Brief: Reframe The Business Case For Identity and Access Management In Security Terms

IAM Is More Than Just Operational Streamlining

by Andras Cser
with Stephanie Balaouras and Jennie Duong

WHY READ THIS BRIEF

The responsibility and the budget for identity and access management (IAM) often reside with a number of different business and technology management teams. Historically, the easy business justification for IAM investment came from its impact on administrative operational efficiency — for example, help desk agents spend less time resetting passwords, and automated access recertification campaigns save managers and application owners time. For security and risk (S&R) professionals, IAM has become crucial to improving the company’s overall security posture. However, to gain budget and increased control for a function not always under their direct control, S&R pros will have to reframe the business case for IAM in security terms and make a direct connection to the CIO’s top technology initiatives. This report presents the most important security benefits of IAM in its component areas — access management and identity management — to help S&R professionals build a solid case for implementing IAM.

YOU CAN’T SECURE YOUR ENTERPRISE WITHOUT ZERO TRUST IDENTITIES

In Forrester’s Zero Trust Model of information security, one of the core tenets is the mandate to reduce and strictly enforce access control. Time and time again, we see breaches occur as the result of compromised or stolen employee credentials or a malicious insider with excessive privileges. For S&R pros that want to prioritize IAM, it’s not always a simple matter. In some businesses, groups such as human resources and finance often tussle with each other and the security team over ownership of key employee and other user information. Other businesses will deliberately parcel out various IAM functions and components. For example, in some financial institutions, the security team owns identity administration, but the risk department owns authentication strategy because of the direct connection between authentication and fraud management. As a result, if S&R pros want to prioritize IAM, they must have the will and the skill to explain its vital importance to the company’s overall security posture and bring together a cross-functional group of stakeholders. To do this, you’ll need to break down the benefits of its core components — access management and identity management.

ACCESS MANAGEMENT CENTRALIZES CONTROL AND LOWERS SECURITY COSTS

Access management (AM) encompasses web single sign-on (SSO), federated access management, and entitlement management within applications. Popular vendors of on-premises AM products include CA Technologies, ForgeRock, IBM, NetIQ, and Oracle; those offering identity-as-a-service in the cloud include CA Technologies, Centrify, Okta, OneLogin, Ping Identity, and Sailpoint. According to Forrester clients, AM:
■ Centralizes access control. Enforcing policies that control access to most, if not all, enterprise applications is important not only for end user convenience (since an employee can log in once to the SSO environment and navigate between applications without having to log in again) but also for security. Developers designed many applications to perform authentication and authorization solely within their own silo — but AM provides a single chokepoint to control access to all web applications and, in many cases, thick-client applications.

■ Allows application developers to use centralized and more secure IAM features. AM provides a single, highly secure, uniform, and repeatable framework for managing how users log into applications. Application developers should not rely on one-off security and application-specific authentication mechanisms — they should instead leverage the mechanisms and frameworks that a commercial off-the-shelf AM solution provides. This not only improves security, but it also greatly reduces application security development costs, as app-dev teams don't have to reinvent the wheel every time they code access control into their applications.

■ Follows a centralized access policy management scheme for applications. Centralized application access management policies are a good thing, because they provide a single point of enforcement for user access to tens, hundreds, or even thousands of applications. Administrators have one window into access policies and can audit, version, and set alerts for any changes in policy. This allows for a coherent set of rules governing application access.

■ Centrally audits all application and data access. The beauty of centralized AM is that in order to find forensic information in case of a data breach or unauthorized user access to applications, investigators or auditors don't have to track and correlate the user's activities in the access logs of multiple applications. This information is all in one place: the audit logs of the AM solution. This significantly reduces the time to carry out forensic investigations and gives a reliable, 360-degree view of a user's access. Companies can further improve their security posture by integrating AM solution logs with a security incident and event management (SIEM) solution; this provides even more visibility and access analytics intelligence.

■ Makes it easier to protect against OWASP vulnerabilities in applications. When a company develops its own authentication methods, it needs to protect every application from OWASP vulnerabilities individually. AM solutions centralize these defenses and make them much more robust. AM solutions have industrial-strength session token-management methods, encryption key rotation schedules, and protection that far exceed the security, robustness, and scalability of most solutions built in-house.

