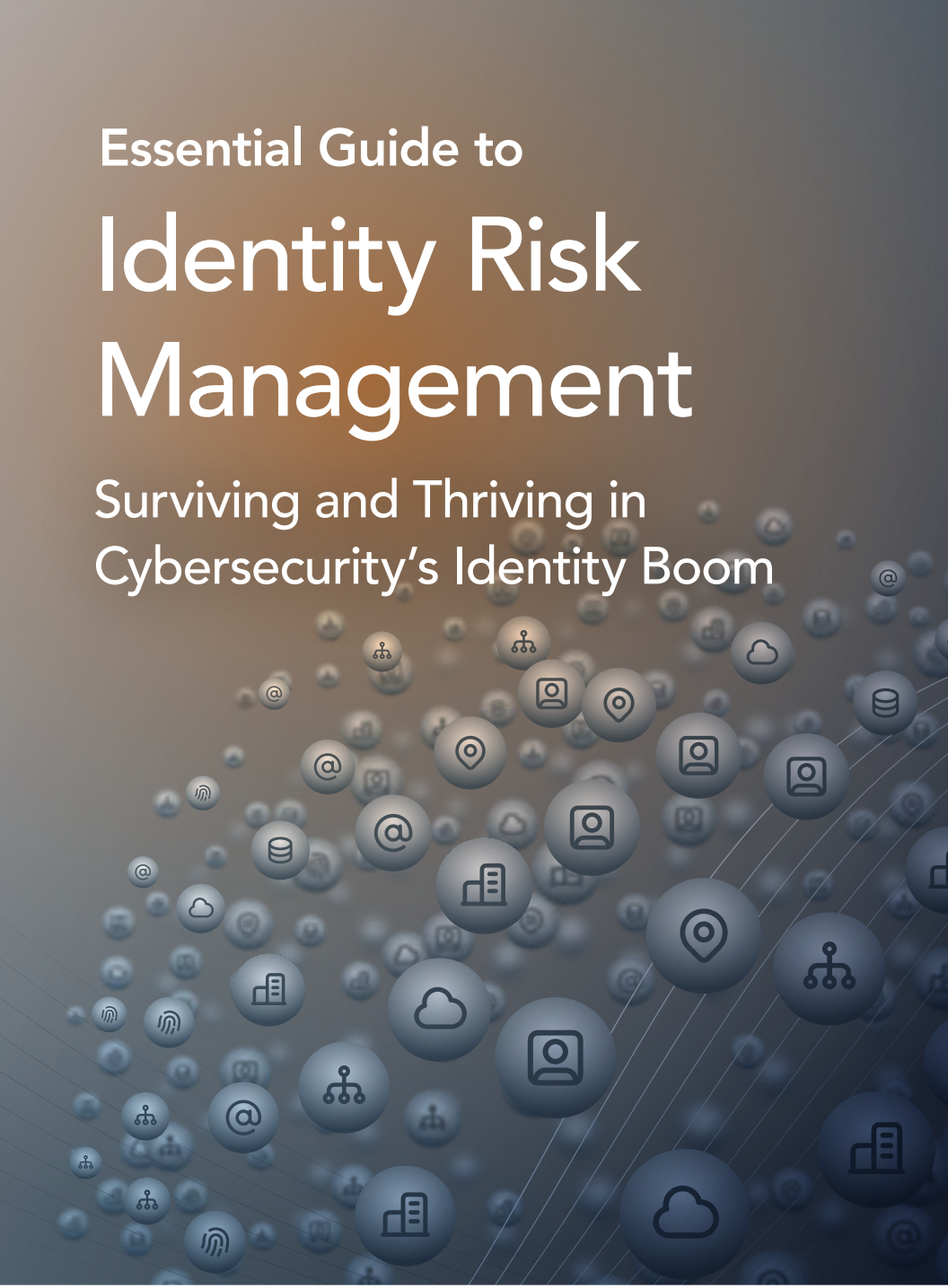
Essential Guide to

Identity Risk Management

Surviving and Thriving in Cybersecurity's Identity Boom



Michael Thelander and Jon Friedman
Foreword by David Canellos, CEO of Axiad

About Axiad

Axiad is an identity security company tackling the growing threat of compromised credentials, which drive over 70% of enterprise breaches. The sprawl of human and non-human identities across organization silos creates security blind spots that existing tools fail to secure. Axiad tackles this problem head-on, detecting identity risks and poor credential hygiene across systems, providing actionable insights, and enhancing security without needing a complete overhaul. Axiad makes identity simple, effective, and real. Discover more at axiad.com or follow us on LinkedIn.

Essential Guide

to

Identity Risk Management

Surviving and Thriving in
Cybersecurity's Identity Boom

Michael Thelander
and Jon Friedman

Foreword by David Canellos, CEO of Axiad

CYBEREDGE
PRESS℠

Essential Guide to Identity Risk Management

Published by:
CyberEdge Group, LLC
501 E. Las Olas Boulevard
Suite 300
Fort Lauderdale, FL 33301
(800) 327-8711
www.cyberedgegroup.com

For general information on CyberEdge Group research and marketing consulting services, or to create a custom book and eBook for your organization, contact our sales department at 800-327-8711 or info@cyberedgegroup.com.

ISBN: 978-1-948939-43-0 (Paperback)
ISBN: 978-1-948939-44-7 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Copy Editor: Susan Shuttleworth
Graphic Design: Colleen R. Abel
Additional Artwork: Yoshi Takebuchi

Table of Contents

Foreword

I've spent over 20 years in cybersecurity, with a career that's spanned some of the most transformative advancements in our industry, from the evolution of privileged access management to secure web access and zero trust networking. I've been both a witness and a contributor to some of our most evolutionary leaps. But one area has been notably slow to evolve, despite its critical role: identity.

Identity is the core of cybersecurity. Our increasingly interconnected, increasingly digital world drives organizations to ceaselessly expand the number and type of identities they deploy. Cloud services, containerization, remote work, and mobile technologies have stressed traditional models of identity and access management (IAM) and shown their shortcomings. The growing complexity of enterprise environments continues to create new security and risk challenges. Mergers and acquisitions compound this complexity.

Identity-related breaches are now the leading causes of cyberattacks. In 2023, compromised identities were behind more than 70% of incidents, with attackers exploiting weak credentials, misconfigurations, or poorly managed access controls. Despite significant investments in IAM solutions, organizations continue to face critical gaps in their ability to prevent, detect, and respond to these risks. The attack surface grows exponentially, and organizations struggle to keep pace.

Current IAM systems were simply not designed to address these emerging risks. A more comprehensive, layered approach to identity security is necessary to bind risk analysis, continuous monitoring, and rapid response capabilities into a dynamic "mesh." Importantly, this approach shouldn't require a rip-and-replace of existing IAM systems. Neither should it call for layering on yet another "platform." (These are the very actions that have created new identity silos, increased complexity, and raised costs.) Instead, it must leverage this

modern mesh architecture to extend the value of existing IAM investments and continually reduce risk.

This guide introduces the basic concepts of identity risk management (IdRM) and explains how it meets the challenges described above. IdRM is not just about preventing unauthorized access; it's also about identifying and mitigating identity-related risks that emerge from the sheer scale of users, devices, and applications within every enterprise, large or small. As organizations adopt new technologies, expand their digital footprint, and modernize their IT infrastructure, their attack surface only grows. Founded on emerging identity fabric principles, IdRM pulls together information from all the disparate applications and systems where human and non-human identities can reside (or hide) and provides a 360-degree profile of both individual and organizational identity risks.

IdRM provides a proactive and pragmatic approach to security by offering visibility into identity risks before they escalate into major security incidents. It allows organizations to identify weak points, manage risks effectively, and apply risk based policies to better protect their sensitive assets and data. This is more than just adding features to traditional IAM: it's an adaptive, dynamic, and holistic view of identity security that responds to an ever-evolving threat landscape.

In the last 20 years I've never been personally involved in a disruption as large and as positive as the one Identity Risk Management (IdRM) promises to be.

