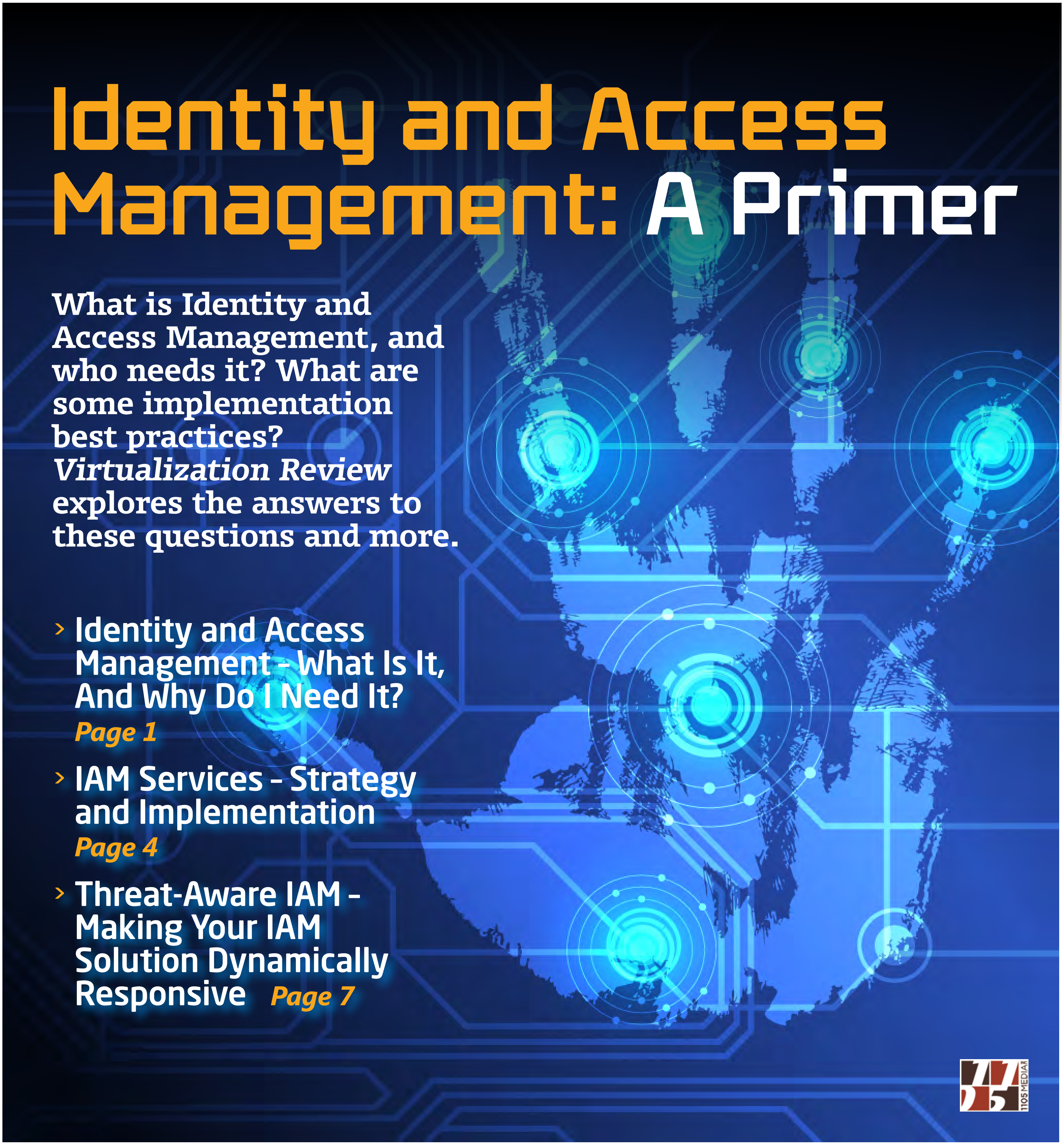
CONTENT PROVIDED BY

POWERING THE NEW IT GENERATION
VIRTUALIZATION REVIEW

CONTENT SPONSORED BY

Centrify®



Identity and Access Management: A Primer

What is Identity and Access Management, and who needs it? What are some implementation best practices? *Virtualization Review* explores the answers to these questions and more.

Identity and Access Management – What Is It, And Why Do I Need It?

