Future-ready Identity and Access Management

By Todd Peterson, IAM evangelist, Dell Software

Software

Q: Why do we have technology?

A: Technology empowers people to do their jobs better, which ultimately helps them reach organizational objectives more quickly and more completely.

Q: Why do we have security?

A: We have security because not everyone is trustworthy and if the information used to reach organizational objectives falls into the wrong hands, it can be abused, misused or violated.

Q: What does identity and access management (IAM) have to do with technology and security?

A: IAM is the controls put in place to make sure that the right people have the correct access to technologies and data that exist solely to achieve organizational objectives.

Q: So why is it all so hard?

A: Sit right back and I'll tell a tale … there is no easy answer.

The great unknown

Most of the challenges we face with security, and IAM in particular, are based on the diversity of the systems that must be controlled, the complexity of the disparate solutions put in place to secure access to those diverse systems, and the constantly shifting landscape of users and the ways those users choose to access those systems.

Every time a new system is introduced or a new access opportunity presents itself, we face a crossroads. On the one hand, we can do our very best to secure the new system or the new access method on its own, hopefully (emphasis on "hope") with the ability to draw on existing security practices or technologies; or we can take a step back and redesign security across the board so that everything, including the new player, is addressed as a unified whole. The second option is ideal yet entirely impractical, while the first option is the reality of the situation and the root of the problem.

We don't know what tomorrow will bring. We can't redesign our security systems every time something new comes up. We can't throw out existing investments and proven systems and practices simply because the new investment doesn't "play nice" with them. So we're left doing the best we can with the hand we've been dealt, but often that isn't enough. Risk doesn't go away simply because we're trying hard. Compliance doesn't rest because we have the best intentions. And users don't forgive security-caused inefficiency simply because systems don't play nicely with each other.

In other words, the future is the great unknown and no one can afford to wait for the future to arrive before making critical IAM decisions.

How we got here

When thinking about future-ready IAM, I like to look at and learn from the past.

Let's look at the tale of two platforms: Windows and Unix/Linux. Back when Unix was king and Linux was gaining ground, and when Windows NT was all the rage, the only way to secure those systems was by treating each server as an independent island. That meant from an IAM standpoint each user had a unique account, an independent authentication method and unique authorization. So, clearly, administration was a nightmare.

To overcome the problem, the *NIX world pursued complex synchronization scenarios and non-secure tools that made things slightly better, but only as long as everything remained constant. Unfortunately, this complex synchronization by the *NIX world, doesn't support a future-ready IAM solution. In fact, it was wholly unequipped to address pending trends.

Windows, on the other hand, took an entirely different approach. Rather than attempt to make the disjointed approach to IAM work, Microsoft took a step back and evaluated the right thing to do with an eye on the flexibility and scalability necessary to address whatever the future would hold and consequently an opportunity to help influence the future. The result was Active Directory, a single source of authentication and authorization for all things in the Windows universe. And the rest, as they say, is history.

... the challenge of the day must be addressed quickly and with the tools available at the moment.

Interestingly, the *NIX world soon embraced the concept of the unified directory for all servers and the thriving Active Directory bridge industry was born. Rather than create its own unified directory, *NIX chose instead to take advantage of what Microsoft had already done – future ready IAM at its best.

The culprit in most IAM approaches that are rigid and not future-ready is the necessity that the challenge of the day must be addressed quickly and with the tools available at the moment. Keep in mind, the vast majority of vendors' IAM solutions are designed to address a single problem, on a small set of systems, for a specific type of user access scenario. Consequently, it is not in the vendors' best interest to encourage a forward-looking, universal approach to solving the problem. The single sign-on (SSO) industry is a perfect example of this. Early SSO solutions simply synchronized passwords to overcome the difficulties of disjointed servers. Subsequent solutions addressed thick-client applications with the storage and replay of passwords. However, when the cloud and federation came into the mix, newer solutions were designed to optimize the advantages of the web. The password synchronization solution was not ideal for thick client applications, and the password replay solution did not do what was best for cloud and SaaS applications. And modern federation solutions typically ignore all the legacy needs of servers and thick clients. None are future-ready.