In this guide, we'll explore the fundamentals of IdRM, describe the risks organizations face, and recommend techniques to mitigate them. You'll learn how a proactive, risk-based strategy can not only protect identities but also strengthen your organization's overall security posture. Embracing IdRM will help you defend against identity-related threats and prepare for the future of cybersecurity…whatever shape it takes.

David Canellos
CEO
Axiad

Introduction

Today, countless identities are continually dispersed across an enormous variety of systems and platforms. We sometimes refer to this as "the identity boom."

This book outlines how the current identity boom has been shaped by modern computing trends; provides guidance on how to corral fragmented identities; describes how identity information can be discovered, correlated, analyzed, and quantified; and offers a roadmap to using identity informatio to contain attacks, assess risks, and reduce the fastest-growing attack surface: our enterprise identity ecosystem.

Chapters at a Glance

Chapter 1, "The Identity Attack Surface and Identity Risk Management (IdRM)," discusses why identity security is so challenging and outlines the basics of identity risk management.

Chapter 2, "A Short Overview of the IdRM Process," lays out the phases of an IdRM process and suggests why IdRM is a step toward creating an identity fabric.

Chapter 3, "Where IdRM Fits in the IAM Landscape," explains how IdRM solutions strengthen AM, PAM, CIEM, IGA, and other IAM functions.

Chapter 4, "Who Should Care About IdRM?" explores how security professionals at all levels can employ IdRM solutions to improve their day-to-day outcomes.

Chapter 5, "Identifying Your Identity Risks," discusses how IdRM solutions discover, ingest, and analyze identity data and how analysts can use this information.

Chapter 6, "Quantifying Your Risks," reviews how risk scores for individuals and groups can be calculated, visualized, and employed to reduce risk.

Chapter 7, "Fortifying Your Identities Against Risk," highlights how IdRM helps organizations improve and automate remediation and attack surface hardening.

Chapter 8, "Selecting the Right IdRM Solution," provides a checklist of criteria for selecting an IdRM solution that meets the requirements of your organization.

Helpful Icons

Tips provide practical advice that you can apply in your own organization.

When you see this icon, take note as the related content contains key information that you won't want to forget.

Proceed with caution because if you don't it may prove costly to you and your organization.

Content associated with this icon is more technical in nature and is intended for IT practitioners.

Want to learn more? Follow the corresponding URL to discover additional content available on the Web.

Chapter 1

The Identity Attack Surface and Identity Risk Management (IdRM)

In this chapter

- Review why the identity attack surface is *the* pivotal battleground for threat actors and security teams today
- Examine four reasons why identity security is so challenging
- Understand the basics of identity risk management

"I am large, I contain multitudes."

— Walt Whitman

Identity: Today's Pivotal Attack Surface

"Attack surface" is a fundamental concept of security. Among the most critical jobs of any cybersecurity group are understanding, reducing, and monitoring its organization's attack surfaces.

Until recently, cybersecurity experts described an organization's attack surfaces as a combination of physical devices (such as workstations, smartphones and servers) and digital entities (such as applications and websites).

Now these experts include identities as another attack surface. In fact, many leading industry analysts view identities as the most important attack surface. We frequently hear the phrase *"identity is the new perimeter"* and calls for *"identity-first security "*

Why? Because threat actors have found that they can easily steal or buy identity-related information, including valid access credentials, and then swiftly use these "keys to the kingdom" to penetrate networks and access applications and data. From there they can move laterally within an organization's computing infrastructure and exfiltrate data.

The proof? Statistics show that identities and identity-related information are key tools in most major cyberattacks today and the most common targets of attacks. They are also the biggest headaches for security operations center (SOC) and user support teams. For example:

- ☑ Verizon's widely read 2024 Data Breach Investigations Report (DIBR) found that **80% of web application attacks used stolen credentials.**
- ☑ The Identity Defined Security Alliance's *2023 Trends in Security Digital Identities* report showed that **91% of organizations experienced one or more identity-related breaches in the last year, and 45% of organizations experienced a negative reputational impact from an identity incident.**
- ☑ Of the 14 tactical areas described in MITRE's ATT&CK framework, five (initial access, persistence, privilege escalation, credential access, and lateral movement) include **multiple techniques for compromising and exploiting identities.**

Definitions: attack surface and identity

Attack surface: "The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment." *NIST SP 800-53, Rev. 5*

Identity (general use): "the condition of being oneself…and not another." *Dictionary.com*

Digital identity (in IT): a unique digital representation of **a person or thing** (an entity) who is authorized to access and use information resources, together with the **attributes, accounts, entitlements, credentials,** and **secrets** associated with that identity. *Axiad*

Four Reasons Why It's So Hard to Protect Identities

Of course, cybersecurity teams already expend a tremendous amount of effort managing and protecting identities. Why are they failing to prevent threat actors from acquiring and using identity-related information? Four reasons stand out.

Identity information is scattered everywhere

Identity information includes user identities and their attributes, accounts, entitlements, credentials, and secrets like keys and tokens used for validation and encryption. In a typical enterprise, these items are scattered across:

- ☑ Directories and identity management systems
- ☑ Password and secrets managers
- ☑ Workstations, servers, and other devices
- ☑ On-premises applications
- ☑ Cloud platforms
- ☑ "Shadow IT" cloud applications and services (unauthorized by, and often unknown to, security teams)

To save time and mental effort, humans often reuse passwords. In June of 2024 the largest trove of passwords ever leaked – 9.9 billion passwords in plain text! – was made public via a list called RockYou2024. We can be sure that many of these passwords are being used in scripted, automated credential stuffin attacks to compromise personal and business accounts.

In addition, credentials and secrets are often hard coded in software and exposed in memory on workstations and servers.

In recent years, digital identities have been scattered across many divergent systems serving different purposes, both on premises and in the cloud. Because so many identities are poorly tracked, most organizations have no way to assemble a

complete picture of the identity information for any person or machine. ("Machine identities" are discussed below.) In fact, security teams often find that most users have multiple ident - ties spread across different networks, applications, services and systems, which can't be correlated or linked.

Silos disrupt prevention and remediation

IT and security teams devote much time and effort to findin and remediating vulnerabilities, misconfigurations, and issues that expose identity information to outside threat actors and malicious (or just careless) internal users. Unfortunately, they perform most of these activities in silos, such as identity management systems, cloud operations systems, endpoint management tools, software development environments, and operational and IoT systems.

Because of this compartmentalization:

1. It is difficult or impossible to share information tha would allow organizations to detect identity-specific risks and assess policy violations.
2. Identity-related vulnerabilities, misconfigurations, and issues are only prioritized within their respective silos.

This second point is much more serious than most people realize. Even when individual groups can rank remediation tasks within their own silo, there is no way to prioritize globally. Teams waste time and effort on tasks that are seemingly urgen but are actually a low priority for the enterprise as a whole.

Advanced technologies have increased complexity

Cloud applications – both internally developed software running on public cloud platforms and cloud-hosted SaaS applications – have their own directories and services for man- aging identity information and access. They also bring into the picture their own management and administration accounts that, if accessed through compromised credentials, could give threat actors the means to bring business operations to a halt.

With the broad use of cloud applications, organizations now face the critical task of protecting a large new set of identities and systems with tools designed for legacy applications running on premises.

In addition to presenting a raft of new cloud identity protection requirements, advancing technologies are creating new complexities that make it harder to protect identities and credentials related to:

- ☑ Mobile workers, digital nomads, and work-from-home users
- ☑ Contractors and virtual teams using collaborative applications that manage text, documents, and audio and video file
- ☑ Business partners and supply chain vendors whose personnel and products need access to an organization's information assets
- ☑ Online software repositories

Business activities like mergers and acquisitions and expansion into new markets also create challenges related to merging or extending identity management processes.

Machine (non-human) identities change the game

Machine or non-human identities (NHIs) are a special case of advancing technologies that increase identity management challenges.

There are two types of machine identities. The first ype is for **software entities** such as workloads, service accounts, APIs, AI entities, automation tools, and robotic process automation (RPA) services. The second type is for **physical devices,** including workstations, servers, personal devices, internet of things (IoT) devices, and industrial systems. Both need identity lifecycles, including entitlements and credentials, so they can appropriately access and interact with other information resources.

