CORE SECURITY

Intelligent IAM For Dummies

Core Security Special Edition

CORE SECURITY

Table of Contents

Introduction

Identity and Access Management (IAM) systems provide the capability to create and manage user accounts, roles, and access rights for individual users in an organization. They typically incorporate user provisioning, password management, policy management, access governance, and identity repositories in an often complex design.

Because providing IAM is a huge task, you're likely to face many challenges. You may be asked to confirm the accounts in your IAM system and the access rights for each, which can be a daunting and difficult task. Unfortunately, the environments that IAM systems support are often subject to both purposeful attacks and inadvertent permission creep due to changing roles and rights within your organization. In many organizations, periodic reviews of accounts and permissions and manual remediation tasks that try to fix them are the only way to manage rights issues.

Keeping track of who should have access to what can be a seemingly impossible and unending task. Organizations face new challenges as they provide multitudes of devices and systems access to data while attempting to manage the tangled web of rights, permission, and accounts that their users need.

About This Book

With new risks appearing and compliance requirements always present, organizations need a way to manage risks and threats. That's where Intelligent Identity and Access Management (Intelligent IAM or IIAM) comes in. This book shows you how to leverage Intelligent IAM to help keep your organization's identities and accounts safe and secure.

Chapter 1

Introducing Intelligent Identity and Access Management (IIAM)

In This Chapter

- Understanding what IIAM is
- Looking beyond traditional IAM
- Knowing whom IAM is for

This chapter introduces you to Intelligent Identity and Access Management (IIAM or Intelligent IAM). After reading this chapter, you should have a better understanding of what IIAM is. You also learn why traditional IAM is no longer enough in today's ever evolving world. Finally, this chapter informs you of whom IIAM is for.

What Is Intelligent IAM?

Intelligent IAM (IIAM) encompasses all the administrative processes used in Identity and Access Management (IAM), but the processes are influenced by real time data. IAM solutions that use intelligence continuously collect, monitor, and analyze large volumes of identity and access related information, combining data not only from provisioning and governance solutions but also from security products and other external systems. IIAM solutions are often designed to be used with a provisioning system, a governance system, or both.

IIAM solutions, which include integrated identity analytics and intelligence (IAI), help find key information hidden in complexity and provide visibility into context and comparative data. These solutions may help organizations

- Avoid security breaches by continuously monitoring for policy violations and vulnerabilities and by uncovering problems hidden in large volumes of data
- Strengthen risk management by reducing vulnerabilities immediately and by highlighting individuals and resources associated with high risks
- Continuously improve provisioning, governance, and other IAM processes by focusing attention on weak links and ineffective processes
- Improve the productivity of IT staffs by giving them tools to quickly and reliably conduct analyses, find patterns, identify anomalies, and spot trends

Why Is Traditional IAM No Longer Enough?

Until recently, traditional IAM encompassed only provisioning and governance products needed to evaluate or audit access to confirm that the access provided is in compliance with business policies and external governance regulations.

Some examples of traditional IAM functionality include the following:

- Provisioning solutions automate the granting and revocation of access to applications, IT systems, and services; tangible assets such as laptops, smartphones, and security badges; and intangible entitlements such as access to secure areas.
- Governance solutions provide tools to enable compliance with government regulations, industry standards, and organization policies, and to verify that compliance.
- IAM solutions have helped organizations automate operations, reduce manpower needs, simplify audits, and provide users with access to the applications and resources they need. Yet traditional IAM processes are far from perfect.

Organizations are still challenged by issues such as lingering abandoned accounts for users no longer affiliated with the organization, proliferating orphaned accounts with no administrative oversight, people with inappropriate access to data, and policy violations. These challenges increase the level of risk to the organization.

In Figure 1-1, you can see the impact abandoned accounts have on your organizations. With so many accounts left with no owner, you greatly increase your risk of a breach.

