The Low Hanging Fruit of IAM

Three fundamental things you should be doing

Written by Joe Campbell, principal solutions architect, One Identity

Introduction

As a Security Principal for the One Identity family of identity and access management solutions, I get the unique opportunity to work with a wide and diverse range of customers. From small local business to large multi-national enterprises, as well as government agencies and militaries, my team's insights were gained through engaging and helping a wide variety of customers and end users. This knowledge is a valuable commodity. We continue to build it by closely monitoring industry trends and the ever changing cyber security landscape. We also help our customer's apply a real-world approach to this ever challenging space.

Security and IAM solutions are multi-layered. They starts as simply as training users on safe computing practices and can end with fine-grained dynamic authorization rules applied to web services or cloud-based applications. In fact, there are so many security offerings and disciplines available that oftentimes organizations don't know where to begin. In this white paper, I will address this daunting issue: where to start and where to go from there.

With the extremely broad offering of security solutions and the costs associated with each, the first step is the toughest. At a minimum, your network should have the two default security mechanisms; a capable directory technology like Active Directory or LDAP, and a feature-rich firewall solution. But once you have those pieces in place, then what?

If you were to evaluate the recent security breaches, you would find that nearly all of them could have been nipped in the bud with three simple security solutions; multi-factor authentication, secure web access management and privileged access management. These solutions

If users can't get to their stuff in an easy manner, they will find another way — probably one that introduces risk to your organization

are relatively inexpensive, easy to leverage, and provide the fastest ROI and peace of mind.

Multi-factor authentication

The need to ensure that the person logging in is, in fact, who they claim to be is fundamental to security. The vast majority of breaches are perpetuated by nefarious people who obtained credentials that allowed them to login to systems to which they should not have access. The easiest way to prevent this unauthorized access is to raise the level of assurance that the person logging in is really who they say they are. And multifactor authentication is the de-facto approach.

We all know what multifactor authentication is (something you know PLUS something you have), and we all know we should have it. But why haven't we done so already? Basically, I see that most organizations have at some point tried multifactor authentication and the user response was so negative that it was either killed as a project or made so limited in scope as to be irrelevant.

A typical approach to MFA is to simply ask the customer for a one-time-password (OTP) in addition to their normal login credentials. In an MFA-enabled environment, you could almost broadcast your credentials in public, and the people who hear you still won't be able to login as you unless they have your unique token generator. So, what's so bad about that?

Here's a sample of what's bad about that:

- An OTP was difficult or inconvenient to get
  - User's need to carry around an extra device, like a card or key fob.
- If you didn't have your token, there was no way to do your job
- The MFA setup wasn't 'smart' — or very adaptive.
  - User frustration often sounds like this: "Why am I prompted every time for a token, when clearly it's still me sitting here using the system?"

Well, much has changed. Let's take One Identity's Defender product as an example:

- You can get the one-time password via almost any conceivable type of token
  - SMS Text Message
  - Email
  - Native Smart Phone Applications
  - Desktop applications (Windows, Linux, Mac, etc.)
  - Even the traditional key-fob/USB thingy-type tokens
- Modern helpdesk and web portals make any operation faster
  - User token management and requests are self-service.
- There is no reason to bother the help desk.
  - Modern user-helpdesk features involve simple clicks, and not complex engineering.

Honestly the biggest change in the MFA landscape is the smart phone. Smart phones are ubiquitous. I mean, don't most 13-year-olds have a smart phone these days? But alas, we still have that pesky enforcement point, right? Not necessarily.