Machine identities dramatically increase the complexity of identity management and security because:

1. The number of identities to be managed and protected has soared, driven by the phenomenal growth in IoT devices and cloud-hosted software workloads. Published estimates of the ratio of machine to human identities range between 10:1 and 50:1.
2. NHIs involve types of attributes, accounts, entitlements, and credentials that differ in essential ways from those associated with human users (e.g., humans rarely have "owners," serial numbers, software parent processes, or OAuth tokens).
3. Most identity management and identity security products are designed only to handle human users.

Introducing Identity Risk Management (IdRM)

Given that identities are so pivotal for cybersecurity, yet are becoming harder and harder to protect, is there a way to dramatically improve identity security without incurring high costs or disrupting existing identity management products and processes?

There is a way, and it's called identity risk management (IdRM).

IdRM is a synthesis of technology and process that enables security and identity management teams to collaborate and to quickly and accurately:

1. **Identify identity-related risks** across the entire enterprise
2. **Quantify these risks** and set priorities for their remediation
3. **Fortify identities** against current and future risks

Easy, but not simple

While these steps sound easy, they take a lot of work. For example:

- ☑ Identifying identity risks involves creating a complete picture of identity information for every human and machine user by discovering and collecting information from many sources about their identities, accounts, entitlements, and credentials.
- ☑ Quantifying risks and setting priorities entail correlating identities (including multiple identities for the same user) and assessing risk factors and the potential impact (blast radius) for each instance.
- ☑ Fortifying identities against risk requires a knowledge base to recommend remediation actions for each risk and integrations to automate the process of delegating the actions to the appropriate people or processes.

Fortunately, IdRM makes it possible to accomplish most of this work using computers, without involving people except a few in supervisory roles.

The what, why, and how of IdRM are described in the following chapters of this guide. We discuss the IdRM process, explain where IdRM fits within the broader domain of identity and access management (IAM), review who benefits from it, and cover related topics.

What we mean by identity risks

For the purposes of IdRM, identity risks are situations that either expose identity information to theft or manipulation or that violate policies or best practices for creating, using, managing, and protecting user identities, accounts, entitlements, credentials, and secrets. Examples include:

- Identity information residing in unmanaged and insecure locations
- Accounts that have never been used, are orphaned (no longer associated with an active user), or are dormant
- Accounts that are overprovisioned (have entitlements for actions not needed for the user's legitimate activities)
- Identities and identity information not covered by appropriate controls; e.g., encryption or multifactor authentication (MFA)
- Identities that have not been updated or refreshed.
- Anomalous behaviors related to access requests or administrative actions, such as creating accounts or upgrading entitlements

IdRM solutions communicate these risks across the identity ecosystem.

Identity Hygiene Plus Identity Security Posture Management

IdRM primarily provides powerful capabilities for two major identity management domains: identity hygiene and identity security posture management (ISPM). Secondarily, it supports a third domain, identity threat detection and response (ITDR).

Identity hygiene

Identity hygiene is concerned with creating and managing identities in ways that enforce policies and minimize risk; for example, by remediating orphan and overprovisioned accounts and detecting and eliminating exposed credentials. IdRM helps organizations dramatically improve identity hygiene by collecting, correlating, and assessing security information across silos and computing environments and better prioritizing remediation activities.

Security posture management

IdRM helps security teams obtain complete visibility into identity risks across the enterprise, identify areas with the highest risk, prioritize identity initiatives and investments, and track progress over time.

ITDR

Once attacks are detected by ITDR tools, IdRM solutions can help incident responders contain them by determining the blast area of compromised identities and identifying similar identities that might be affected.

Who needs IdRM?

Identity management and security practitioners who aim to strengthen identity hygiene and prioritize remediation activities

Identity security and GRC leaders who must identify, isolate, and prioritize identity risks across the enterprise

CIOs and CISOs who want to improve the organization's security posture and protect its intellectual property and brand

Chapter 2

A Short Overview of the IdRM Process

In this chapter

- Learn about the phases and main activities of an IdRM process
- Consider why an IdRM solution might be the best next step toward creating an identity fabric

"What we know matters... but who we are matters more."

— Brené Brown

What does it really mean to say that IdRM is a technology for identifying identity risks, quantifying these risks, and fortifying identities against risk? This chapter provides a high-level view of the activities involved, and they are discussed in more detail in chapters 5 through 7.

Identifying Identity Risks

Discover and ingest identity information

The first job of an IdRM solution is to discover and ingest identity information from across the enterprise. This process requires integration with a wide variety of systems where user identities and identity information are created, stored, and managed. They include:

- ☑ Enterprise and cloud-based directories and identity management systems
- ☑ On-premises and SaaS applications
- ☑ Machine identity management products
- ☑ Certificate management platform

IdRM solutions can also discover, ingest, and analyze identity information from places where it shouldn't be, such as:

- ☑ Unauthorized online shadow IT services
- ☑ Identity dump sites and hacker marketplaces on the Dark Web

To discover and ingest identity information, IdRM solutions can work with industry frameworks and standards such as the Open Cybersecurity Schema Framework (OCSF), the Risk Identification and Site Criticality Toolkit (RISC), and the Continuous Access Evaluation Protocol (CAEP). There are also newly emerging standards like the Interoperability Profile for Secure Identity in the Enterprise (IPSIE).

Their ability to ingest a full range of identity information from diverse sources allows IdRM solutions to overcome one of the biggest challenges in identity management – providing visibility and analysis across the usual silos of identity management and security.

IdRM solutions are not designed to centralize the storage and administration of all identity information. That would require duplicating massive quantities of data and hundreds of complex workflows. Instead, IdRM tools integrate with existing identity management tools to provide global visibility and risk analysis.

Correlate and map the data

IdRM solutions correlate and map the identity data they have ingested by:

- ☑ Finding identities and accounts in multiple systems that may belong to the same user, so they can be correlated and analyzed together
- ☑ Building "identity graphs" that show connections and relationships between identities, groups, roles, entitlements, credentials, secrets, and other entities
- ☑ Giving analysts a global view of all identity information for each person or machine across the enterprise and the ability to drill down into specific

Quantifying Identity Risks

Analyze and assign risk scores

After they have correlated and mapped identity information, IdRM solutions can analyze the data and assign risk scores based on a range of factors related to vulnerabilities and security issues. (Examples of risk factors are discussed in Chapter 6.) Of course, many other tools assess risk in IT environments, but IdRM focuses on identity-specific risks and collects that data from adjacent systems.

Risk scores enable identity security systems and analysts to focus on the highest-risk identities in their domains and prioritize their remediation activities.

Compare groups

Risk scores can also be aggregated by computing environment, business unit, business function, and other groupings, and the results can be compared. This gives identity security teams a global view of identity-related risks, so they can:

- ☑ Pinpoint areas and groups with the highest risk profile
- ☑ Prioritize remediation tasks globally rather than locally
- ☑ Know where to perform risk assessments and root cause analyses that will have the biggest impact on reducing the identity attack surface and improving the organization's identity security posture

Fortifying Identities Against Risk

Initiating remediation

IdRM solutions can initiate remediation actions by alerting identity security teams to vulnerabilities and other security issues. They can speed up remediation processes by providing contextual information, and in some cases, AI-generated recommendations. With the proper controls, they can automatically communicate with security tools to immediately contain attacks and remove vulnerabilities.

In addition, IdRM tools can enrich identity data with context and analysis and can send the enriched data back to the source systems. This closes the loop and makes identity management and security tools more accurate and effective

Planning and tracking improvements

Security teams can utilize risk scores and comparisons to direct identity security resources and investments in ways that will have the biggest impact on reducing overall risk. In addition, they can develop tracking systems and dashboards that quantify changes in risk over time to show progress toward meeting identity security goals.

The Best Next Step Toward an Identity Fabric

Industry analysts and security experts are encouraging organizations to implement an "identity fabric" framework that unites disparate identity services and use cases. IdRM can help organizations achieve many of the goals of an identity fabric. For example, IdRM tools can correlate information from multiple identity management systems, provide global visibility into identity risks, and prioritize remediation based on risk.