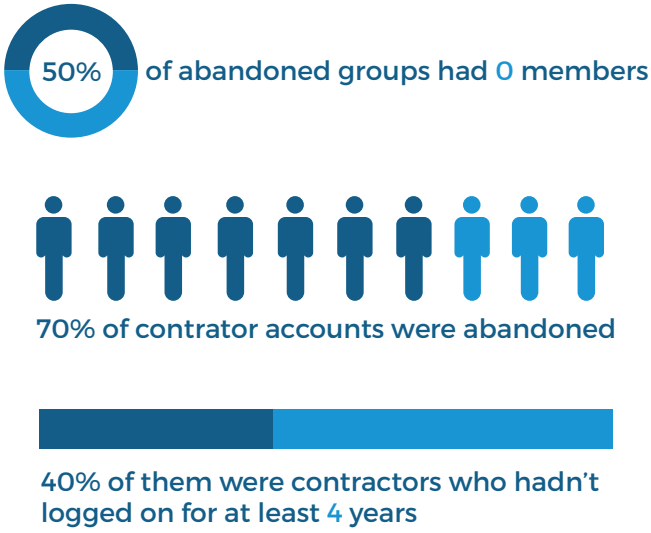

Figure 1-1: Abandoned or orphaned accounts are a huge risk for companies.

Who Is Intelligent IAM For?

The most frequent users are IIAM administrators and analysts, security professionals, incident response teams, compliance officers, and fraud prevention staff. These individuals use the system to identify policy violations and suspicious activities as they occur and to analyze identity and access data in order to uncover and mitigate vulnerabilities.

Other users may include the following:

- IT operations and support teams who take advantage of notifications and alerts to respond to access problems and support users
- Business managers who can better understand access rights in their departments, ensure that everyone has the permissions needed for his or her work, and prevent people from accumulating excessive permissions that might lead to violations of security or privacy policies
- "Resource owners" (administrators managing applications, databases, files, and other corporate resources) who want to avoid over provisioning of access to their resources
- Compliance and risk officers and auditors who can quickly gather meaningful information to simplify audits and assessments and who can implement micro certifications to ensure ongoing compliance with policies
- IAM administrators and analysts and other security professionals who can use data to align role definitions with business needs and to drive continuous improvement in account provisioning, governance, and other IAM processes
- CIOs, CISOs, and other executives who can track trends and monitor improvement in their organization's security posture

Chapter 2

What Can IIAM Do for You?

In This Chapter

- Looking into adding identity and analytics intelligence
- Turning complex data into actionable information
- Understanding trouble spots and areas of high risk
- Collaborating with peers and different roles
- Investigating individuals, groups, and situations that are high risk

This chapter explains what Intelligent Identity and Access Management (IIAM) can do for you or your organization.

You understand the benefits of adding identity and analytics intelligence and discover how an IIAM solution can turn complex data into actionable information and find trouble spots, as well as high risk areas. Finally, this chapter teaches you how IIAM can compare across roles and with peers, as well as investigate high risk individuals, groups, and situations.

Adding Identity and Analytics Intelligence

By connecting with an organization's applications and collecting information, IIAM solutions continuously monitor information about identities and collect data related to resources (including applications, databases, and files), access rights, access policies, and user activities such as creating accounts and logging on to applications.

This information, which may amount to gigabytes or terabytes of data, is organized in a data warehouse, as seen in Figure 2-1. Identity and Access Intelligence (IAI) is applied and analyzes the identity and access data using advanced analytic tools to perform data mining, statistical analysis, data visualization, and predictive analytics.

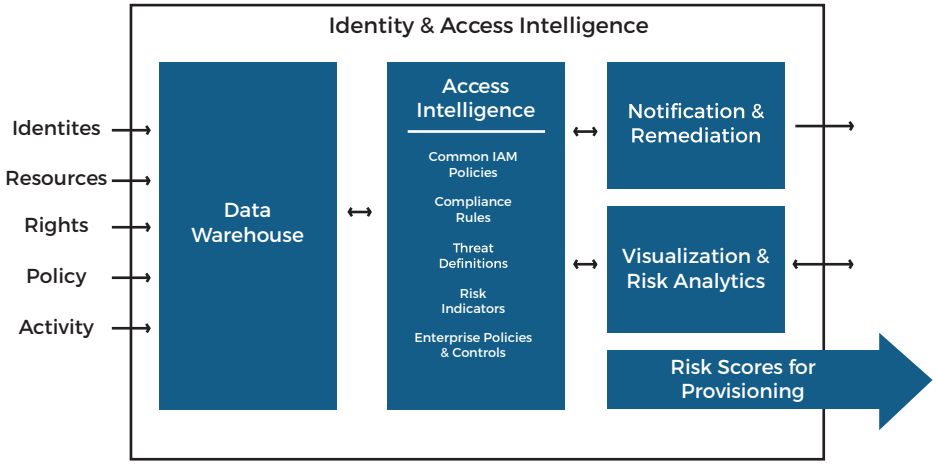

Figure 2-1: Data dissemination capabilities when using IIAM.