■ Makes it easier to integrate adaptive and multifactor authentication into applications. Without AM, companies need to integrate every single application individually and repeatedly with multifactor authentication such as one-time password tokens, smart cards, and biometrics, and risk-based authentication, AKA adaptive or contextual authentication solutions like CA
Technologies RiskMinder/AuthMinder, Entrust/Datacard IdentityGuard, and RSA Adaptive Authentication. But AM frees firms from this by allowing them to have a single point of integration between authentication solutions and business applications. This is the cornerstone of the process of eliminating passwords for application authentication.

- **Uses federation to free you from managing passwords for business partners.** Managing passwords for business partners is not a good idea; your organization takes on additional help desk costs as well as the extra risk of losing those users’ passwords. AM provides a one-time, simple integration of business partner access by using security assertion markup language (SAML) and OAuth without forcing applications to deal with this task.

- **Mandates a single password.** A common and seemingly intuitive counterargument against AM solutions is that one password is less secure than multiple passwords (“Don't put all your eggs in one basket.”). In reality, if one password gets compromised — say someone finds a yellow sticky note with all of your passwords written on it in your desk drawer or underneath your keyboard — you have no way of assessing if other passwords were also compromised and need to be reset. If you only have one password, then that’s the only password that needs to be reset in case of a password breach — speeding the mitigation of a security incident.

- **Enables uniform password strength via password synchronization.** Passwords will be a necessary evil of access control for the foreseeable future, so it’s important to ensure that they are equally strong across all applications. By centralizing passwords, AM ensures that firms can enforce secure password policies more effectively. Forrester sees organizations mandating that passwords contain eight to 12 characters — at least one of which is an upper-case character and one of which is a number — and do not contain dictionary words, one of the user’s names, or their ID. In short, AM ensures that there are no weak application-level passwords in the enterprise. Password change regimes, timeouts due to inactivity, and wrong-password lockouts are also much more easily and effectively implemented with AM.

- **Monitors employees’ access to deter and reduce employee fraud.** A centralized AM solution provides a single window into all employees’ access across all applications and data assets. This usually means that employee access is much more transparent and that there is an easy way to monitor, alert on, and intercept any suspicious access, not just within an application but also across applications. This serves as a deterrent for any employees considering committing fraud.

- **Reduces the risk of cloud by greatly improving cloud workload access control.** Cloud SSO solutions like Okta, OneLogin, and Ping One centralize access management to cloud workloads. Firms managing employee access to the cloud (infrastructure-as-a-service and software-as-a-service business applications) through one central chokepoint greatly reduce their risk of shadow IT applications and unauthorized use of the access privileges of terminated users.
Easily integrates with mobile device management platforms to reduce BYOD risk. In the face of disappearing legacy VPN and network perimeters and increasing user requirements to provide SSO between mobile applications, new-generation AM solutions improve security. Newer mobile apps all use security on the application programming interface level (primarily OAuth tokens) and thus are part of a centralized and more secure AM framework.

Centrally consumes security intelligence for dynamic fraud management. Modern AM solutions not only integrate with SIEM solutions but can also consume logs and signals from SIEM and other security intelligence platforms. This means that an AM solution can proactively terminate the live sessions of users whose risk score suddenly increases — for example, if a user tries to access too many things or downloads too much data all at once. This allows AM solutions to be a much more useful and integral part of layered enterprise cybersecurity defenses.

**IDENTITY MANAGEMENT REDUCES EXCESSIVE PRIVILEGES**

In addition to managing the requirements for and update schedule of passwords and lockouts, identity management (IDM) solutions improve firms’ security posture. Example of IDM solutions include CA Technologies Identity Manager and GovernanceMinder; IBM ISIM; NetIQ Access Governance and Identity Manager; Oracle Identity Manager and Oracle Identity Analytics; and Sailpoint IdentityIQ and IdentityNow. S&R pros employ user account provisioning, access request management, access recertification, and role management solutions to do this because IDM solutions:

Eliminate stale user accounts via password management and synchronization. If an IDM solution manages user IDs and passwords across many user directories (e.g., Active Directory, LDAP, or relational database management systems), then it can easily detect stale user IDs — those belonging to an inactive user — or user IDs whose associated passwords have not been reset in the past three to six months or do not meet minimum complexity requirements. Password management solutions force periodic password resets and synchronize a single password to all managed endpoints, such as user directories and applications.

