DELL Software

Get Your IAM Project Back on the Fast Track by Considering Business Agility

Get management behind your identity and access management strategy by demonstrating how it delivers business value as well as security

Written by Bill Evans, senior director of identity and access management, Dell Software

Abstract

For years, identity and access management (IAM) has been seen as the project of denial, restriction, limitation and sometimes failure. The processes and technologies required to enhance security seemed also destined to stifle collaboration and interfere with revenue-generating work. In fact, at times, the processes forced employees, partners and customers to spend precious time searching for ways to circumvent the IAM infrastructure in order to do their jobs.

With the next generation of IAM solutions, this no longer needs to be the case. In addition to delivering security, these new modular and integrated solutions enable the business. For example, these solutions:

- Enable IT to offload those pesky decisions of who needs access to what and put them in the hands of business owners who can better address them
- Empower auditors to get what they need without interrupting the business
- Enable individual workers to get swift and controlled access to the things they need to be productive and do their jobs

Therefore, IT professionals tasked with the paradox of securing the enterprise in the face of declining project dollars need to recast their IAM projects' benefits beyond just providing security. Today, your IAM project can not only solve today's (and tomorrow's) security threats, but also add business value through increased operational agility. This white paper explains how.

> Today, your IAM project can solve today's (and tomorrow's) security threats, and also add business value by increasing operational agility.

Introduction

Why organizations are reluctant to invest in IAM

For years, organizations have invested in monolithic IAM solutions as a panacea to solve both efficiency and security issues. But many (dare I say most) of these organizations have yet to see the fruits of their investments and labor — in large part because the IAM strategy was flawed from the outset. Many of these efforts were predicated on the belief that "if we deploy this IAM product, it will be used," which just wasn't (and isn't) the case. IAM, properly understood is not a product; it's a project — and an ongoing project at that.

In fact, IAM deployments have failed so often that most organizations today have either been burned by their own IAM initiative gone wrong, or they know someone else who has. In either case, C-level leaders, finance departments and auditors are reluctant to invest in anything related to identity and access management.

What's an IAM professional to do?

That leaves you, the IAM professional, tasked with solving both today's and tomorrow's critical security issues — all without adequate funding. According to Saugatuck Technology, "spending on security today averages just 0.0023 of annual revenue, or the annual operating budget for government agencies and non-profits. The impact of this paltry level of spending on security is keeping cyber-thieves coming back for more and will continue making cyber-theft pay handsomely and with few if any consequences."[1]

The solution to this problem lies in recasting our understanding of IAM itself. Many people look at security as an investment in something NOT happening, as opposed to an investment in something actually happening (like revenue generation). In other words, they look at security investments as insurance policies, and IAM projects have been focused exclusively on solving security threats by controlling privileged accounts, ensuring swift provisioning and deprovisioning, enforcing strong passwords, and so on.

This mistaken understanding of IAM needs to be corrected. In today's world, IAM pros need to present their IAM initiatives not as products to be implemented but as projects that can do both of the following:

- Solve today's (and tomorrow's) security threat
- Deliver business value by driving enhanced agility

How to position your IAM request so it gets funded

I know what you're thinking at this point: "Sure, Bill, I understand what you are saying. Rather than beg for IAM solutions as a security-only play, I should update my request with how this investment will make the business better. But that's easier said than done."

To be sure, there is no one way to ensure a successful request. But I can provide you with several examples of how others have positioned their IAM projects to ensure new, additional or continued funding.

IAM improves productivity by providing easing the delegation of access.

In most companies, the rank and file employees might schedule their own travel and complete their own expense reports, while management get an executive assistant (EA) who acts on their behalf. But what if the EA to the vice president is out sick the day that the VP needs to change flights while traveling in the Far East? How fast can your IT department provide a different EA with the access required to perform the last-minute travel change on behalf

[1] *Saugatuck Technology, "Cyber Risk and Spend on Security: How Do You Compare?," October 30, 2014.*

Share:

f **g+** **in** **t**

DELL

of the primary EA? More to the point, what happens if that timeframe isn't fast enough and the VP gets stuck overseas and misses his or her child's baseball game? Likely, the VP arrives back at HQ and chews out the VP of IT.

In this situation, what's the value of being able to reassign or delegate access rights? Pretty vital. But in reality this is just a provisioning and access control function of an IAM solution.

Scenarios like this should help you to recast IAM as an enabler of business agility — in this case, by keeping VPs traveling, but more broadly by keeping the company productive.

IAM improves agility by putting access decisions in the hands of the business. Has something like this ever happened to you? Marketing, in its never-ending quest to generate interest and additional business, launches a new campaign. In this case, the goal of the campaign is to drive additional pension contributions, which are handled by your pension management application. And lo and behold, the campaign works like a charm — except that marketing failed to forecast that success, and now the call center is inundated with requests. Customer calls are going unanswered because you don't have enough reps with access to the pension application to help out.

What if the business, without the help of IT, could enable access for an additional set of resources to the pension management application? In other words, the line-of-business (LOB) people do not have to fill out some form on a random SharePoint site that gets sent to IT who forwards it to IT management where it sits because someone is in a meeting, and so on. Rather, the LOB manager can authorize access immediately for the right group of reps, and it's all logged and audited. The business gets reps on the phone faster, sales increase and the business is ... wait for it ... more agile.