These data analysis tools aren't generic. They draw on IAM specific policies, rules, and risk indicators to provide information of immediate value to IAM administrators, analysts, compliance officers, and incident responders.

An Intelligent IAM solution provides the following:

- Reports and graphics showing IAM activities and risk factors
- Notifications and alerts about policy violations and suspicious events
- "Micro certifications" triggered by questionable activities and events
- Automatic remediation, such as removing entitlements and disabling administrator accounts obtained without approval
- Risk scores that can be shared with provisioning systems and other applications (for example, a score that can be used to determine if special approvals are needed for a provisioning request)
- Ad hoc reports and analyses, created by analysts to explore specific issues and risk

These capabilities allow Intelligent IAM solutions to help organizations overcome the governance gap, the complexity gap, and the context gap — all covered in Chapter 3.

Rapid Response: Turn Complex Data into Actionable Information

An Intelligent IAM solution should not only be able to monitor key data continuously, but also it should provide a flexible range of options for rapid response and remediation. In most cases, the appropriate option is a notification or alert to a staff member who can investigate and determine whether or not the alert represents an issue that requires follow up. This type of alert is shown in Figure 2-2.

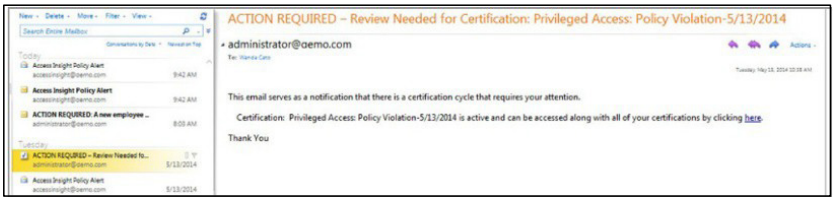

Figure 2-2: Example of an email alert.

In other cases, a specific action should be triggered, such as a micro certification, or even automatic remediation. In all cases, the solution should not only provide notification of a possible violation or issue, but also it should provide related data, and if possible recommended actions to make it easier to address the situation. The solution can also improve security analysis and risk management.

Finding Trouble Spots and High Risk Areas

An Intelligent IAM solution can pinpoint trouble spots, weak points, and quickly answer key questions such as the following:

- Which accounts have the most privileged entitlements and haven't reset a password in hundreds of days?
- Which individuals have the highest number of access rights when compared to peers?
- Which business units have the most orphan accounts?

An Intelligent IAM solution can provide answers to questions in seconds, helping security and IAM analysts to:

- Quickly detect potential indicators of attacks and security breaches (for example, a user account receives privileged access directly to a target application)
- Focus their efforts on high risk situations (for example, accounts with many privileged entitlements that haven't reset their passwords in over 90 days — check out Figure 2-3)