In fact, for many organizations considering an identity fabric initiative, implementing an IdRM solution is the best next step and provides early wins in a short timeframe with a modest investment.

Chapter 3

Where IdRM Fits in the IAM Landscape

In this chapter

- Understand how IdRM solutions strengthen AM, PAM, CIEM, IGA, and other IAM functions
- Note how IdRM can support incident responders
- See why other IAM systems can't duplicate IdRM

"Coming together is a beginning, keeping together is progress, and working together is success."

— Henry Ford

Identity and access management comprises a variety of security disciplines, each with its own processes and technologies. This chapter examines where IdRM fits into the IAM domain and how it interacts with different components

IdRM Doesn't Duplicate Existing IAM Processes

IdRM does not duplicate or displace existing components of IAM. Rather, it ingests and analyzes data from many identity-centric sources and IAM systems, enriches the data, and provides tools, reports, and risk scores that can be used by security practitioners and managers across many IAM disciplines. Generally, IdRM solutions have no impact on existing IAM processes or computing infrastructure.

IdRM Supercharges IAM Prevention Activities

Industry analysts divide IAM defenses into "prevention" and "detection and response" layers. Activities in the prevention layer are concerned primarily with identity hygiene and identity security posture management (ISPM). They reduce and harden the identity attack surface prior to specific attacks. Identity threat detection and response (ITDR) activities detect and contain specific attacks as they occur

The primary advantage of IdRM is making existing prevention activities more efficient and effective, although it also cont - utes to ITDR, as illustrated in Figure 3-1.

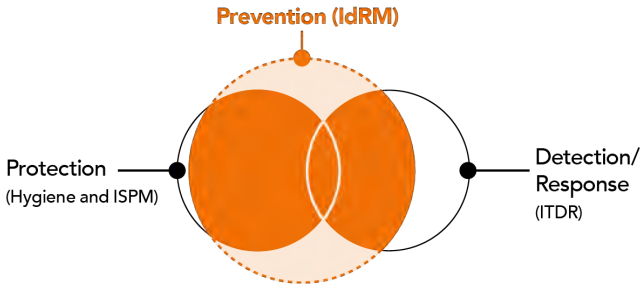


Figure 3-1: IdRM strengthens security solutions that prevent identity-related attacks and enriches many detection and response capabilities.

Reducing the identity attack surface (identity hygiene)

Much IAM effort and investment goes into managing systems that "give the right people the right access at the right time" based on policies and risk. This is the focus of zero trust initiatives and the primary function of technologies such as:

- ☑ Access management (AM)
- ☑ Privileged access management (PAM)
- ☑ Cloud infrastructure entitlement management (CIEM)
- ☑ Identity governance and administration (IGA)

But most organizations have thousands of vulnerabilities, overprivileged and orphaned accounts, and other issues that:

- ☑ Expose identity information and credentials to theft and compromise
- ☑ Allow threat actors who have obtained legitimate credentials to exploit them and move laterally across systems and networks

IdRM solutions give identity management and security teams working in areas like AM, PAM, CIEM, and IGA expanded visibility that crosses silos, as well as new analytic tools. These features help them find and remediate more vulnerabilities and policy violations related to user identities, accounts, entitlements, and credentials.

Hardening the attack surface

IdRM solutions also provide data on what types of identity-related risks are most prevalent and the frequency of each risk type by system, business function, and geographical area. This data enables managers to harden the identity attack surface by targeting resources and controls in areas where they will have the biggest impact on reducing risk.

IdRM Supports Incident Response

IdRM solutions can assist SOC analysts and incident responders in containing attacks and remediating the conditions that allowed them. For example:

- ☑ If a user's passwords have been compromised, IdRM could find other identities and accounts associated with the same user that might be vulnerable.
- ☑ If an attack exploits a particular vulnerability or security issue, an IdRM system can show other places in the organization with the same issue so analysts can investigate whether they have also been attacked.
- ☑ If an IdRM tool detects that a user's privileges have suddenly been escalated, it can alert analysts that an attacker may be manipulating the entitlements of a compromised account.

What Other Tools Can't Do

You might ask: "Don't existing IAM tools have similar capabilities?" Some do, but within silos. Usually they can't:

- ☑ Ingest, normalize, and correlate data from identity sources on multiple data center and cloud platforms and in SaaS applications
- ☑ Provide complete contextual information from across the enterprise to assist with remediation and response
- ☑ Assess risk and create risk scores using a consistent methodology across the enterprise
- ☑ Provide a global picture of an enterprise's identity attack surface and identity risk posture
- ☑ Tell the CISO which identity-related risks are most likely to cause a major data breach

What about frameworks and standards?

Several identity-related frameworks and industry standards, including OCSF, RISC, IPSIE, and CAEP, promote interoperability among IAM systems. IdRM solutions work with them to integrate with a wide variety of IAM tools.

However, none of these frameworks or standards provides a sufficiently comprehensive integration language or is widel enough accepted to collect and normalize identity data from all the major human resources products, IAM solutions, and cloud-native identity management tools.

In practice, security solutions based on these standards tend to generate *yet more* identity-related alerts on top of the ones that already overwhelm SIEM and XDR tools.

In short, IdRM solutions provide unique capabilities for identifying and managing identity-related risks without duplicating existing tools or placing additional burdens on security staff or infrastructure.

Chapter 4

Who Should Care About IdRM?

In this chapter

- Explore how security practitioners can employ IdRM solutions to improve their day-to-day job performance
- Review how IdRM solutions can help identity security leaders, CIOs, and CISOs achieve their goals

"By 2025, identity and access management leaders who foster interdisciplinary fusion teams will gain control of 50% more identity and access management decisions than those who do not."

— Gartner research note: *Improve IAM Architecture by Embracing 10 Identity Fabric Principles,* by Erik Wahlstrom, Mary Ruddy, 6 February 2024. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

As we have mentioned, IdRM solutions enhance and support a wide range of IAM disciplines. But who, exactly, are the people who benefit from IdRM, and how can IdRM solutions help them do their jobs better?

Security Practitioners

When you look carefully, you find that a surprising number of people work with identities and identity-related information on a daily basis. The "interdisciplinary fusion teams" referenced in the quote above are often present, but not always working together yet.

IAM teams

Most people in IAM spend time managing processes for onboarding and provisioning users, granting users enough entitlements to do their jobs but no more, ensuring that privileged users are protected with extra security controls, ascertaining that access control policies are being enforced, monitoring user access to cloud applications and services, and related activities that fall into categories or disciplines like AM, PAM, IGA, and CIEM.

These identity and security managers can use IdRM solutions to identify users with excessive privileges, high-risk accounts (e.g., those that are orphaned or dormant), users associated with two or more identities that could be linked or consolidated, users who are managed inconsistently (e.g., as privileged users for some applications and as ordinary users for others), identity information stored in insecure locations, and violations of identity security policies (like continuing access to privileged IT accounts when employment or a contract has been terminated). While other IAM products also help with some of these tasks within silos, IdRM solutions are unique in their ability to pull together and analyze data from across the enterprise and multiple cloud platforms.

OT, IoT, and DevOps security teams

People responsible for security in areas such as operational technology (OT), industrial control systems (ICS), IoT devices, and development operations (DevOps) often lack tools and processes for systematically managing "machine" identities and implementing rigorous access controls in their domains. IdRM solutions can help them uncover identity-related risks. assess their identity management processes and synchronize those processes with their organization's main IAM or IGA policies and procedures.

Auditors, SOC teams, and others

Members of audit and compliance teams can use IdRM solutions to detect and track violations of security and privacy policies related to access control and identity protection, or to document compliance with those policies. For example, they can help identify accounts where MFA policies are required,

or where they should be required but aren't. They can provide a dynamic snapshot of an enterprise-wide MFA deployment process.

As described in the previous chapter, IdRM technology can provide information to SOC analysts and incident responders that helps them contain attacks and remediate the conditions that allowed them.

Other groups outside of IT may also have a strong interest in how access to information resources is managed. These include software development, DevSecOps, third-party risk management, and fraud prevention teams. IdRM solutions can help them identify identity-related risks in their domains.