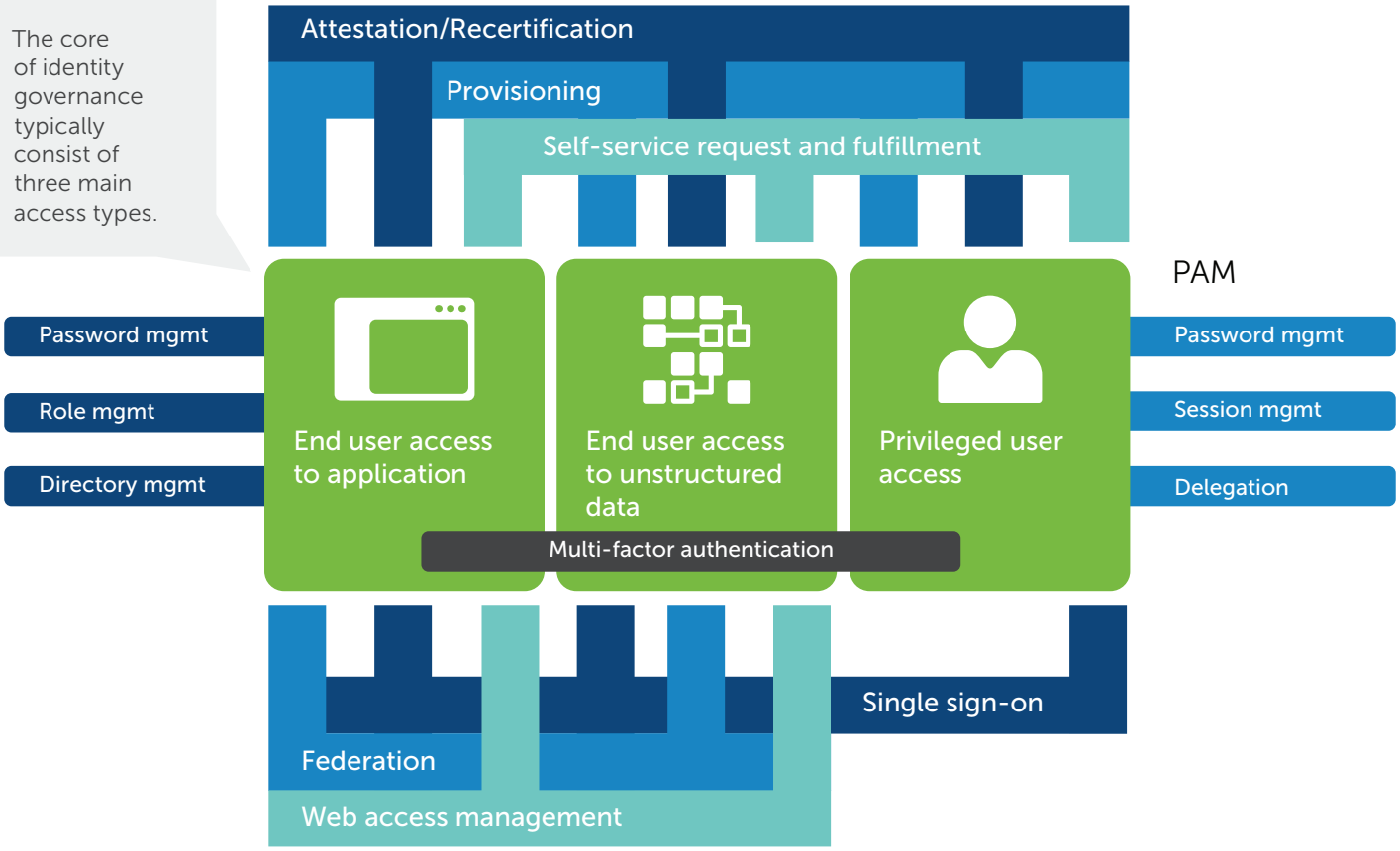
It's generally accepted in our industry that around 99 percent of the time, the user attempting to authenticate into a system is actually that user and not an impersonator or a hacker. When we understand that, our philosophy on authenticating users can transform from making it inherently difficult for users to making it simple, easy, fast and secure. Subsequently, we could reallocate our authentication-computing power to identifying threat or anomalies of a hacker hitting the environment.

What do you need to make this transformation? You need risk-based authentication. You'll get that with Cloud Access Manager (CAM), One Identity's web-access management (WAM) platform.

Identity governance

IAM entails many elements but some fundamental technologies can facilitate the implementation of your security project and set it up for long-term success, including the blue areas in the figure below.

The core of identity governance typically consist of three main access types.



Regardless of how a user accesses resources — including privileged accounts — from inside the network, via the web or federated credentials, you can benefit from adaptive-security functionality of multi-factor authentication to ensure they are who they say they are.

Web access management

Which brings us to the second piece of low-hanging fruit. The whole point of computers, IT and all of that stuff is so that people can do their jobs better. Providing easy, optimized access to the applications and data that users need is critical. After all, if people can't get to their stuff in an easy manner, they will find another way — one that is probably non-secure, and introduces risk to your organization.

That's where a web access management solution, such as One Identity's CAM, comes in. Instantly, it bares fruit, if you will, due to its many security benefits, a few of which we've highlighted below:

- **Single sign-on to any web application.** CAM provide organizations with unified access for federated applications as well as non-federated applications. It supports extending SSO and externalized security to the following web security paradigms:
  - Legacy authentication models: Form-fill, Windows authentication, basic authentication and header injection. Nearly anyway that legacy or custom-built web applications need to authenticate is supported.
  - Federated authentication protocols: SAML 2.0, WS-Federation, WS-Trust (for O365 thick clients), OAuth, and OpenID Connect. It supports most methods used by modern federated applications, including Salesforce, Office 365, Google Apps and thousands of other mission-critical apps.
- **Secure reverse proxy.** CAM also provides secure remote access that minimizes the negative impact on end users. CAM's reverse proxy allows you to connect to intranet applications from the internet without a VPN. We understand that a VPN is essential technology but also feel that companies often rely too heavily on VPN access at the cost of user convenience when, in fact, a reverse proxy technology is more than adequate for a high number of access types — and much more secure for others.
  - User don't always have VPN and/ or they need to access internal sites from places where their VPN technology is either difficult to leverage or simply forbidden by policy. Image a mobile phone or the local library, these are places where a user should never, or can't, configure VPN connections.
  - Partners with VPN access? Some companies find that the only way they can provide a partner access to an internal web resource is to provide VPN access. This is a tremendous risk that can become unnecessary once a reverse proxy is available.
- **Auditing.** Because CAM can be the identity provider (IdP) for your federated applications and all your other applications, it becomes the default audit trail for your entire environment. Without an IdP like CAM, how do you know what your users are accessing? You would need to go to every application developer to collect user audit data; if it was even available. With CAM, you'll know every detail of every user's access from connections made to cloud targets, like Google Apps, to connections made to legacy systems with no built-in audit capabilities at all.

Finally, and probably most importantly, CAM is installed with a built-in risk engine – called the Security Analytics Engine. With the introduction of a risk engine to your web access management strategy, you will have an intelligent, adaptive authentication capability that allows your trusted users to authenticate quickly, while making the challenge for an attacker all but insurmountable. Enabling the risk engine in your environment means instantly filtering your traffic for the following risk indicators (to mention a few):

- **User behavior**. I like to refer to this as the user's forensic thumbprint. CAM's risk engine creates a unique profile for each user in your environment, taking into account factors like client IP addresses, geographical location, typical time of day, the browser used, and more. If a user's connection exhibits the typical profile for that user, then the risk is low. However, if that same user is connecting from overseas, or on a machine we've never seen from an IP address in a blocked region, the risk is off the charts and that connection is automatically denied.
- **Blacklist filtering.** There are many public blacklists available on the Internet... in fact, Dell SecureWorks produces an industry leading blacklist that to which you can subscribe. But think for a moment, if these blacklists are available, why aren't you filtering out these connections already? Our risk engine can leverage public blacklists as well as your own custom blacklists.
- **Malware detection.** Firewall solutions can automatically detect machines on your network that exhibit the signatures of malware, adware and spyware. But rather than simply sit on the information or do a wholesale denial of access, it sends this type of data to the risk engine where those indicators are used to calculate a risk score for users connecting to your web applications.
- **There's more.** Again, there are more capabilities to list here, but this document would grow quite a bit. Other valuable plugins can do things, such as
  - Measure the legitimate time it would take for a user to connect from one location to another, and raise risk if the user seemed to travel a long distance in a short amount of time
  - Refer to your internal directory and determine if a particular user has elevated roles (like domain administrators) and assign risk accordingly.

So, what do we do with this information? We calculate a risk score. If that risk score is low enough, your users will not see a multi-factor prompt. The higher the risk score, the more involved the authentication process and the more restricted the access they may gain (if they aren't denied). Your users could be asked for a multi-factor token or even blocked completely. That's adaptive authentication – or context-aware security. Again, the goal here is to make it as easy as possible for our users to connect while simultaneously blocking attacker at every opportunity. This is something you can only do with a risk engine, and you get that right out-of-the-box with One Identity's CAM.

So, these two solutions - a capable MFA solution and a simple secure WAM strategy – can quickly seal up security holes in your organization. Now it's time to grab our last piece of low hanging fruit but this time it's a piece of fruit that many organizations don't even realize exists. It's like a unicorn fruit (??). It's one that could have prevented many of the most high-profile data breaches. It involves protecting our most important assets with privileged access management (PAM).

Privileged access management

In any organization, there are administrators who literally have the keys to the kingdom; and rightly so. For a company to run smoothly, someone must have the root access to servers to provide maintenance, troubleshooting and configuration. But that privileged access comes with serious risk, to the organization and the person with those responsibilities.

Once a hacker gets access, his or her next step after breaching your organization is to elevate their privileges and create back-door accounts to further their access. If your domain administrator's credentials are compromised or a latent Kerberos identity is decrypted and replayed, the attacker has carte blanche access to your organization's most sensitive data.

But imagine a scenario where your administrators don't even need to know what the credentials are to access a secure server. In fact, what if nobody in the organization knew what those credentials are? It is this idea that drives the concept of PAM. In a company using PAM, like One Identity's Privileged Password Manager product, a dedicated hardened appliance manages all the credentials to your secure servers, infrastructure, applications, databases and everything else. And it does this independent of human interaction.