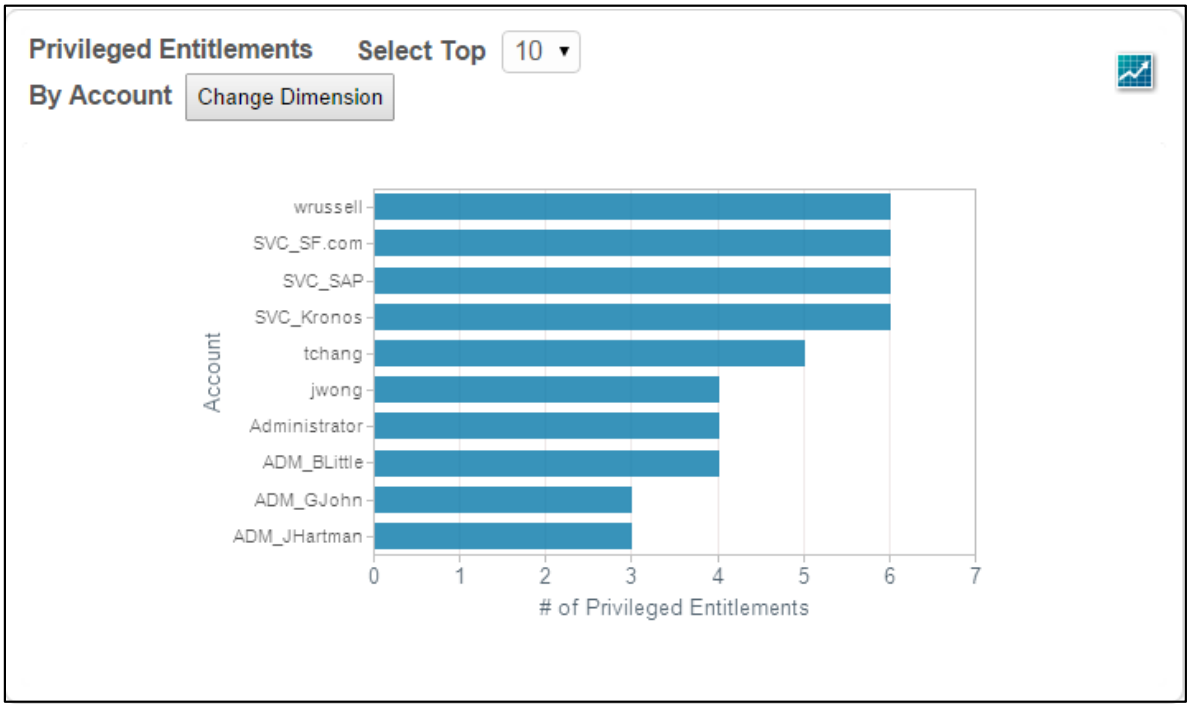

Figure 2-3: An example of privileged entitlements.

Comparisons across Roles and with Peers

An IIAM solution can correlate data to compare users with others in the same role, or with any individual in the organization who might provide a useful benchmark. Analysts, business managers, and resource owners can answer questions like "Does John Smith have more access rights than other financial analysts?" and "How do the access rights available to John Smith compare with those of Jane Jones and William Brown?"

These comparisons are extremely useful for assessing new access requests from individuals, for identifying excessive rights that accumulate when people move through different positions, and for highlighting outliers that may indicate a process problem or a misbehaving user.

Comparisons with peers also have the advantage of giving enterprises a way to identify elevated access (and risk) without the expense of a major initiative to define and manage roles.

Investigating High-Risk Individuals, Groups, and Situations

With an intelligent IAM solution, you can investigate and analyze high risk individuals, groups, and situations, as well as compliance violations. This process makes it easier to answer questions like the following:

- Are there domain administrator accounts whose passwords have never been changed?
- Which non sales systems has this salesperson been accessing?
- Is anybody accessing patient medical information without a genuine "need to know"?
- Which accounts with at least five entitlements haven't been used in more than 30 days?
- Does this account have a suspicious number of privileged entitlements?
- Should part time employees receive all the access rights they are routinely granted?
- Do contractors continue to access resources after their projects end?
- Are system administrators routinely assigned rights they don't need to perform their jobs?
- Does this business unit have an abnormal number of accounts with unnecessary entitlements (that is, access rights that have never been used)?