Identity Management Leaders

What about chief identity officers, vice presidents and director of IAM, enterprise security or identity architects, and others who lead or direct IAM activities?

IdRM solutions can help these managers:

- ☑ Improve the productivity and effectiveness of their teams
- ☑ Identify and isolate identity risks across on-premises, multi-cloud, and hybrid infrastructures
- ☑ Prioritize remediation and identity risk reduction activities based on global risk comparisons rather than local departmental impacts and preferences
- ☑ Share identity information and promote collaboration among IT security, risk, audit, human resources, and business staff
- ☑ Protect their organization's brand from identity-directed attack vectors such as account takeover (ATO) and phishing attacks
- ☑ Help unify IAM processes and policies for human and machine identities
- ☑ Identify non-compliance (and document compliance) with identity management policies and standards

- ☑ Increase the consistency of IAM processes and identity risk postures across business units, regional organizations, and newly acquired companies
- ☑ Help develop and fine-tune strategies for improving IAM processes and programs, then track implementation progress

CIOs and CISOs

IdRM solutions can help CIOs, CISOs, and other top IT executives:

- ☑ Accelerate cloud transformation by identifying and reducing risks related to protecting identities and managing access control on cloud platforms
- ☑ Mitigate staff shortages by increasing the producti - ity and effectiveness of existing IT security team
- ☑ Prevent many identity-related attacks and more quickly contain others
- ☑ Assess business acquisition and merger targets for identity risk issues and alert due diligence teams
- ☑ Document compliance with identity-related sections of IT frameworks and regulatory standards
- ☑ Facilitate systematic, continuous assessments of the organization's identity security posture
- ☑ Assess, quantify, and report to the CEO and board members on risk levels, security posture, and compliance

IdRM solutions have many potential beneficiaries. nvolve a cross-section of these people in planning and implementing your IdRM program. Think about how to educate them on using IdRM data and tools to address their specific challenges. Go "outside the box" and think about business teams, strategic initiatives, and business partners. And be sure to develop feedback loops so you can continuously improve IdRM processes and apply them to new use cases.

Chapter 5

Identifying Your Identity Risks

In this chapter

- Learn how IdRM solutions discover, ingest, and normalize identity information across silos
- Understand the power of correlating identities
- Examine how analysts can use identity data to pinpoint identity security issues and problematic identities

"Things don't turn up in this world until somebody turns them up."

— James Garfield, 20th President of the United States

You can't reduce risks that you don't know about (obviously). But with identities, it's not enough just to *discover* all the identity-related information in your enterprise. Risk and policy compliance are determined by the ways user identities and their attributes, accounts, entitlements, credentials, and secrets fit together. Often you can't judge risk until you understand those relationships. This chapter discusses how an IdRM solution can comprehensively identify different identity risks by discovering, normalizing, correlating, and mapping identity information.

When people have multiple identities

Chief financial officers (CFOs) work with a lot of sensitive information. Most organizations closely monitor their CFO's interactions with core financial systems. But do they know all the unfederated identities on various email systems, social media accounts, cloud storage services, and collaborative applications (like Slack) that also belong to the CFO? Are they sure the CFO doesn't have accounts on systems that shouldn't handle the organization's most sensitive financial data? Probably not.

The same usually applies to many people in product development, engineering, and other critical departments. A good example is solution architects, who often have access to critical systems that are not under the purview of security and compliance teams.

You can't assess risk accurately, or even know that some risks exist, without being able to connect all the identities of key users (ideally with an identity graph – discussed below).

Discovering and Ingesting Identity Information

The first step in any identity risk management process is to discover and ingest as much identity information of all kinds as possible. This requires interacting with a wide range of applications and services, including:

- ☑ Human resources management systems (HRMS)
- ☑ Enterprise and cloud identity directories
- ☑ Privileged access management (PAM) and identity governance and administration (IGA) products
- ☑ Cloud-based and legacy on-premises identity providers (IdPs) that manage digital identities and support access-related functions like single sign-on
- ☑ Security and networking products such as extended detection and response (XDR) and secure access service edge (SASE) tools
- ☑ Security information and event management (SIEM) and security orchestration, automation, and response (SOAR) products

- ☑ Machine identity management solutions
- ☑ Certificate lifecycle management service
- ☑ SaaS applications and API-based services related to multiple cloud environments and on-premises and legacy solutions
- ☑ Logs from traffic-monitoring and directory syste

As we mentioned in Chapter 3, IdRM solutions also need to work with standards and frameworks such as OCSF, RISC, IPSIE, and CAEP. These help IdRM tools discover and ingest identity information from a variety of sources without custom integrations.

You can find out more about OCSF at https://github.com/ocsf, about RISC and CAEP at https://openid.net/wg/sharedsignals/, and about IPSIE at https://openid.net/wg/ipsie/ipsie-charter/.

Normalizing the data

An unsung but critically important capability for IdRM solutions (and for any other technology that works with disparate information sources) is data normalization.

An HRMS system, an enterprise directory, and a PAM solution might all record users' first names, last names, home addresses, job titles, business units, and office locations, bu they might store those items in different formats using di - ferent abbreviations or codes. Normalizing such data means putting it into a standard structure and common formats. Only with normalization can identity-related information from multiple sources be correlated, aggregated, and analyzed.

If you want to remember what makes IdRM solutions differe t from other security analytics products, the first item on the list is optimizing discovery, ingestion, and normalization for identity-related information. In the identity management domain, all the analytic power in the world won't help unless you have comprehensive data in standardized formats that enable comparisons and analysis across these disparate identity silos.

Correlating Identities

The next step in the IdRM process is correlating identity information from all relevant on-premises systems, cloud platforms, and SaaS applications to generate a comprehensive and definitive identity for each person and machine in the enterprise.

This process can be almost entirely automated, although there may be points where human decisions are appropriate. For example, it may be advisable to have a person rather than an algorithm decide if two accounts with names that are similar belong to the same person.

This is one of the areas where AI can be extremely valuable. With machine learning, a model can continually fine-tune itself by observing how human analysts accept and reject correlation suggestions.

If you're looking to correlate identities, then look for IdRM solutions that are taking a phased approach to deploying AI. The first stage could use machine learning to gather and summarize context and advise people on actions. The second phase should evolve to begin automating processes so people can step out of the loop and focus on monitoring and tuning instead of making every decision.

Identity graphs

IdRM solutions should be able to create an "identity graph" for each person that maps:

- ☑ All known identities and their organizational units
- ☑ Suspected additional identities – or "shadow identities" -- of that person
- ☑ Attributes, including not only personal and HR data, but also technical information such as frequently used devices, IP addresses, and locations, credentials, and biometric markers like fingerprint
- ☑ Credentials, entitlements, and permissions
- ☑ Policies and controls (for example, required to use MFA for authentication)

Figure 5-1 shows an excerpt from an identity graph.

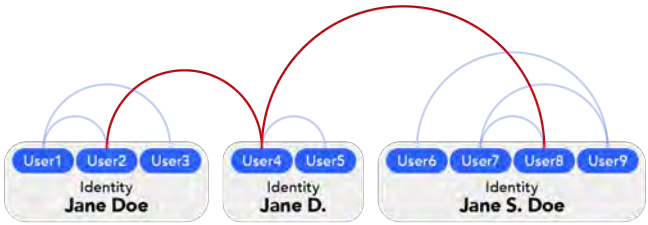


Figure 5-1: An identity graph connects different observed identities to show relationships and reveal risks.

Drilling Down to Uncover Issues

By correlating identity information within and across different environments and providing tools to drill down into the details of individual identities, an IdRM solution can enable identity management and security teams to immediately identify security issues and policy violations. Figure 5-2 shows a common scenario.

Figure 5-2: A comparison of user identities reveals active identities for a user who has had an identity disabled for administrative reasons.

By looking at Figure 5-2, an analyst might deduce that:

1. These three user identities are almost certainly associated with the same person.
2. That person is likely an ex-employee, since someone (probably in HR) has disabled one of the identities.
3. Two of the identities remain active, meaning that they could be used by the ex-employee or a threat actor who acquired that person's credentials.
4. This is a high-risk situation because one of the identities is privileged and likely has access to sensitive data and/or key systems.

