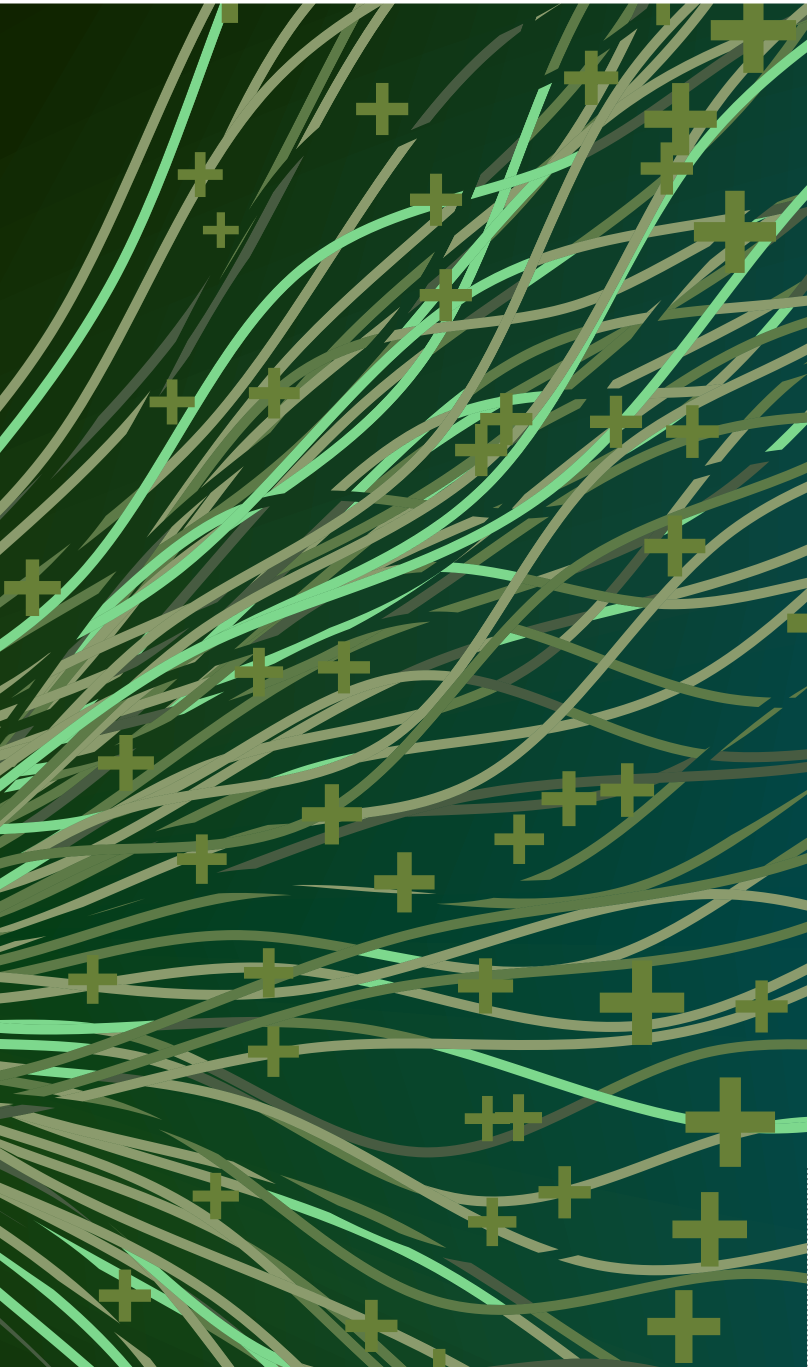


E-Guide

IS THIRD-PARTY MANAGEMENT IAM'S NEXT MISSION?

TechTarget | SearchSecurity

Home

Is third-party management IAM's next mission?

IDENTITY AND ACCESS management of employees is complex enough; but now IAM must extend to third-party vendors too.

IS THIRD-PARTY MANAGEMENT IAM'S NEXT MISSION?

Michael Cobb

Are the unmonitored activities of contractors and business partners who are accessing your internal systems keeping you up at night? Based on what happened in 2014, maybe more people should be losing sleep.

Identity and access management deployments are notoriously complex, prone to failure, and things are getting worse as legacy technology encounters next-generation applications. Today's IAM programs manage a far wider range of user types and access points. Bring your own device (BYOD), cloud computing, and the rapid spread of distributed applications and data have all added to the security challenges. As the traditional network perimeter continues to disappear, robust IAM becomes more important as a layer of defense to protect sensitive corporate data from the threats posed by less security-minded suppliers, partners and customers.

Home

Is third-party management IAM's next mission?