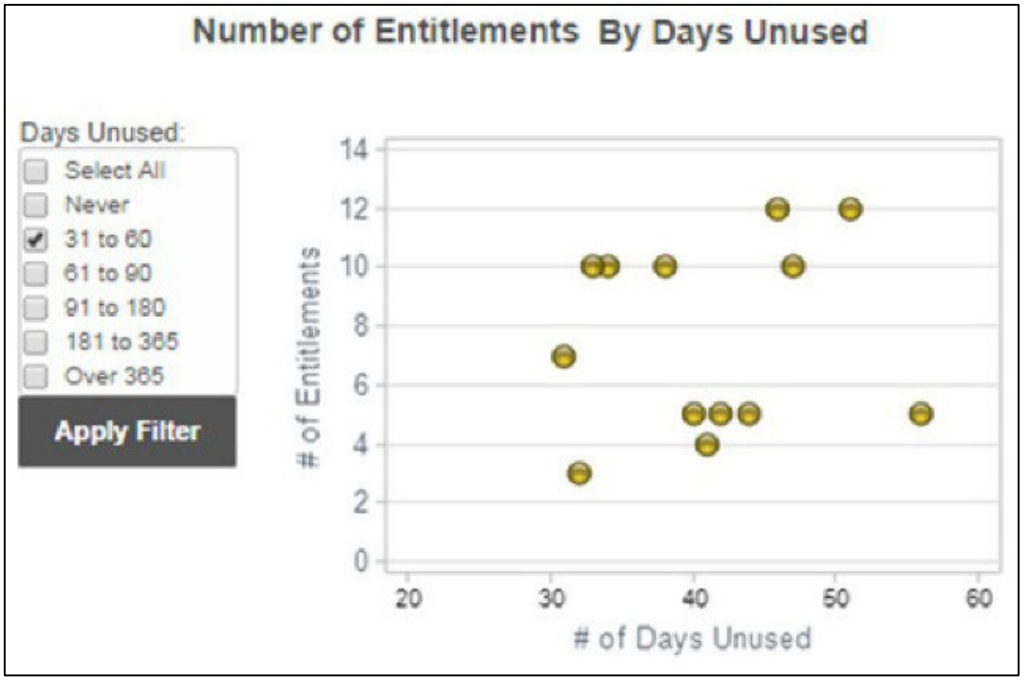

Figure 2-4: Number of entitled accounts 31-60 days unused.

Chapter 3

Analyzing Account Relationships

In This Chapter

- Identifying risks and areas for improvement
- Examining provisioning and governance
- Preventing policy violations
- Getting better information for reviews and audits

Context is everything. Analysts need the ability to drill down into the relationships between users, accounts, groups, entitlements, roles, and applications. With interactive analysis tools like the Access Explorer application, part of the Courion Access Assurance Suite, an Intelligent Identity and Access Management (IIAM) solution makes it easy to identify connections that would otherwise remain obscure and difficult to deduce.

In this chapter, you discover how to analyze account relationships. You see how IIAM works to assess risk and identify high priority targets for improvement. This chapter also illustrates how IIAM works for the continuous improvement of provisioning and governance. Finally, this chapter explains how IIAM helps prevent policy violations at the point of origin, as well as provide better information for management reviews and audits.

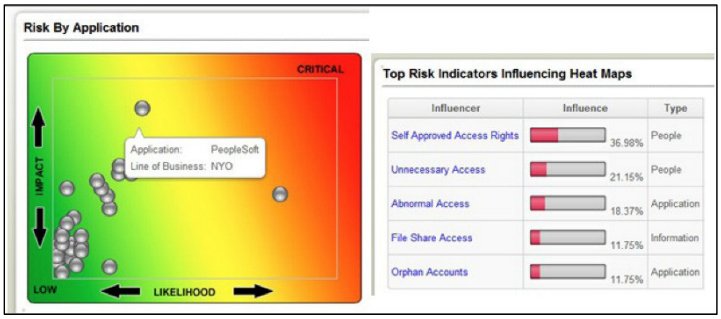

Figure 3-1: A typical heat map.

Continuous Improvement of Provisioning and Governance

Most users of Intelligent IAM solutions focus on the immediate benefits provided by continuous monitoring, rapid response to immediate threats, and tools to analyze risks, patterns, and trends. But organizations shouldn't overlook the importance of strengthening their investment in existing IAM systems.

Intelligent IAM can support the continuous improvement of account provisioning, governance, and other IAM processes.

Reducing over-provisioning and under-provisioning

Over provisioning and under provisioning are occupational hazards for everyone who defines and manages roles. Over provisioning creates security vulnerabilities by granting unnecessary entitlements to a role. Often this comes about when a single individual with unique needs requests new privileges that are then assigned to the role rather than the individual, and the privileges are mistakenly given to everyone in that role.