While the analyst would need to verify one or two deductions before acting, the IdRM tool might save an hour or more in collecting and searching data. Or the relationship between the three identities might never come to light at all because they exist in different environments

In addition, discovering and comparing identity information can point to identities that are problematic because they are:

- ☑ **Stale or dormant** (i.e., unused for a long time, and therefore probably unnecessary and in violation of the principle of least privilege)
- ☑ **Inconsistent with similar identities** (i.e., lacking attributes or relationships typical of people or systems with similar roles)
- ☑ **Uncorrelated with any other identity** (without provenance and more likely to belong to external threat actors or rogue insiders than to normal employees with multiple accounts)

Generating Quick Wins for IAM and Security

Unfortunately for frustrated managers, many technology projects don't provide concrete results for months or years.

IdRM isn't like that. The elapsed time from beginning implementation to activating the type of correlation, identity graphing, and drill-down capabilities summarized here is typically days or weeks.

Deploying an IdRM solution can generate quick wins in multiple areas:

- ☑ Reducing risk by highlighting identity-related vulnerabilities and issues
- ☑ Saving identity and security teams many hours otherwise spent collecting and sifting through identity information
- ☑ Determining the organization's insurance-related identity security compliance level (see the next chapter's section on cyber insurance for more details)

Chapter 6

Quantifying Your Risks

In this chapter

- Review the factors that go into creating a risk score for individual identities
- Explore how risk scores can be calculated for departments, systems, regions, and other groups
- See formats for visualizing identity risk across an enterprise

"You can't run a business without taking risks."

— Millard Drexler

Quantify to Compare and Prioritize

As Millard Drexler states, business is about taking risks. However, it sure helps to quantify those risks. An organization takes a great step forward when it can comprehensively map identity information and identify the risks that might accompany those identities. But the essential next step is to be able to quantify the risks so security teams can:

- ☑ Compare and rank identities so the highest-risk ones can be remediated firs
- ☑ Aggregate and visualize risk by platforms and groups so the teams can track their organization's identity security posture and systematically reduce the identity attack surface over time
- ☑ Calculate enterprise-wide identity risk (the aggregate number of individual identity risks across the enterprise)

You should have a common scale for identity risks across your enterprise. The best way to rank them is usually with numerical risk scores, for example, on a scale of one to 10 or one to 50. Numerical scores are easy to add up and average. Non-numerical methods like low/medium/high classifications are used by many security tools but don't provide a deterministic risk level. Numerical risk scores are also flexible; they can be easily mapped to a scale like low/medium/high if needed.

A Note on Cyber Risk Insurance

The adoption of IdRM can play a major part in obtaining cyber insurance. The companies that write cyber insurance policies increasingly evaluate how organizations mitigate identity-related risks. They are looking for data to assist them in quantifying the risk factors.

Insurers now prioritize robust identity controls such as continuous monitoring, risk-based access, strong MFA deployments, and adaptive response policies. Organizations have reported benefits like reduced premiums, faster policy approvals, and enhanced coverage terms when they implemented such measures and documented a reduction in risk. In fact, data shows that companies with comprehensive identity risk practices can reduce their cyber insurance premiums by up to 20%. As IdRM adoption grows, it will provide insurers with greater confidence and help organizations secure more-favorable insurance terms.

Risk Scoring for Individual Identities

In a general sense, the risk to an enterprise associated with an individual identity is determined by:

- ☑ The identity's exposure to compromise
- ☑ The controls in place to protect it (or lack of them)
- ☑ The extent of its access to critical resources (its "blast radius") and the potential impact on the business if it is compromised and used for malicious activities

- ☑ Its likelihood of being targeted by threat actors
- ☑ Indicators of malicious actor or account takeover activity outside the organization, for example, compromised corporate data for sale in Dark Web marketplaces

Of course, there are no single, observable pieces of data that summarize exposure, or protection, or extent of the blast radius, or probability of already being compromised. But an IdRM solution can assess risk based on many factors related to the identity's attributes, permissions, observed behaviors, and relationship to other identities. Risk factors for identities include:

- ☑ Being privileged (having entitlements to access critical applications, data, infrastructure, or workflows
- ☑ Being orphaned, stale, dormant, or never used
- ☑ Being overprivileged relative to peers' identities
- ☑ Having membership in shared accounts with significant entitlements
- ☑ Interacting with sensitive data or applications in an anomalous fashion.
- ☑ Missing key attributes (e.g., not having a manager for people or an owner for software workloads)
- ☑ Missing credentials or using weak passwords or invalid certificate
- ☑ Using phishable or easily spoofed credentials
- ☑ Having missing, misconfigured, or inconsistently applied controls (e.g., MFA not being required for authentication, or obsolete versions of encryption)
- ☑ For machine identities, having no expiration date or an excessively long lifetime
- ☑ Making unusual requests to access resources, create new identities, or upgrade the entitlements of existing ones
- ☑ Being associated with compromised identities
- ☑ Being uncorrelated with other identities (and therefore more likely to belong to threat actors)

Once identities have been analyzed and given risk scores based on factors like these, analysts can rank them, as illustrated in Figure 6-1. Identities can be ranked by risk score within groups or globally across the enterprise.

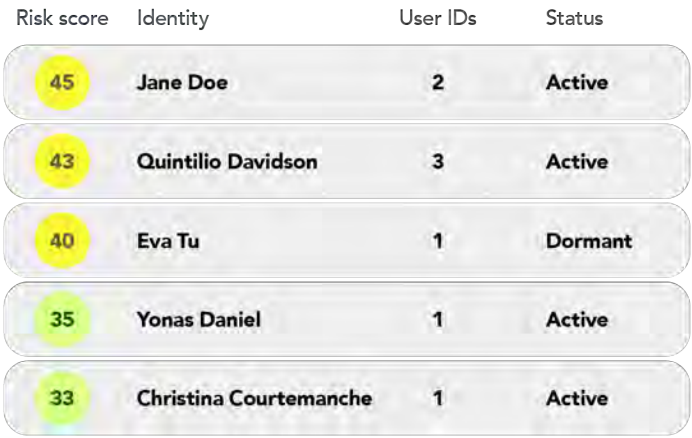


Figure 6-1: Quantified identity risks can be ranked for easy prioritization and triage.

Risk Scoring for Groups

Once individual identities have been given risk scores, an IdRM system can create aggregate risk scores for any kind of group defined by the organization, such as

- ☑ Departments or functions (finance, legal, IT, engineering)
- ☑ Platforms, systems, and applications (Azure Active Directory, AWS, email)
- ☑ Regions (Central United States, Brazil, Nordic, Africa)
- ☑ Business units or initiatives (headquarters, manufacturing, an acquired company being integrated into corporate systems)

An IdRM solution can create risk scores simply by aggregating the scores of all the identities belonging to the group.

However, group risk scoring can be enhanced by calculating group-wide metrics. Examples might include the percentage of identities within a group that:

- ☑ Have excessive permissions
- ☑ Are orphaned or dormant
- ☑ Are missing key attributes
- ☑ Are not using MFA for authentication
- ☑ Have weak credentials or invalid certificate

Visualizing group risks

Risk scores for groups can be ranked in descending lists similar to the one in Figure 6-1. However, to provide additional insight, they can also be displayed in visualization formats. For example, Figure 6-2 is a bubble diagram where groups with the highest risk—a combination of threat and possible impact—are shown in the largest bubbles.