By Greg Crowe

Since many IT challenges come from outside the network, it is easy to overlook problems that may arise from within. Whether through negligence or collusion, the simple truth is an organization's data is most vulnerable from contact with the people that use it every day. An Identity and Access Management (IAM) solution can help mitigate information loss by controlling who gets access to what when, and for what reasons.

While they usually go hand in hand, IAM is actually composed of two parts, Identity Management and Access Management. Before one can really grasp an IAM strategy, an understanding of these two components interrelate is essential.

Identity management comprises the methods by which digital identities are managed and controlled.

Identity management comprises the methods by which digital identities are managed and controlled. A "digital identity" can be pertinent information about a person, a department, a service, or even a computer. In the case of a person it would include things such as passwords, location, and other credentials. The two main areas of identity management are maintaining the user directories and keeping track which roles are assigned to which users.

Access management essentially works the problem from the other end. It is the process by which access to information is regulated. This is usually done through a system of policies that keep track of the various roles' permissions and restrictions. This is further broken down into authentication and authorization (which keeps track of which roles have access to what data).

Essentially, the goal of IAM is to create and manage user identities and their related access permissions to information and other organizational resources. This is extremely important, because the greatest threats to a piece of information's security are from its authorized users.

Most commonly, a specific user will be able to delete or export a document because they have more privileges to it than they need or should have. This is due to permissions policies that either errs on the side of giving more open permissions or that tries to apply "cookie-cutter" permissions to users that need more detailed tweaking.

Another popular cause of improper information handling is through third parties that may have needed limited access at one point, but those permissions were not properly expired and the right time. Essentially, it is necessary to decide when these doors need to be closed at the point that one of them gets opened.

There are external threats that an IAM solution needs to address, but these involve culprits gaining access by means of duping unwary users. By using lies and deception, a criminal can gain things such as login information from employees and thereby get access to an organization's information. Education is important in preventing this type of breech, but but a good IAM solution should be able to mitigate damage by controlling location- and time-based logins.

By using lies and deception, a criminal can gain things such as login information from employees and thereby get access to an organization's information.

A sound IAM strategy is vital for increased cost savings and IT productivity. Without it, an organization faces regulatory compliance issues and puts data at risk because the network may not be secure.

With an increase in cyber attacks every year, keeping your information secure is at the same time a difficult challenge and one that must be met without exception. A sound IAM strategy that is adhered to by every member of your organization is an essential tool that will help you achieve this. VR

Greg Crowe has been writing about computer technology and its applications in the business and government workspaces for about ten years. Originally working as a network administrator, he has also design and maintained many websites over the years. He likes to think that if can teach one person something new on the topic at hand, then his work here is done.

IAM Services – Strategy and Implementation

By Greg Crowe

In today's climate of high-tech cyber-threats, having a system in place to maintain and monitor digital identities and their access to sensitive information is essential. But once you've decided that an identity and access management (IAM) solution is necessary for your organization, where do you go from there? While every network will have its unique requirements, there are some general steps that need to be taken in order to get an IAM solution ready to meet your needs.

The first step to the implementation of any technology is the planning stage. At this point you need to examine what your users need to access to do their jobs, as well as the temporary needs of any contractors you might have. You also need to examine your network's information and categorize it by how sensitive it is, as well as which types of users may need to access it. This is probably the biggest and most time-intensive step in the entire process, but skimping here can cost a lot of time and money down the line.

You need to examine your network's information and categorize it by how sensitive it is, as well as which types of users may need to access it.

As with most network and technology adaptations, designing a framework is a vital first step. This framework needs to define a set of policies and standards for the identity and access management needs of your network. They may include defining minimum authentication levels and methods, such as using two-factor authentication as a minimum requirement to perform administrative tasks. This may also involve identifying acceptable levels of encryption, as well as directory and meta-directory structure standards. Data exchange formats and methods (such as XML and DSML) should also be considered at this time.

Once these needs are outlined, then it's time to move on to defining the IAM architecture. First and foremost, this needs to be in line with the existing security architecture in an effort to bolster it instead of competing with it. There are several key components that every IAM service will have. The most critical is Directory Services, which acts as a repository for the users' ID profile information, and it plays a key role in user authentication and enabling on-demand service delivery. Then comes User Provisioning, which helps oversee end-to-end user life cycle management. Authentication Services helps identify the user through various authentication methods, including digital certificates. The Access management infrastructure is based on a defined policy, and authorizes access to information systems and applications.

Lastly there are the Portal Services, which provide a single interface to all web-enabled systems and applications.

