



Techniques for Transitioning to an IAM Suite

Organizations often fill their IAM needs with a variety of disparate techniques and applications, many of which are home grown or built by a variety of third parties. This tip will explain out an organization can ensure a successful transition from multiple products and tools to a single suite. It will look at:

- How to successfully map functionality from old product/tool functions to new ones
- How to evaluate and manage new and existing policy exceptions
- Guidelines for implementing custom connectors with legacy applications

Sponsored By:



Understanding multifactor authentication features in IAM suites

Joel Dubin May 20, 2008

Just as compliance has driven the growth of identity and access management (IAM) suites, compliance has also driven the growth of multifactor authentication.

More specifically, interest in multifactor authentication has been driven by regulations like the Federal Financial Institutions Examination Council (FFIEC) directive calling for multifactor authentication for Internet banking transactions. Multifactor authentication has also benefited from a growing trend toward merging physical and logical security, which is dependent on multifactor authentication products for managing the combined use of traditional passwords along with newer technologies like smart cards and biometrics.

So it's no wonder that as multifactor authentication has grown, it has become an increasingly important part of the technology offered in enterprise IAM suites.

But does multifactor authentication work effectively as part of an IAM suite? Does multifactor authentication deliver on its promises of increasing security, or is it just another nuisance to users? Do IAM suites add anything new to multifactor technology, or is it more of the same? What are some best practices for incorporating multifactor authentication into an IAM suite? These are some of the issues we'll explore in this tip.

Defining multifactor authentication

First, let's briefly define multifactor authentication. There are three authentication factors: something you know, something you have and something you are. Something you know would be a shared secret that you memorize, like a user ID and password. Something you have would be a device, like a smart card or a one-time password (OTP) token, and something you are refers to a physical characteristic, like a fingerprint, facial pattern or voice recording.

Multifactor authentication combines two or more of these factors to create a layered defense. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into a target system.

Some have claimed multifactor authentication is a hassle and difficult for users, and doesn't offer extra security, since smart cards can be hacked and OTP tokens have been breached by man-in-the-middle (MITM) attacks. However, by and large multifactor authentication systems have proven to successfully augment security for access management systems and breaches, though trumpeted in the media, are still relatively rare.

Considerations for multifactor authentication within IAM suites

IAM suites offer multifactor authentication functions in the form of access management component add-ons. They don't function as separate components by themselves, and despite the recent consolidation in the IAM sector, standalone multifactor authentication vendors haven't been targets.

So when shopping around for an IAM suite, consider the multifactor authentication capabilities that may already be—or could be—integrated with the suite’s access management functions. Remember, multifactor authentication is an afterthought for IAM suites. It’s an add-on, not a standard feature, and may not necessarily be included in a vendor’s basic package. Most importantly, consider the strength and flexibility of the access management piece. If it can accommodate multifactor authentication, then it’ll comfortably mesh with the rest of the suite. If the access management piece itself is the weak link, don’t expect to make it work better by bolting multifactor authentication on top of it.

Fortunately, as demand for multifactor authentication has grown, IAM suites have evolved by updating identity profiles with the digital identity data underpinning multifactor authentication and updated login screens to accommodate physical devices.

Although some security experts question whether multifactor authentication actually increases security—they say it isn’t perfect and can be cracked just like any other authentication system—it does add an extra layer of security for IAM suites. What’s different about IAM suites that make it better protected by multifactor authentication? IAM suites, for the most part, even when connecting remote offices and systems, sit behind the firewall deep inside a company’s network. The user base is employees, over whom the company has control through access controls, and not customers over whose security the company has little or no control. Even outside vendors and partners, who might access the company’s network through the IAM suite, must still be vetted before being added as authorized users. And those outside users can still be required to use multifactor authentication.

Whether or not multifactor authentication is a nuisance to users depends more on how it’s rolled out, deployed and implemented than on its functionality within the suite. Since an enterprise IAM suite deployment is a major undertaking and should be done in phases. The same phased-deployment rule applies to IAM attachments, like multifactor authentication, so all bugs and kinks are worked out before its deployed enterprise-wide.

Since multifactor authentication is bolted on to IAM suites as an option rather than a feature, IAM suites don’t anything new to multifactor technology. The advancement of multifactor technology is independent of IAM suites.

Multifactor authentication best practices

Before diving into multifactor authentication, as a best practice, conduct a thorough risk analysis of the systems requiring access. Because of the higher overhead in hardware and implementation of multifactor systems, they should only be used for protecting high-risk data or transactions.

And the selection of which multifactor device to use should be driven by the enterprise’s business needs. Smart cards are one of the easiest to set up and install and can be expanded for merging physical and logical access, if this is a requirement. Biometrics, originally only used for securing physical access to facilities and high-risk money transfers, now comes as a standard feature, even on some laptops. But, again, it’s not a standard feature of all access management systems, so first make sure it’s part of your IAM suite.

Part of the convenience of IAM suites is their ability to scale as an organization grows, either internally or through acquisition. Check that your chosen multifactor system can also scale in tandem, so that your suite doesn’t outgrow it.

About the author: *Joel Dubin, CISSP, is an independent computer security consultant. He is a Microsoft MVP, specializing in web and application security, and the author of The Little Black Book of Computer Security available from Amazon. He hosts a regular radio show on computer security on WIIT in Chicago and runs The IT Security Guy blog.*

Resources from VeriSign



[Best Practices for Selecting and Deploying an IAM Suite](#)

[Tips for Overcoming Authentication Challenges](#)

[Access Management in 2008: Challenges to Expect and How to Address Them](#)

[Podcast: Expert Tips to Overcoming Authentication Challenges](#)

About VeriSign

VeriSign, Inc. (Nasdaq: VRSN) operates digital infrastructure that enables and protects billions of interactions every day across the world's voice, video, and data networks. VeriSign operates the systems that manage .com and .net, handling up to 31-billion Web and email look-ups every day, and provides global enterprises with trusted security solutions. VeriSign also run one of the largest telecom signaling networks in the world. Additional news and information about the company is available at www.verisign.com.