We've all heard the horror stories: Lax security at third-parties continues to be implicated in major breaches. Home Depot's network was breached when hackers used a third-party vendor's user name and password to acquire elevated rights. Jimmy John's point-of-sale system was hacked when criminals were able to obtain the login credentials from the chain's payment technology vendor. When attackers compromised Fazio Mechanical Services Inc., a heating, ventilation and air conditioning subcontractor, to gain access to Target's network the resulting loss of debit and credit card information had a domino effect that rippled through the retail and financial services industries. The high costs to those industries, namely banking, finally got the U.S. on board with Chip and PIN. The list goes on, and organizations need to change how they manage third-party access so that they don't join it.

When it comes to opening information systems up to third parties, enterprises need to re-examine their technology-led approaches to IAM; otherwise it can be costly. The good news is that many security breaches can be avoided by implementing best practices and simple or intermediate IAM controls.

Home

Is third-party management IAM's next mission?

NEW STRATEGY NEEDED

Despite the exploits of contractor Edward Snowden, whose NSA data is still being leaked on the Internet two years after he left the U.S. intelligence agency, many companies have yet to design IAM programs specifically for third parties (non-employees), particularly when it comes to governance and monitoring, according to Gartner Inc.

How do you know it's time to rework your IAM strategy for trusted third-parties who have access to your internal systems and data? Your program is coming up short if it's generating excessive maintenance and management costs, and causing performance problems due to an increasing number of employee, supplier and customer identities.

Aging IAM deployments can delay new projects without support for modern applications, cloud services or scalable single sign-on (SSO). This situation can propagate data silos due to the difficulty of migrating or consolidating pools of information. Worst still is the increasing struggle of ensuring that third-party access (authorization and authentication) to sensitive data and infrastructure remains controlled and compliant. As with many aspects of information security in today's interconnected world, automation is needed to handle the explosion in the volume of data and types of users that collaborative

Home

Is third-party management IAM's next mission?

organizations need to manage.

When Intuitive Surgical Inc. found 30% of its IT support tickets were password resets, the Sunnyvale, Calif., purveyor of robotic systems for minimally invasive surgeries, deployed identity management and governance software from Avatier. One module of the software suite, which creates a single system for access requests, saved three hours on user provisioning and automated the password reset process, freeing up valuable time for Intuitive Surgical's support technicians. Avatier's technology, which automates group expiration and access management, is used by the U.S. Air Force, Starbucks, Marriot Worldwide and ESPN, among other companies.

Computer passwords, which first appeared in the mid-1960s at MIT, still play a significant role in enterprise IAM programs despite their well-documented limitations. With the advent of cloud computing and the Internet of Things, legacy IAM deployments that can't accommodate alternative authentication methods (multifactor and digital certificates), and deliver SSO, will become a security liability and a major constraint on business aspirations. Enterprise and partner IAM systems (ideally) should support the same authentication methods, protocols and standards.

Home

Is third-party management IAM's next mission?

WHO, WHAT, WHERE AND WHEN

In global organizations, hundreds, maybe thousands, of vendor and supplier technicians require remote access to information resources to help maintain operations. This task is made more difficult because non-employees are not tied into internal HR systems and hierarchical workflows.

Without careful management, these relationships pose significant risks that can affect revenue and expenses. The Ponemon Institute's "2015 Cost of Data Breach Study: Global Analysis," co-sponsored by IBM, puts the average cost per stolen record at $154; the cost tops $300 in healthcare and education. If a third party is the cause of a data breach, it increases costs an average of $16 per record, the biggest negative factor on the overall cost, according to Ponemon's findings.

It doesn't matter whether data is on-premises or off, the responsibility for data security ultimately lies with the organization, not its providers or suppliers. An assessment of the risk posed by allowing third-party access to internal resources should take into account, should a compromise occur, the potential damage to intellectual property and private data, brand reputation, availability, compliance and the bottom line. The risk assessment can be used to flag areas in which more due diligence is necessary or access should be withheld.

Home

Is third-party management IAM's next mission?

Only trusted business partners and suppliers that add real value to the organization should be considered eligible for (least privileged) access to internal apps and data on-premises or in the cloud. Before granting access, you should conduct an in-depth assessment of the third-party's ability to perform required activities in compliance with data protection laws and best practices. This will involve an audit of their systems, a third-party assurance report, or a completed self-assessment form. A key area to concentrate on is how the third party manages the roles and access privileges of its own employees. Orphaned accounts and excessive privileges should be treated as serious concerns.

Periodical reassessments should be carried out to ensure ongoing compliance with the security standards set out in the contract. Procedures for dealing with non-compliance include:

- Notification of the failure and a period in which to address the non-compliance;
- Help in remediating the failure;
- Terminating access to sensitive data; or
- In serious cases, terminating the contract entirely.

Home

Is third-party management IAM's next mission?

The main objective is to rectify any lapses in third-party security before vulnerabilities can be exploited.

While active oversight of well-documented and binding service level agreements is vital, controlling and monitoring third party access with business and technical controls is even more critical.