Eliminate uncertainty in manual IAM joiner, mover, and leaver processes. The process by which users get all of the application and data access rights they need is often manual, inaccurate, and slow — and thus insecure. Using an automated IDM platform to automatically provision users and serve as a central point for user access requests and manager access request approvals forces companies to rethink, simplify, and consolidate their legacy manual joiner, mover, and leaver processes, invariably resulting in better overall visibility and higher security for controlling application and data access rights.

Enforce separation of duties (SoD) reactively and proactively. IDM and access governance platforms maintain a set of rules dictating which application and data entitlement combinations are toxic and should never be assigned together to a user’s profile. Maintaining SoD policies
manually is a very hard job: You have to periodically look at all of the entitlements a user has, determine which of them conflict, and remove any conflicting entitlements. In addition to this reactive measure, you must proactively (and manually) look through all of the entitlements that a user is asking for at the time of the request and ensure that they do not violate SoD rules. IDM solutions automate the tedious job of SoD maintenance, leaving far fewer ticking time bombs of excessive and toxic user access in place. This also improves a company's security posture.

- **Reduce the security threat surface via automated access recertification.** Manual periodic access recertification campaigns are usually inaccurate and involve a lot of rubber-stamping, as reviewers often lack a full 360-degree view of the user's entitlements. IDM solutions automate recertification, greatly reducing the reliability, accuracy, and timeliness of these campaigns. In some cases, this results in 50% to 60% fewer users with excessive or toxic privileges, improving identity security. Access governance often drives projects to eliminate, integrate, and/or reconcile user directories. The fewer the instances of user information that you have to protect, the more you can protect them and the lower the likelihood of user data being stolen.

- **Unify access request processes and generate a paper trail.** Manual access request and approval processes may result in an unreliable or nonexistent paper trail tracking how a user got access — for example, who requested it and who approved it. IDM automates access request and approval processes, giving a single window into how users gained their access. Forrester clients also report that the simplification of access request workflows in itself results in higher levels of security.

- **Enable identity context in data access governance.** Understanding which shared network drive a security group membership provides access to, and, conversely, which security group memberships grant access to a shared network drive, is critical in preventing data loss. Maintaining this bidirectional mapping between shared network drives and security groups manually is an impossible task: Over time, inaccuracies and inconsistencies will appear. IDM solutions offer automatic bidirectional mapping between data assets to security groups (attributes) that greatly improves a company's data security.

**Recommendations**

**MEASURE IAM SUCCESS WITH SECURITY METRICS**

If you want to maintain or increase your budget as well as your control of IAM, you must define, measure, and track security metrics that matter to you but also other technology management leaders. The administrative and operational benefits of IAM are still important, and technology management pros often use them to justify initial investments, but if you really want to reframe the business case for IAM to include security, you have to demonstrate the benefits in concrete terms. Here are a few simple ways to get started with IAM security metrics:
- **Create a prioritization scheme for applications and data.** Most companies report that, to be able to protect their applications and data, they need to inventory and prioritize those applications and data. IAM platforms can help highlight audit logs of user access to applications. Based on IAM access logs, S&R professionals should put applications that handle often accessed sensitive (e.g., financial) data, or applications with one-off access controls or proper access recertification schedules high on the priority list.

- **Define and track IAM proxy measures for security exposure.** Typical proxy measures include the number of stale accounts, the number of accounts whose passwords were reset more than six months ago, and the number of SoD violations. Then track how IAM systems reduce these metrics.

- **In case of a breach, identify and add the identity-related metric that may have contributed to it.** In the unlikely case of a security breach, clearly identify the IAM-related artifact or metric which, if managed properly, would have contributed to preventing the breach. Then track and manage that metric with the IAM solution. Such metrics may include, for example, number of orphan accounts in databases, number of default and unchanged network equipment, Windows Administrator or Unix root passwords, and age of employee’s passwords.

### ENDNOTES

1. Forrester believes that S&R pros must eliminate the soft chewy center by making security ubiquitous throughout the network, not just at the perimeter. For more information, see the October 7, 2014, “No More Chewy Centers: The Zero Trust Model Of Information Security” report.

2. Malicious breaches are increasing and compromising externally and internally sensitive data; in the past two years, healthcare and financial service industries have experienced some of the worst breaches and heaviest fines. For more information, see the November 14, 2014, “Lessons Learned From Global Customer Data Breaches And Privacy Incidents Of 2013-14” report.


5. This is a process in which managers and application owners review and then either approve or reject their employees’ or application users’ access rights.