Under provisioning occurs when an entitlement that's genuinely needed for a role isn't assigned, forcing all or most people in the role to request that entitlement on an exception basis. This is a drag on the productivity of the employees and of the managers and resource owners who must repetitively review and approve their ad-hoc requests.

Intelligent IAM helps people who define and manage roles reduce over provisioning and under provisioning. With a few clicks, they can determine the following:

- Which entitlements are rarely or never used by current members of a role, so those entitlements can be removed from the role
- Which entitlements are frequently or always requested by members in a role, so those entitlements can be added to the role
- Which individuals have excessive entitlements compared with others in the role, so the behavior of those individuals can be examined and the individuals can be assigned to more appropriate roles

Activity related information, such as last login and last trans- actions executed, also provides insight into whether rights are really needed. For example, if a resource hasn't been accessed for three months, there's a strong chance it's not required for that individual or others in the same role.

Continuous monitoring closes the governance gap

Organizations have blind spots when it comes to violations of security and privacy rules. Account provisioning systems provide users with appropriate access to corporate resources when they join a company or change roles. However, changes and exceptions to rules and roles over time introduce excessive rights for individuals, leading to policy violations and access related vulnerabilities. In many organizations, access permissions are granted outside of approved provisioning processes. An example would be when application or database administrators grant access rights based on direct requests from a user.

Organizations should run periodic certifications asking man- agers to verify that existing access rights for their subordi- nates are necessary and appropriate. Unfortunately, busy managers often treat these as "rubber stamp" exercises. They don't take the time to review each entitlement and consider its implications. In many cases, they lack the knowledge and tools to identify policy violations.

An Intelligent IAM solution can address these problems by providing not only the prevention on the front end but also continuous monitoring of identity and access related data and events throughout the life of the user. Violations can be iden- tified as soon as they occur (see Figure 3-2). Changes made outside approved provisioning processes can be flagged and reviewed. Data can be correlated to pinpoint Segregation of Duties (SoD) violations and other complex policy violations before they can be exploited.

An example of typical SOD violations

Access certification processes and other governance tools are helpful but typically leave problems undetected for months. They aren't comprehensive and holistic enough to ensure that least privileged access to corporate resources is granted consistently and aren't reliable enough to provide accurate data for audits.

An Intelligent IAM solution can address these problems by providing not only the prevention on the front end but also continuous monitoring of identity and access related data and events throughout the life of the user. Violations can be iden- tified as soon as they occur (see Figure 3-2). Changes made outside approved provisioning processes can be flagged and reviewed. Data can be correlated to pinpoint Segregation of Duties (SoD) violations and other complex policy violations before they can be exploited.

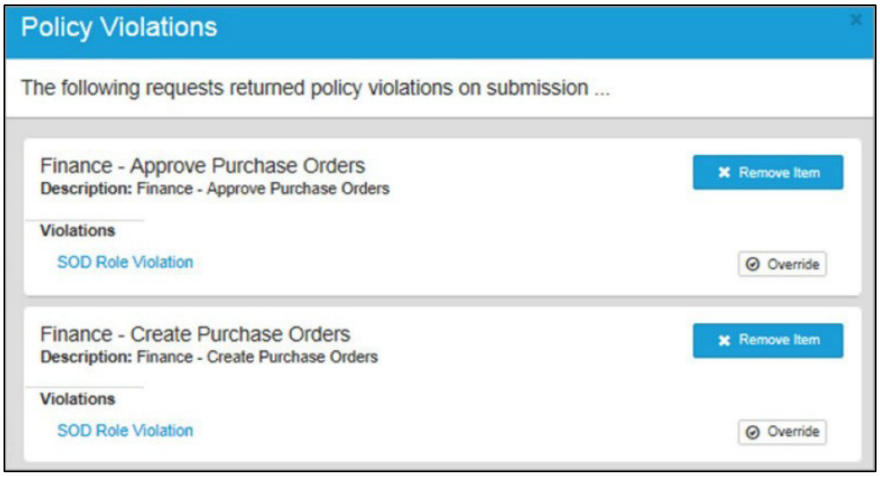

Figure 3-2: Violations shown for review.