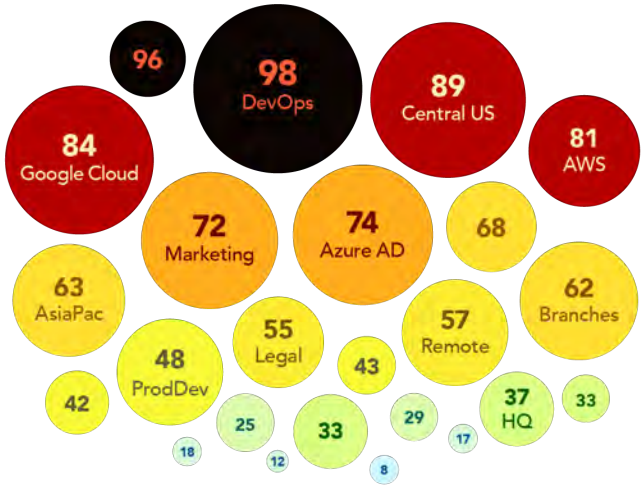


Figure 6-2: A bubble diagram organizing and highlighting groups with the highest risk.

Figure 6-3 provides an at-a-glance drill-down look into the major risk groups within one business unit.

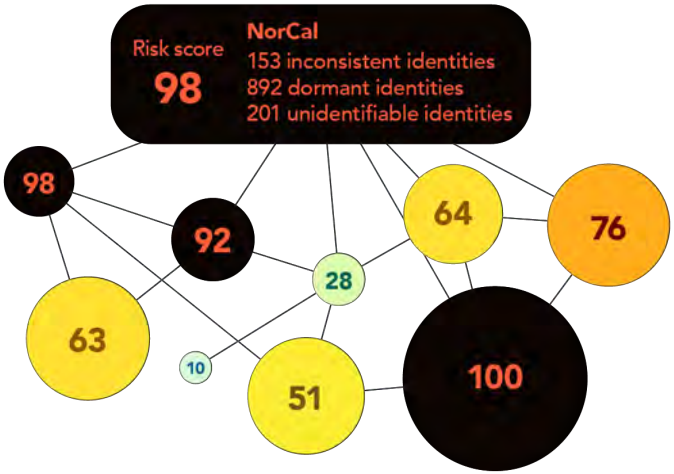


Figure 6-3: A drill-down into risks within a business unit helps analysts identify and quantify embedded risks and suggests where stronger controls are needed.

Using MITRE ATT&CK to Quantify Risk

As mentioned briefly in Chapter 2, the MITRE ATT&CK framework highlights many adversary tactics and techniques that focus on exploiting weaknesses in identity security. As a refresher, a "tactic" is the "what" of an attack. The 14 tactics included in the ATT&CK framework capture objectives adversaries try to accomplish during an operation, such as persist, discover information, move laterally, execute files, and exfiltrate data. "Techniques" represent "how" an adversary achieves these objectives by performing a specific action. About half of ATT&CK tactics rely heavily on compromising identities, including:

- ☑ Reconnaissance (10 total techniques, of which about half are directly related to identity hygiene)
- ☑ Initial Access (10 techniques, about half related to identity)

- ☑ Persistence (20 techniques, about 5 of which are identity centric)
- ☑ Privilege Escalation (14 techniques, half of which are identity focused)
- ☑ Credential Access (14 techniques, ALL of which will now or in the future exploit identity risks)
- ☑ Collection (17 techniques, half of them centered on tools like Adversary-in-the-Middle)
- ☑ Command and Control (18 techniques)

An IdRM solution can close the gap between identity silos and the tactics and techniques being mapped by your SOC teams. Also, quantifying risks through reliable, automated scoring can shorten reaction times.

The list above is only a portion of ATT&CK tactics. You can find out more about MITRE ATT&CK at https://attack.mitre.org/matrices/enterprise/.

Using AI to Quantify Risk

AI is still underutilized in many cybersecurity domains. IdRM, however, is one of the fields that can benefit most from ju - cious use of AI. AI technologies will enable IdRM solutions to quantify and rank identity-related risks with more sophistication and insight by leveraging:

- ☑ Threat intelligence about emerging attack techniques and IoCs
- ☑ Intelligence about attacks on the organization's business and supply chain partners
- ☑ Large volumes of event and status data ("signals") from endpoint and network security products
- ☑ Risk scores and alerts from identity security products that monitor events such as access requests, credential issuance, and privilege escalation

AI may also help IdRM solutions adjust the weight of different risk factors based on how they correlate with security outcomes.

Sharing Risk Scores with Identity Security Frameworks and Tools

The OCSF framework provides a method for creating and employing risk scores and confidence percentages based on identity-related risks. If your organization is planning to use security products based on this framework, IdRM tools can supply risk scores in OCSF-compliant formats to improve the accuracy and timeliness of risk analysis.

IdRM risk scores can also be shared with products that perform continuous authentication and manage access using frameworks and standards like CAEP and the SSE (Shared Signal and Events) framework it profiles.

Finally, IdRM risk scores can provide valuable input to adaptive authentication products, fraud detection systems, and other cybersecurity tools.

The Power of Quantification

Now that you have seen how IdRM solutions can quantify, rank, and display risks for both individual identities and groups, you can better appreciate the statements we made earlier about IdRM providing data and insights that enable identity and security teams to:

1. Prioritize remediation
2. Track and manage their organization's overall identity security posture
3. Focus resources to systematically reduce the identity attack surface
4. Ensure compliance with cybersecurity risk insurance policies

In the next chapter we will go into more detail about the processes that implement those improvements.

Consider having a round-table discussion about how your organization can leverage identity risk scores and rankings. Invite participants from identity management, the SOC, HR, security architecture, and other groups. You will probably gain a sense of the most valuable applications and uncover previously unsuspected use cases.

Chapter 7

Fortifying Your Identities Against Risk

In this chapter

- Examine the ways that IdRM helps organizations improve and automate remediation and attack surface hardening
- Understand how to overcome "fear of fortifying"
- See how an IdRM solution can leverage AI to fortify identities

"Hardening is the practice of making a system or application more secure than its default configuration."

— Darril Gibson

After identifying and quantifying identity risks, the next logical step is to fortify your identities against these risks. This includes remediating vulnerabilities, repairing misconfigurations, and fixing other security issues to reduc opportunities for threat actors to obtain and exploit identity information. These actions harden the identity attack surface and aligns it with the organization's policies and controls.

Most organizations already expend considerable resources on these activities, but not always efficiently. In this chapter w review how IdRM can improve remediation and attack surface hardening by:

- ☑ Facilitating prioritization
- ☑ Informing, automating, and accelerating remediation processes
- ☑ Improved planning and investments

Fortifying Identities

Global visibility and prioritization

As outlined in the previous chapters, IdRM solutions discover, correlate, and map user identities and related information, analyze relationships among identities, create risk scores for individual identities, and aggregate and compare risk for groups of identities.

IdRM thus enables identity and security teams to find identity related risks they would have overlooked, and to prioritize remediation tasks both within groups and globally. It also helps them see the groups (or departments, platforms, applications, regions, etc.) with the most risk so they can determine root causes and apply resources where they will have the greatest impact.

Enriching remediation

When SOC and identity management teams receive alerts about vulnerabilities and security issues, they often spend considerable time gathering information to determine if the alert is a false positive, and if not, what action should be taken. An IdRM solution can enrich the data analysts use to make these decisions. It provides critical context, insights and recommendations so analysts can make judgements faster and more accurately.

Automating remediation

IdRM solutions can be configured to send alerts and contextual information to SOC and identity management teams and integrated with ticketing and issue tracking systems. These connections help accelerate remediation and incident response workflows

In appropriate circumstances, IdRM systems can also integrate with security tools and cloud management systems to perform remediation and attack containment actions automatically. For example, when an IdRM solution detects high-risk identities or indicators of attack, it might initiate automatic processes to:

- ☑ Revoke permissions
- ☑ Revoke certificate
- ☑ Suspend credentials
- ☑ Force new credential issuance
- ☑ Revoke just-in-time access to an application or cloud platform

Overcoming Fear of Fortifying

Managers responsible for identity and security management sometimes develop a "fear of fortifying": that is, a reluctance to fully automate remediation processes because they might disrupt a business process or annoy important system users.

These are absolutely valid concerns. However, it is important to balance the "risk of breaking internal things" with real external risks. Always playing it safe with processes only seems like a low-risk strategy until a major data breach occurs because containment and remediation were delayed too long.