When an administrator needs to gain access to a high-risk workstation, they simply authenticate against the PAM server, supplying MFA credentials, if necessary, and they 'check-out' the password to a secure target for a predetermined amount of time. With the One Identity solutions, not only can they check out the credentials to a secure server but can also dynamically open remote control sessions that are recorded in a DVR-like fashion.

Not only is the organization free from having high-risk access protected by a managed password appliance, but the administrator is also protected. For instance, imagine something has gone wrong in your environment. Typically, all suspicions would be aimed at the administrator. But if that administrator could actually replay the video capture of what he did during the period he had checked out credentials for that server, he could prove that he was not the one that 'dumped the user table'.

Make your fruit salad

Fortunately, the solutions described above are not difficult to implement, but they are cost effective, and deliver a security coverage that would have prevented some of the most notorious breaches in recent news. Rightfully so, many companies are reticent to invest in the giant framework security products they see today, as there is legitimate concern about realizing ROI. So, how you do consume and overcome this security challenge? Easy: one bite at a time.

In the mélange of fruit to which we've just introduced you, you have three distinct — but very integrated — solutions. You can start anywhere. Whatever your greatest need is, and then move on to the next priority. You

> Every organization should be prepared for when its best security efforts aren't quite enough.

don't have to take it all on at once. These three security products — multi-factor authentication, web access management and privileged access management — are a tasty mix. Plus, you can start to recognize ROI in days, not months.

Governance: how to limit damage when the inevitable happens

Are there still risks — even with all three solutions implemented? Of course. In spite of the best technology, the best intentions, and the most diligent oversight — security is not a perfect science. Every organization should be prepared for when its best security efforts aren't quite enough. Such as when a user exposes their credentials; or a contractor receptionist allows an impersonator dressed as an exterminator into the server room; or someone drops their keys in a parking lot. These things happen. Even with MFA, WAM and PAM in the mix, sometimes it's still not enough to protect your organization if an attacker is motivated and lucky. So, are we left to wait for the inevitable or is there something we can do to mitigate the risk? The answer is simple: governance.

The notion of IAM governance is beyond the scope of this white paper. However, we should can explain why a more strategic IAM strategy that includes modern governance is so important.

Governance solutions like Identity Manager provide a number of features, including some of the following relevant capabilities:

- **Provisioning.** A governance system should not only control provisioning to your internal directory (like a feed to Active Directory from your ERP) but to the universe of applications to which your users connect. It should be universal in nature.
- **Attestation.** A governance system should be capable of reviewing the access granted to the user community and provide insight as to when those users leverage those systems or if they actually should continue to have access to those systems.
- **Workflow.** Any change to a system, access right or user database should be controlled through a carefully designed workflow with proper audit controls.

Of course there are many other features of a full-blown identity management system, such as dynamic role memberships, user self-service and more. But consider the three solutions discussed in this document.

The simple fact is, if and when your environment is breached, how are you to know, if you don't have governance in place? If an attacker's first tangible goal is to create a back-door account and escalate his privileges, are you going to see that happen and be able to react to it?

Identity Manager will see those out-of-band changes and inform your administrators that it has identified the changes as a risk. What we're talking about here is a way to be as proactive as we can. It is a governance platform that provides the final security blanket we need when all else has failed.

Summary

So yes, you need governance. It is the Holy Grail that every IT security team should be striving for. But we recognize that the budgets are not always there or that we haven't effectively evangelized the executives to make the story complete. So do we give up? No, we prioritize, pick the low hanging fruit and prepare our organization as best we can.

Think about what an attacker is going to do.

- He's going to steal credentials
  - No worries, we have MFA in place.
- He's going to use stolen credentials to access privileged management servers
  - No worries, we don't even know the credentials to those servers.
- He's going to compromise a contractor's laptop and gain access via VPN
  - Nope, our partners connect through a reverse proxy
- He's going to connect to our web portal using brute force attacks
  - Again, with our risk engine covering our web assets, we're safe.

So, take another look at the quick security wins you can get with the low hanging fruit of IAM. When when you are ready to apply modern governance, you'll be confident that the rest of your organization has already been protected in the best ways possible.

About the Author

Joe Campbell is Principal Solutions Architect at One Identity. He is an accomplished software developer with an extremely diverse background. His career spans innovations for some of the world's biggest companies; and he's pioneered new, award-winning technologies in wireless, RFID, visualization, communications and telephony. As a trusted security advisor, his experience in security and software architecture makes him a highly-respected visionary and leader in the technology industry.

For More Information

© 2016 Quest Software Inc.
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

About One Identity

The One Identity family of identity and access management (IAM) solutions, truly offers IAM for the real world including business-centric, modular and integrated, and future ready solutions for identity governance, access management, and privileged management.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.