Other options
There are many other opportunities for an IAM solution to make the business more agile. For instance:

- Provide a gearbox manufacturer's design partner with access to the company's chassis design details through federation and the partner's own self-service application, thus streamlining business.
- Enable single sign-on (SSO) to the new cloud-based lead-nurturing app the CMO purchased without telling IT.
- Give a ship's captain access to SAP on his iPad so he can update the delayed arrival time into dock when he's in the middle of the Atlantic.
- Give the $3,000-per-day consultant root access to every machine she needs within five minutes of her arrival at work, thereby minimizing billable delays.

IAM enables mobile and cloud initiatives by mitigating security concerns.
Still not convinced? Let's look at two of the most overused tech buzzwords of the last five years: cloud and BYOx (where x = device, identity, whatever).

Undoubtedly, your IT management team is wrestling with how to best deal with these phenomena. Perhaps you have remote sales people who want their email (which contains sensitive attachments) on their personal iPhones. Or maybe a VP received a new tablet as a birthday gift and wants to use it to access the financial system.

On the cloud front, maybe you are dealing with "shadow IT" — various departments are procuring their own IT solutions like Campfire for project management or some cloud-based marketing automation system. Or maybe it's as simple as employees storing confidential material on Box so they can work on it from home on their personal computers.

Whatever the situation, when confronted with these obvious security gaps, the business people almost always sing a familiar refrain, "I need this so I

IAM can improve agility by putting access decisions in the hands of the business.

Share:

> **You can help build your case for IAM funding by showing how having good access control — one hallmark of an IAM project — enables BYOx while at the same time eliminating 50 percent or more of the risk of the BYOx project.**

can be more productive and we can remain competitive."

And then mayhem ensues.

Again, it doesn't have to be that way. If we look at the IAM investment as a way to enable the business, it can go a long way to mitigating these security gaps. For example, when employees use their own devices for company work (BYOD), IT typically focuses on the "remote wipe" capabilities. But you also need to think about the importance of accurately and tightly controlling access.

Perhaps this tale sounds familiar: An employee is hired to job A and accordingly is given access to applications A1 and A2 and to database A3. Then that employee transfers to job B and is given access to B1, B2 and B3 — but his access to A1, A2 and A3 is not rescinded. Now this employee is able to access resources he should no longer use. Eventually this employee travels and his mobile phone is stolen. Simply by cracking the phone's four-character security code, the thieves will have access to A1, A2, A3, B1, B2 and B3. Essentially, because this organization had poor access control, the risk of BYOD doubles (or triples, or worse).

You can help build your case for IAM funding by showing how having good access control — one hallmark of an IAM project — enables BYOx while at the same time eliminating 50 percent or more of the risk of the BYOx project.

Advice from Forrester Research
Forrester Research's report, "Use Commercial IAM Solutions To Achieve More Than 100% ROI Over Manual Processes,"[2] lays out additional advice for making a case for project dollars for your IAM project:

You can only garner executive and business support with quantifiable costs and benefits. Much like a business plan for a startup, IAM requires a plan and cost benefit analysis to justify spending for a project and garner executive support.

Using a spreadsheet to quantify the benefits and costs will force discipline and give you quantified results — readily usable in a presentation to senior stakeholders when asking for an (increased) IAM budget. To build your business case for IAM you must show:

- *How much the company is currently spending on manual processes.*
- *How you stack up compared with other companies.*
- *How leaving security functions decentralized undermines security.*

Conclusion

In today's world, it's mandatory for organizations to have the right security policies and practices in place to prevent intrusions, protect intellectual property, maintain privacy, and ensure compliance with corporate policies and government regulations. Nevertheless, obtaining approval to move forward with an IAM project to deliver that security can be a challenge because of past project failures. Therefore, IAM pros need show how IAM technology both delivers security and enables business agility.

With today's modular and integrated IAM solutions, IT can secure data, meet uptime requirements, satisfy compliance obligations and increase productivity by giving users faster access to the data and applications they need to do their jobs. For example, by putting control over access into the hands of LOB users, IAM enables business agility as well as more accurate provisioning. By enabling the organization to make new employees,

---

[2]*Andras Cser with Stephanie Balaouras and Jennie Duong, "Use Commercial IAM Solutions To Achieve More Than 100% ROI Over Manual Processes," Forrester Research, December 4, 2014.*

Share:

partners and consultants productive faster – whether by facilitating collaboration with partners, giving a high-priced consultant the right access instantly, or ensuring an employee has the necessary access to cover for a sick team member – IAM improves agility and adds business value. The trick is to change the conversation from restrict and deny to permit and enable, making IT the force for "yes" rather than "no."

About the author

Bill Evans is the senior director of product marketing for Dell's identity and access management businesses. With more than 18 years of experience as a product and marketing manager for various IT solution providers, Bill has a wealth of experience in the creation and positioning of software products targeting specific IT pains. In his current role, he drives the strategic direction of the Dell IAM team, which includes setting product and solution positioning, creating the global direction for demand generation and other sales support efforts, and providing content for sales enablement activities. Previously, Bill served as product marketing director for Dell's Windows and SharePoint businesses and as general manager of the SharePoint and Notes transition business unit at Quest Software.

> With today's modular and integrated IAM solutions, IT can secure data, meet uptime requirements, satisfy compliance obligations and increase productivity.

Share:

For More Information

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.

Share:

WhitePaper-IAM-BusinessAgility-US-VG-25644