Once the architecture is defined, the next step is coming up with the specifications for the services you have defined that you need. This will entail identifying components you may already have in place that might be altered to fit the new architecture. In many cases, you may be faced with the decision on whether to try to integrate an existing piece, or scrap it to make room for something that is designed to work with the other new components. This is always a tough decision, and the answer will vary depending on innumerable factors including budget and manpower.

The most high-tech solution is not worth much if the users themselves are not trained and encouraged to comply with the policies you set forth.

Fortunately there are many vendors out there offering both cloud-based and server-based IAM solutions, so the likelihood of finding one that coincides well with your planned architecture is pretty good. But don't make the mistake of designing your needs around the product as many organizations do. If you take the time to go through these steps, and then find a product that matches (or can be altered to match) your architecture, you will save time and money in the long run.

The last step may seem like the most innocuous, but it is every bit as vital as each of the others – devising compliance and auditing strategies. The most high-tech solution is not worth much if the users themselves are not trained and encouraged to comply with the policies you set forth. This often can be the most challenging and ongoing factor in any IAM system, and of course there is no roadmap for this step as every organization will need to handle its users differently.

Like any enterprise solution, if the time and effort is taken in each of the stages of planning, then you will end up with the solution that works best for your organization. **VR** *—GC*

Threat-Aware IAM – Making Your IAM Solution Dynamically Responsive

By Greg Crowe

One thing is certain in the information security field: the threats will not stand still for you to defend against them. Following this philosophy, antivirus technology has gone from checking against periodically updated static lists to sophisticated pattern recognition that tries to predict threats. It has become clear that identity and access management (IAM) needs to evolve in a similar way.

IAM services have been using procedures and architectures where identities are handed out from a central location, and those identities are given access to certain areas of information for a specific lifespan. This works perfectly well in a system where all of the logins are made either on premises or through virtual private network gateways. However, with the advent of the cloud and the proliferation of mobile devices, it is harder to control how a user logs in, yet you still need to make sure that everyone has access to what they are supposed to — and nothing more.

Threat-aware, or dynamically responsive IAM is essentially a new way to approach the way you utilize your IAM service. When done properly, it improves the way IAM works in two ways. First, it helps you think like an attacker and prevent threats before they occur. Secondly, it opens identity provisioning to accommodate mobile users while still allowing traditional users to connect the same way they are used to without adding any additional burdens.

Threat-aware, or dynamically responsive IAM is essentially a new way to approach the way you utilize your IAM service.

There are several areas that you need to concentrate on in order to get your IAM services up to snuff with these new techniques designed to combat advanced threats. The first area concerns safeguarding mobile, cloud and social access. In order to accomplish this, you need to find ways to validate "who is who" when users connect from outside the enterprise. Also, the enforcement of policies on the cloud, social and mobile fronts needs to be rigidly proactive.

Preventing advanced insider threats is definitely an important goal in this new approach that can't be overlooked. This involves a more hands-on management and monitoring of privileged access within the network than that of a traditional IAM setup. You also need to work it from the other end and take more focused steps to defend the data from unauthorized access. Establishing an audit trail is a must. Every time a trusted insider accesses anything, a record needs to be created. And someone needs to pay attention to that too, ensuring that nobody is working outside of their authorized area.

While some aspects of security are being looked at in more detail, other areas are being simplified for reasons of efficiency, specifically the identity silos. Federated access can better enable online collaborations, and unifying identities can make for more efficient directory management in the long run. While many tasks, like the aforementioned need to examine audit trails to check for insider threats, many other areas can be automated. After all, a computer is tireless when looking at patterns and access log information, and can alert administrators when any threshold is met that might constitute a danger.

Threat-Aware IAM is an idea whose time has come.

The last area revolves around reporting, and the system's ability to deliver actionable security intelligence. Generally the system administrators need accurate and pertinent information in order to be more proactive in their duties. This can lead to more streamlined identity management across all domains, and also more targeted monitoring of entitlements and activities.

Threat-Aware IAM is a relatively new concept, so you will find much fewer companies offering products or training in this area than with IAM in general. However, this is an idea whose time has come, so we can expect this to be more and more plentiful, especially as advanced persistent threats and those who deploy them continually rack up successful breaches in what is becoming a full blown crisis of cyber security. While a scary concept, all of the advanced persistent threats, and the growing awareness about them, should also make finding what you need to improve your IAM architecture a bit easier as companies rally and build threat-aware intelligence to help defend against these new forms of attack. VR

—GC