)

5. Using only standard java technologies (java, beanshell, HTML, jsp, JavaScript, XML, some Apache projects)

6. Possibility to deploy the solution on different DBMS and application servers of your choice

7. Very fast implementation of the solution with custom modifications"

– Andrey S., IdM Consultant at a tech services company with 100-1000 employees

Room for Improvement:

"We would like to have a bit more flexibility in how the screens are laid out and the content. Some of our clients prefer feature-rich UI/screens whilst others would like to have simpler interaction and presentation.

Report writing is much better in the latest

versions, but it is still not comparable to what one can get out of dedicated reporting tools."
– **Matt C.**

"Some of the features like multi-aggregation and self healing feature in case of corrupted certificates would be pretty useful which would enable easy debugging in case of issues."
– **SecConsultant790**

"1. The price is very high
2. The partnership program is very inflexible
3. Provisioning. This functionality sometimes require too much coding to implement some customers' requirements
4. "Ease of use." IdentityIQ has a function that can be described as duplication (this can depend on the point of view) for example, groups, population, and work-groups
5. Implement the support of organizational structure"
– **Andrey S.**

Read more SailPoint IdentityIQ reviews on IT Central Station

Note: These reviews of select identity management products come from the IT Central Station community. They are the opinions of the users and are based on their own experiences.