A privileged account management (PAM) solution implemented with little foresight may act as a barrier to future PAM activities

A future-ready SSO solution would completely cover the latest trends while also embracing legacy needs. It would also include the flexibility to expand into the unforeseen future without wholesale technology replacement. The same holds true for other aspects of IAM – a privileged account management (PAM) solution implemented with little foresight may act as a barrier to future PAM activities, and a governance/provisioning solution that is so reliant on customization that it cannot easily adapt to changing user, environmental, or other needs could prevent the very business agility it is meant to enable.

But in spite of pockets of future-readiness, the vast majority of IAM approaches and solutions are simply not equipped to adapt as new challenges arise. It's no one's fault. You as an organization are tasked with securing your enterprise and making IAM work. You don't have the time or resources to "future-ready" everything that has grown over time. In many cases, a new trend that you choose to adopt to further your organizational objectives cannot wait for the technology providers to catch up and provide you with future-ready solutions. In addition, we as vendors are driven to develop products that will be purchased. If my focus as a vendor is on a small area of IAM (say SSO, a password vault, or an attestation/recertification tool), my motivation is to deliver the solution that will solve your specific pain as quickly and thoroughly as possible. If my solution is future-ready, that's a nice bonus but not the reason I'm in business, or the major benefit I'm going to pitch to get you to buy.

That is unless I offer a broad range of IAM solutions, and the cumulative value of them increases as they work together and address your immediate challenge while also being able to deal with what comes next — even if you and I don't know what that is.

The future-ready approach to IAM

Dell is all about the "future-ready enterprise." To Dell, future-ready is an approach that changes the way your business thinks about IT. If we extend that thinking into the specifics of identity and access management, future-ready IAM changes the way your business thinks about and executes on security.

Dell's future-ready approach is based on five fundamentals that easily extend into the realm of IAM.

1. **Invest in simplicity –** Actively, aggressively understand the value of existing systems and transition off of rigid, aging ones that are expensive to maintain. One of the foundational concepts of the Dell One Identity family of solutions is a modular and integrated approach that ensures that each IAM solution can strongly stand on its own, and the cumulative effect is greater than the sum of its parts.

   Even the name of Dell's IAM suite "Dell *One* Identity" connotes the concept of simplicity. IAM through Dell helps you to get to *one* identity, *one* set of policies, *one* set of access controls, and *one* set of rights to audit. Removing the need to define identities and controls each and every time a system is introduced, a new access scenario is necessary, or a new user population emerges is the ultimate manifestation of future-ready IAM.

2. **Embrace open standards –** Open standards allow for new functionality to flow into any organization, resulting in improved collaboration and interoperability – plus a competitive edge. Dell One Identity solutions draw upon the latest standards, while embracing the proven standards that form the foundation of IAM success. This is true whether it's the myriad standards (Kerberos, LDAP, SAML, WS Federation, OAuth, OpenID Connect, etc.) that allow communication to take place across diverse systems, or the specialized standards (for example PAM, NSS, and RADIUS) that enable specific functionality in specific systems and for specific use cases,

   The Dell One Identity family is meticulously dedicated to supporting them all. This means that Dell's single sign-on solutions work across everything from the most modern federated application to legacy applications that cannot support the latest thing. Or, a multifactor authentication solution can be implemented across virtually any system or user population. With Dell One Identity, there is no proprietary secret sauce that is designed to "hook" a customer into our technology trap with no easy way out. Standards are the essence of future-ready IAM.

3. **Think software first –** Software allows for more flexibility because it's constantly updated and can quickly add new capabilities that are tailored to the needs of your business. Dell has a legacy in excellent hardware, but recently expanded into equally innovative and future-ready software.

Dell One Identity solutions provide the path to the next step in your IAM evolution.

The Dell One Identity family of IAM solutions is one of the crown jewels in Dell's software portfolio. By embracing software's flexibility to adapt as needs evolve and the unforeseen emerges, Dell's IAM solutions have future-ready running through their veins, Dell One Identity embraces the concept of configuration as opposed to customization, open standards rather than closed systems, and interoperability for universal utility instead of solving the problem-of-the-day at the expense of tomorrow's challenge.

Rather than add new software every time a new use-case emerges, Dell One Identity solutions provide the path to the next step in your IAM evolution. For example, tackling the provisioning challenge with Dell One Identity, automatically puts you in a position to address governance needs, without additional investment or another project. Overcoming the management and security challenges of Active Directory with Dell IAM solutions easily expands to non-Windows systems with the simple addition of an AD bridge; addressing federation needs for the latest SaaS application automatically can tackle the single sign-on needs for legacy applications, the need for secure remote access, and the emerging requirement to deliver context-aware security – all from the same solution with no additional investment and no customization.