But there are also ways to smooth the path toward reliable, unobtrusive automated remediation. These include:

- ☑ Testing and tuning automated remediation with small units before rolling out the processes to larger groups
- ☑ Building in rollback capabilities so actions can be reversed
- ☑ Leveraging advanced analytics and machine learning, so systems continually improve their decision-making

Using AI to Fortify Identities

As IdRM solutions mature, they will incorporate AI in more activities for fortifying identities, using AI features to:

- ☑ Gather and analyze more data from more sources to make better remediation decisions
- ☑ Recommend appropriate levels of permission based on peer groups or adjacent teams
- ☑ Generate punch lists to guide identity teams in remediating identity issues
- ☑ Detect overprovisioning by comparing identities for similar users, then suggest cutbacks in entitlements
- ☑ Correlate types of identity risks with observed security incidents for the specific organization and adjust risk scores and remediation priorities
- ☑ Suggest additional monitoring and controls that would have the greatest impact on reducing risk
- ☑ Propose immediate remediation for real-time detected high-priority events, i.e. a "breach in progress"

The MITRE ATT@CK framework mentioned in chapter 6 can provide guidance on fortifying identities. Look across your identities to see which ones intersect with the highest number of ATT&CK tactics and remediate those first.

Hardening the Attack Surface

Some of the greatest challenges for CISOs, chief identity officers, VPs of IAM, enterprise security architects, and other tasked with managing identity security programs are aligning resources with actual enterprise risks and justifying investments in new controls and staff

IdRM helps them by providing hard data on the identity risks most prevalent in the enterprise, the severity of those risks, and the platforms and locations that are most in need of management attention, resources, and investment.

In fact, organizations that try to systematically reduce and harden their identity attack surface without IdRM are essentially flying blind, or at least severely visually impaired

Chapter 8

Selecting the Right IdRM Solution

In this chapter

- Review a checklist of criteria for selecting an IdRM solution that meets the requirements of your organization

"Make good choices."

— Your mother

How to Find Your Switzerland

At the Congress of Vienna in 1815, the great powers of Europe agreed that Switzerland should be neutral. Ever since, the country has served as a meeting place for nations and a diplomatic force for peace and global harmony.

An IdRM solution acts like a Switzerland for the disparate elements of an identity management program. It gathers participants from all corners of the identity ecosystem, gives them a forum to share information and experiences, and generates plans and programs to make identities safer.

We're not going to push that analogy any farther, but we can offer some suggestions on how to find a Switzerland, er, IdR solution, that fits the needs of your organization

A Brief Checklist

Here are a few criteria you should consider in your assessment of IdRM options.

You should also apply these criteria if you plan to develop your own IdRM solution or IdRM capabilities in house.

Ability to leverage existing investments

As we noted in Chapter 3, IdRM solutions should not duplicate or displace existing IAM tools. That means you should be able to:

- ☑ Leverage the full value of your existing investments
- ☑ Prevent overlapping or conflicting IAM processe
- ☑ Avoid affecting the functioning or performance of your computing infrastructure

A wide range of integrations

IdRM solutions should be able to discover and ingest identity information from a wide range of sources. They must also disseminate alerts, contextual information, and remediation recommendations through email, text, and collaboration applications, ticketing and issue tracking systems, security tools, and cloud management systems.

Look for products that:

- ☑ Offer out-of-the-box integrations with popular IAM an security tools, cloud platforms, and SaaS applications
- ☑ Work with APIs and frameworks and standards such as OCSF, RISC, IPSIE, and CAEP, so they can be integrated quickly with additional systems

Enterprise-wide visibility

Many identity security issues and risks can be detected and assessed only by creating a comprehensive picture of identity information and relationships across the entire enterprise.

Of course, IdRM solutions should be able to discover and ingest identity information from a very wide range of sources. But you should also ensure that they can normalize, correlate, analyze, map, and search all that information together.

Enterprise scalability

To be effective, an IdRM solution needs to ingest and correlate large amounts of data from the start and scale to handle massive volumes over time. In addition, analysis and remediation need to be performed quickly so identity and security teams can stay ahead of threat actors. Make sure the IdRM alternatives you are considering are designed to work with the scale and service levels you require.

Meaningful risk scores

IdRM solutions should create risk scores that:

- ☑ Are easy to interpret
- ☑ Reflect a wide range of meaningful risk factor
- ☑ Can be used to rank and compare the risk levels of both individual identities and groups

Value for many teams

Chapter 4 discussed how IdRM information can strengthen the work of many security practitioners and managers. These include IAM and SOC teams, OT, IoT, and DevOps security groups, auditors and compliance departments, identity management leaders, and CIOs and CISOs.

Look for IdRM solutions with tools to help all these groups:

- ☑ Visualize enterprise- and group-wide identity risks over time
- ☑ Drill down on risks for groups and individual identities
- ☑ Understand relationships and contextual information that can be used for better decision making

Assess the Vendor

IdRM is evolving rapidly. When you evaluate IdRM solutions, you should look beyond features that are available in the most recent product release and assess the vendor's ability to meet your requirements over time. Key questions include:

- ☑ Does the vendor have a track record of integrating multiple IAM technologies towards a common end?
- ☑ Is the vendor a thought leader and innovator in this field?
- ☑ How does the vendor's vision and roadmap align with your current and future needs?
- ☑ Does the vendor's architecture and design principles support scalability and flexibility
- ☑ Is the vendor committed to the interfaces, platforms, and standards that "future proof" your investment?
- ☑ Does the vendor have a great track record in areas like customer support and attentiveness to customer input – and above all, are its customers happy?

A Valuable Tool Today, the Foundation of Your Identity Fabric Tomorrow

You can think of an IdRM solution as a stand-alone tool that will provide valuable benefits now *and* as a key step toward a more effective identity security program.

Beyond being just another security tool, IdRM is a business enabler. It helps create and deploy the identity fabric, fortifies the organization's identity security posture, and contributes to governance, risk, and compliance (GRC) efforts. In addition, it enables workers to be more productive by removing frictions associated with poorly implemented identity hygiene.

IdRM also gives IT groups their first experience with "identity fabric thinking" and starts them on a path toward solving persistent, large-scale problems related to identity. Ultimately it helps them unite identity services across numerous platforms and use cases.

We hope you will explore the value of IdRM both as a powerful security tool today and a step on the way to tomorrow's comprehensive, integrated identity fabric.

When it comes to identity risk, **what you don't know** hurts the most.

- Over-privileged roles
- Blast radius overly high
- Passwords available on the dark web
- Risky machine identities
- Multiple uncorrelated identities
- Not protected by MFA

It's already hard to keep track of digital identities, and more are created every day. That may be why over 90% of organizations experience identity-based attacks every year. **Axiad Mesh** helps you identify and quantify the risks your identity teams face every day, and then helps you fortify those identities against non-stop attacks.

AXIAD

WWW.AXIAD.COM | (408) 841-4670
101 Metro Drive, Suite 560 San Jose, CA 95110

Almost every organization has a fast-growing, rapidly morphing, and all too often poorly defended identity attack surface. Learn how to map it and how to defend it.

Many enterprises have found themselves squarely in the middle of an Identity Boom: an explosion of identities that are loosely managed, that belong to humans and machines and applications alike, and that have sprung from aggressive digital transformation efforts. At the same time, identity-based attacks are on the rise and practitioners are looking for help in addressing them.

This Guide provides focused advice on:

- Identity Growth – How and why the identity attack surface has grown, and why traditional security controls fail to protect it.
- Discovery Challenges – How to address the challenges of finding and inventorying identities throughout the modern enterprise.
- Weaponization of Identities – How identities are used by adversaries and targeted by their most aggressive campaigns.
- Identifying Identities – Ingest identity information from multiple sources throughout the extended organization, whether on-prem or in the cloud.
- Quantify Identity Risks – Apply consistent scoring across discovered risks and rank them for prioritization.
- Fortify Identities Against Risk – Learn how to harden identities and mitigate risks.

About the authors

Michael Thelander is director of product marketing at Axiad. Jon Friedman is a managing consultant and senior analyst at CyberEdge Group.

CYBEREDGE PRESS℠

Not for resale

ISBN 978-1-948939-44-7