Enterprise IAM is changing from managing usernames and passwords to checking that the user, their device, their location, their credentials and their request are all valid and appropriate, from geolocation to time-of-day. A contextual range of checks is essential to control third-party access and avoid a repeat of last year's breaches (which relied on compromising third-party credentials).

A growing range of IAM products are designed to handle more open environments, providing identity and access security that is intelligent and contextual. New IAM tools not only make interactions with partner-facing applications smoother, they add context to the identification and authentication process so administrators can dynamically adjust access rights according to the perceived risk. Vendors like Okta and Centrify are leading the way in cloud-based Identity as a Service (IDaaS), while Microsoft and Amazon offer hybrid technologies with cloud-based directories that link to on-premises IAM systems.

Mobile devices, aided by the growing adoption of the Fast Identity Online (FIDO) Alliance's open authentication specification, launched in late 2014, will certainly play a role in the quest for zero-touch and password-free authentication. Security keys for USB devices from Yubico and mobile authentication software from Nok Nok Labs Inc. are already commonplace.

PROCESS BEFORE PRODUCTS

To create an IAM program specifically for third parties, you should have a detailed understanding of what data and services on your internal network and outlying cloud infrastructures you need to protect, and how and by whom those resources will be accessed.

This assessment requires business managers and IT to bring data asset registers and classifications for resources, on-premises and off, up to date. Access points and access rights for users, supplier and consumer applications and devices can then be drawn up so the appropriate authentication methods can be selected to control access. It's important to consider future requirements and roadmaps such as moving in-house processes to a third party. Federated identity management, or the integration of identities from multiple sources, may not be a requirement now, but it likely soon will be.

Home

Is third-party management IAM's next mission?

The Internet of Things means that device identity will become just as important as user identity, so device control and authorization capabilities are a must. Network access control systems will need to be able to support IAM by ensuring that BYOD and IoT devices comply with security requirements before granting them access to the network.

As monitoring is becoming the best way of detecting and preventing malicious activity, an IAM system has to provide detailed access logs, including access attempts. This data will provide many of the clues necessary to spot unwanted or suspicious activity. Although it's a demanding task, this review process will create a clear list of requirements and priorities and show which aspects of an IAM system are the most critical for success.

Data security is also shifting from an "IT problem" to a "boardroom problem," as executives are increasingly held accountable for breaches that damage their corporate brand—so expect a higher level of C-level involvement in any review of IAM strategy.

Once you have established your IAM process, the next step is to assess IAM technologies and services against prioritized objectives. Talk to tool vendors to get a feel for their support and response times to security issues and their ability to support the applications, devices, and authentication methods identified

Home

Is third-party management IAM's next mission?

by your organization as essential to its information security. Ask for proof of performance in authorization response times, scalability and reliability, and test for a convenient and frictionless end user experience: This usually means support for SSO at enterprise scale and the latest protocols needed to run modern applications, software as a service and cloud. Ask for customer case studies and references and make sure your team has adequate time to evaluate each short-listed IAM component. Some vendors charge by user and others charge by line item, so you should evaluate each IAM system using a per-user, per-month cost model to get a true comparison of costs.

OPTIONS GALORE

Whether you are upgrading existing IAM systems or transferring to new technologies, you'll find numerous options. On-premises technologies such as Fischer Identity, IBM Security Identity Manager and AlertEnterprise Guardian Logical work best for enterprises that need customizable functionality and have the resources to manage the integration process.