4. **Build end-to-end security –** End-to-end security allows businesses to remain protected and compliant while building confidence to adopt new technologies – like cloud, mobile, and big data. But you don't adopt new technologies just because they are new – you adopt them because they further your business. And the antithesis of future-ready IAM is the ad-hoc security that so often accompanies the latest trend or newest technologies.

The technologies themselves are great and help you reach business objectives, but the security those technologies require (if done the wrong way) can counteract any gains that drove the decision to adopt.

A future-ready approach considers the entire range of security needs and unifies as many previously disparate systems and practices as possible. For example, typically a firewall is deployed to protect the perimeter and IAM solutions are implemented to control user access. Rarely, do they communicate. In fact, they are rarely even mentioned in the same security breath or purchased in the same security project. Both are extremely important and the cumulative effect of both can be dramatically augmented if they are considered together.

Only Dell can offer both sides of the security coin and only Dell can combine their respective information to raise the security bar.

End-to-end security allows businesses to remain protected and compliant while building confidence to adopt new technologies.

Similarly, a typical IAM deployment addresses provisioning first (often with a rigid, entirely customized, and not future-ready IAM framework) and then adds governance after, with an entirely different solution from an entirely different vendor, along with all the integration headaches and retro-fitting that prevent future-readiness. The same can be said for privileged account management. Implementing one type of solution (lets' say a Unix root delegation solution) from one vendor and another (perhaps a privilege safe) from another, does not bode well for the future.

However, Dell One Identity solutions extend the end-to-end security concept into the realm of IAM. Provisioning and governance are tightly linked. That governance is broad, covering user access, data access, and privileged access, privileged account management is about all the use-cases—not just the ones we like, and authentication covers all the bases including the ones you haven't needed ... yet.

5. **Modernize and automate –** Modern systems save money, enable differentiation and allow labor-intensive processes to be automated.

Even more than poor technology choices, poor operational choices are the biggest barrier to future-ready IAM. A heavy reliance on IT—with its accompanying glut of manual processes, tribal knowledge, and doing the best you can with what you have—can derail even the most well-meaning IAM project. But often, those decisions are forced upon us by the technologies we choose. How can you deal with the unknown future when you're struggling to keep our head above water in the present?

Dell One Identity solutions are all designed to remove the cumbersome manual processes (or the cumbersome collections of non-integrated tools) from the equation, freeing IT and the rest of the organization to focus on what matters most. But it doesn't stop there, Dell's IAM portfolio also focuses on putting the visibility and power of IAM in the hands of the right people – not just the people that know how to use the tools. That means that provisioning can be entirely run by the line-of-business personnel that know who should access what. This then extends to governance activities, which suddenly become quick and easy exercises for the line-of business, not finger-pointing battles between IT and the rest of us.

Similarly giving IT the tools necessary to do what they need to do in an entirely consistent and accurate manner places them in a position to participate in business-enabling innovation. Removing the need for heavy IT intervention every time a new user is added, a new access scenario is required, or the auditor comes calling is the ultimate expression of future-readiness.

A future-ready approach to IAM is achievable, even if you have no idea what the future is going to look like. By following a few basic tenets you can be in a much better position to succeed. Remember:

1. Invest in simplicity
2. Embrace open standards
3. Think software first
4. Build end-to-end security (or IAM)
5. Modernize and automate

Dell, with its Dell One Identity family of IAM solutions is uniquely positioned to help you on your journey to future-readiness. The comprehensive nature of the Dell One Identity portfolio and the advantages of a solution set that drives everything on a path to governance, focuses on business-centricity, a modular and integrated solution-set, rapid ROI, and an intense focus on future-readiness can finally make security – and IAM in particular – a business enabler not a productivity barrier.

To learn more about Dell's unique and powerful view on being future-ready at powermore.dell.com/future-ready/

Learn more about Dell One Identity family of IAM solutions at dellsoftware.com/solutions/identity-and-access-management/

For More Information

The information in this document is provided in connection with Dell 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 Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL 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 DELL 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 DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell 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. Dell does not make any commitment to update the information contained in this document.

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology — delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

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

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com

Refer to our Web site for regional and international office information.

Ebook-FutureReadyIAM-US-GM-26836