These errors and policy violations accumulate over time. Account provisioning systems provide users with appropriate access to resources when they join an organization or change roles. However, continual changes to access rights and exceptions resulting from complex business needs inevitably introduce errors and policy violations. These make the organization more vulnerable to risks such as unnecessary entitlements and privileged access outside of roles.

To some extent, these can be corrected through access certification processes and other identity and access governance procedures. However, these procedures are conducted only semi annually or quarterly. Even then, busy managers often treat major access certification reviews as "rubber stamp" exercises and unintentionally approve inappropriate access rights that can put enterprise data at risk. These problems create a "governance gap" that increases over time, resulting in increased risk to the organization and in audit issues.

This issue isn't just theoretical; evidence shows that the slow detection of security gaps is a serious problem. According to the 2015 Verizon Data Breach Investigations Report (shown in Figure 3-3), 60 percent of attacks were able to compromise networks within minutes, yet more than 80 percent took days, weeks, or months to discover. A 2014 Mandiant study showed that attackers were present on victim networks an average of 229 days before they were discovered.

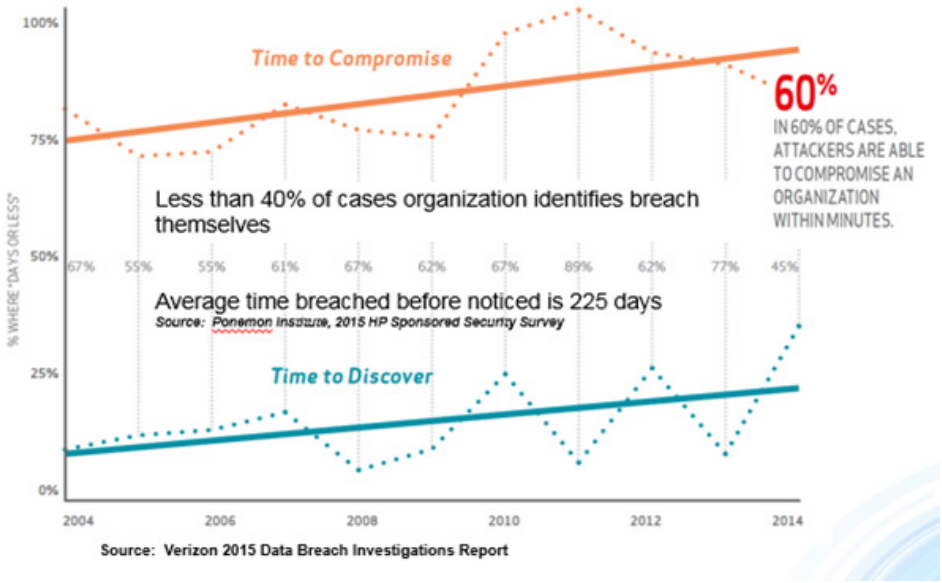

Figure 3-3: Verizon's Data Breach Investigation's Report.

The complexity gap: Information hidden by too much data

Critical information is hidden by complexity. Even a medium sized organization may have tens of thousands of user accounts and entitlements that create terabytes of data related to user identities and accounts, access rights, policies, and user actions. The proliferation of access points to networks through tablets, cell phones, and other devices exacerbates this problem. Traditional IAM systems lack the tools and architecture to pull together and process all this data in a timely manner. As a result, vulnerabilities are difficult to detect in even the most mature IAM implementations.

Although enterprises capture large amounts of identity and access data, they lack the tools to provide context and make meaningful comparisons.

Are privileged users abusing their status? Do a few individuals have far more entitlements than their peers in the same department? Are contractors being given access rights they don't really need? Do certain business units have an abnormal number of policy violations?

With the basic reporting tools provided by conventional IAM systems, it isn't feasible to answer these questions. The system can't enumerate all the different combinations of relationships between identities, access rights, resources, business policies, and governing regulations. That makes it hard — if not impossible — to extract relevant information from the massive volume of IAM data created by the typical enterprise today, and to draw meaningful conclusions quickly enough to protect the business.

Preventing Policy Violations at the Point of Origin

Even with an advanced account provisioning system, managers and resource owners find it very difficult to identify SoD and other policy violations.