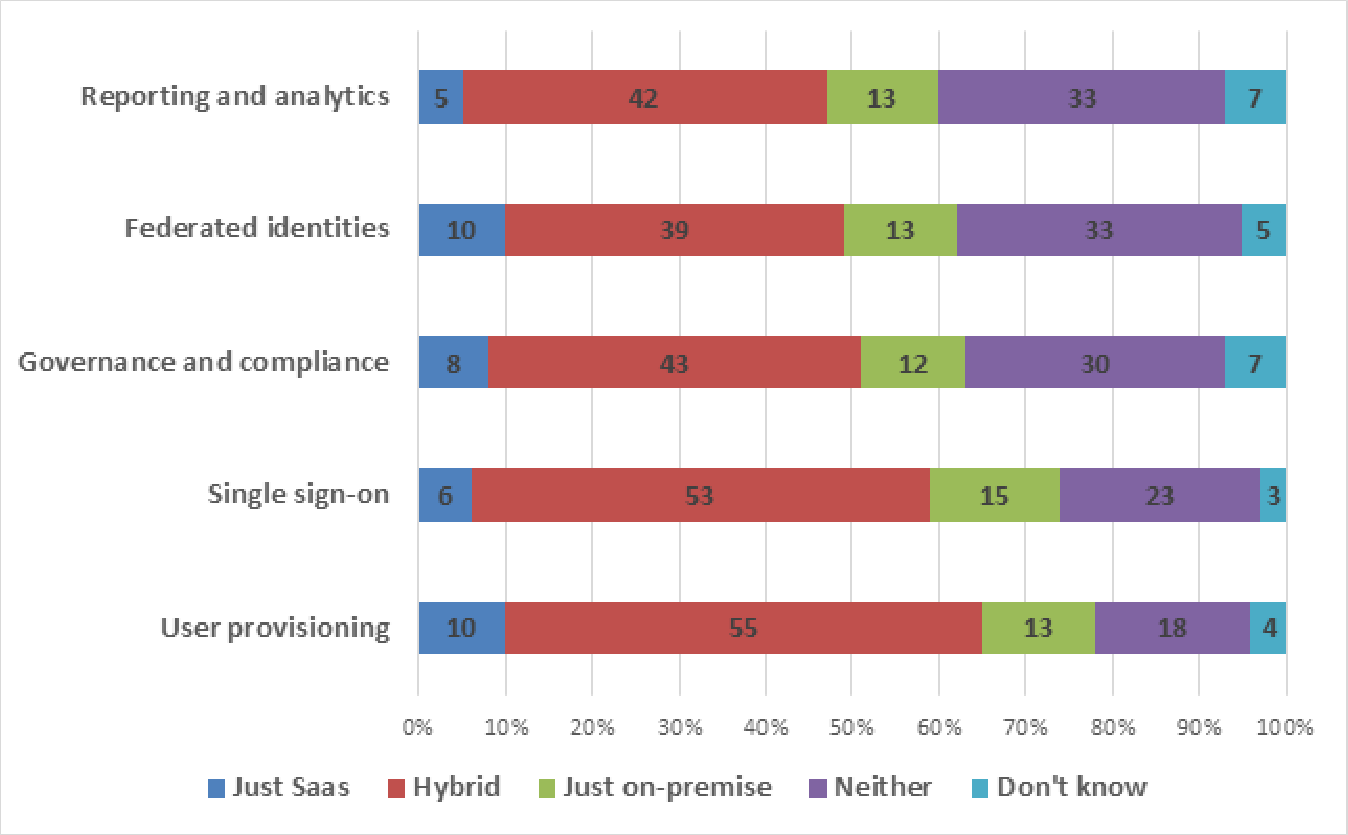
Many products are available on a pick-and-mix basis, such as Avatier's Identity Management Suite. Dell Software offers three separate modules that cover identity lifecycle management—provisioning, access control and

Home

Is third-party management IAM's next mission?

governance—which can be deployed on-premises or through its IDaaS.

HOW IDENTITY AND ACCESS MANAGEMENT IS DEPLOYED



N=300 IT PROFESSIONALS IN FRANCE, GERMANY, U.K. SOURCE: QUOCIRCA LTD

Home

Is third-party management IAM's next mission?

Cloud applications and services generally offer faster implementation and immediate cost savings. As many are pay-as-you-go, the system can be rolled out over a period of time, allowing administrators to learn how a selected group of users handles the transition. OneLogin's on-demand system features support for SSO, multifactor authentication, directory integration and user provisioning; it also offers a regularly updated catalog of pre-integrated applications. Other IAM offerings can be deployed on- or off-premises or as a hybrid, such as CyberArk's Privileged Account Security Solution.

If in-house IT skills and time are in short supply, IAM as a service (IAMaaS) is a good choice as it requires minimal hardware or software on-premises. Many vendors offer a SaaS version of their products, with Okta and Microsoft Azure AD Premium leading the way.

FLUID BUT NO LEAKS

Third-party access introduces operational, compliance and reputation risks but modern enterprises can't survive without opening up their infrastructures and data resources: Identity is the new perimeter.

Without the right IAM program, monitoring non-employees and their level of access to necessary resources can take hours of IT effort, and the process is prone to costly human error. Controlling third party access is challenging because these users are fluid. They represent a weak link in many enterprises' defenses as evidenced by the 2014 breaches, and this needs to change.

An IAM program that automates day-to-day tasks and makes authentication secure yet simple for third-party users will pay for itself by freeing IT staff to perform more value-added responsibilities. It will also keep data assets protected while enabling them to be used in new and innovative ways.

Traditional IAM was developed a decade ago. The sector has changed dramatically in just the past 24 months. Now is the time to take a look at your third-party management program, and evaluate some of the IAM technology and standard innovations that can help protect data as it becomes more widely accessible.

MICHAEL COBB, CISSP-ISSAP, is a renowned security author with over 20 years of experience in the IT industry. He co-authored the book IIS Security and has written many technical articles for SearchSecurity.com and other leading IT publications. He was formerly a Microsoft Certified Database Manager and a registered consultant with the CESG Listed Advisor Scheme (CLAS).

Home

Is third-party management IAM's next mission?

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.