An Intelligent IAM solution can be integrated with a provisioning system to flag potential policy violations at the time an access request is being reviewed. It can also give the reviewing manager or resource owner tools to drill down and look at the recipient's current entitlements and those of his or her peers, to determine if the request is necessary and appropriate. It's far less work to prevent a policy violation at the point of origin than to find it during a large scale certification (or through a security breach).

In the near future, Intelligent IAM solutions may be able to improve provisioning decisions by supplying recommendations based on real time risk scoring. This would allow decisions to be made based on the risk profile of the enterprise, users, and applications at the time of provisioning.

One example of such "intelligent provisioning" would be to set up three workflows so that

- Low risk access requests (as determined by the organization in the IAM solution) are granted automatically without requiring the attention of a manager.
- Medium risk requests are sent by the provisioning system to a manager for approval.
- High risk requests require approval by a manager and escalation to a higher level executive for final approval.

Providing Better Information for Management Reviews and Audits

A great deal of time and effort can be saved during management reviews and audits by using an Intelligent IAM solution to provide reports, including filtering and drill down capabilities, trend information, and data visualization tools. These not only give managers a high level view of progress toward goals (such as eliminating orphaned accounts and policy violations), but also they can show auditors that efforts have been made to address high risk issues, such as monitoring access to the most sensitive data stores and controlling the entitle- ments given to privileged users.

Chapter 4

Ten Things to Look for in an IIAM System

In This Chapter

- Recognizing key features of an IIAM system
- Understanding what to look for when selecting IIAM solutions

Selecting an Intelligent Identity and Access Management (IIAM) system can be a challenge. Capabilities and features vary across the market, and selecting the right tool is important. True continuous monitoring can make a big differ- ence to your organization's capability to both manage your environment and to identify and avoid threats that would oth- erwise exist in your identity infrastructure. Here are ten (okay, nine) features to consider when choosing a solution:

- **Risk analytics:** An IIAM system's strength lies in its capability to show you what risks your organization is facing. You should look for a system that can apply big data analysis techniques to help find the problems you're most worried about before they cause real issues. In short, an IIAM system should tell you what's risky, even if you didn't know it was a concern.
- **Intelligent provisioning:** Linking an IIAM system to your provisioning system should allow you to score the risks that an access request creates and create workflows based on how much scrutiny an access request needs.
- **Alerting capabilities:** Your IIAM system is only as effec- tive as its capability to tell you when something is wrong. Look for an IIAM system that can alert you in ways that fit your business process and preferences.
- **Privileged account monitoring:** Privileged accounts, such as those that belong to system administrators, need to be watched closely for both abuse and for inadvertent growth in rights and privileges. A good IIAM system helps you focus your attention on the most critical accounts when they need it.
- **Strong visualization capabilities:** The complex interac- tions between user accounts and their rights can make finding problems a tedious process of reading error logs and configuration information line by line. Strong visualization capabilities make finding problems and detecting anomalies something you can do at a glance.
- **Continuous governance:** The gap between when users are given rights and when those rights are audited is the time that organizations face the most risk. Micro certification can help by providing immediate review as needed by managers, which ensures that they see and address problems directly.

- **Access rights monitoring:** Polls show that excessive developer access rights are a concern for many organizations. Tracking what access individuals have compared to what they really need is a key feature for any IIAM system.
- **Support for role changes:** When a user's role changes, her rights need to change, too. A good IIAM system should handle when a user's role changes, or if she's terminated, by ensuring that the appropriate rights are removed for that user.
- **Identification of Segregation of Duty issues:** Separating the rights that are required to perform sensitive actions is important, and accounts that end up with too many rights may be able to bypass that. Automated detection is important to prove to yourself and auditors that your separation of duties works.

With an IIAM solution, you give your organization the opportunity to make educated decisions based on real time information. By using continuously collected information, you can monitor and analyze large groups of data to better understand who's accessing your system, what they're using, and how it impacts the organization. Not only does an IIAM system work with provisioning and governance solutions, but also it gives you real time risk analytics and the ability to make sure that only the right people are accessing the right information at the right times.