LEARNING MADE EASY

SailPoint Special Edition

Modern Identity Security

for dummies®

A Wiley Brand



See why identity is the new security perimeter

Discover how identity security drives business value

Tap into AI to automate identity security

Brought to you by

SailPoint

Steve Kaelble

About SailPoint

SailPoint equips the modern enterprise to seamlessly manage and secure access to applications and data through the lens of identity — at speed and scale. As a category leader, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency. SailPoint helps many of the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.



Modern Identity Security

SailPoint Special Edition

by Steve Kaelble

for dummies®
A Wiley Brand

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Modern Identity Security For Dummies®, SailPoint Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2025 by John Wiley & Sons, Inc., Hoboken, New Jersey. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Trademarks: Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit be www.dummies.com/custom-solutions. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-34982-1 (pbk); ISBN 978-1-394-34983-8 (ePDF);
ISBN 978-1-394-34984-5 (ePub)

Publisher's Acknowledgments

Editor: Elizabeth Kuball
Acquisitions Editor: Traci Martin
Senior Managing Editor: Rev Mengle
Client Account Manager: Jeremith Coward
Production Editor: Umeshkumar Rajasekhar

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Explaining what identity security is
- Resolving misunderstandings about identity security
- Grasping the importance of identity security
- Spelling out the key benefits

Chapter 1
Understanding Modern Identity Security

Digital technologies make the world go 'round, and digital identities continually access those technologies. This chapter explores how identity security helps enterprises safely control and monitor access to digital technologies, even as cloud architectures and AI add perplexing complexities.

Defining Identity Security

It wasn't all that long ago that identity security was largely a topic of interest to mostly information technology (IT) people. Then the horror stories started taking over the headlines, and everyone all the way up into the C-suite came to realize that breaches can pose anything from an operational to an existential threat. As IT landscapes became more complex, so did the task of protecting them from cyber threats and ensuring compliance with wide-ranging privacy regulations.



REMEMBER

Lost amid all that complexity is a surprisingly simple fact: Enterprise security is really all about identity. It's a matter of ascertaining and knowing the identity of every person and entity that can access digital resources and critical data, and then ensuring

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

that only the right identities can access only the exact things that they need to access.



REMEMBER

With that in mind, the focal point of safely doing business in today's digital world becomes the idea of *identity security.* Sometimes identity security is referred to as *identity governance and administration* (IGA); however, identity security is much more than that. Identity security goes beyond traditional IGA by combining dynamic access governance, AI-driven insights, policy enforcement, and continuous risk assessment. It's how the business provides vital technology across a diverse workforce, while protecting against the inevitable cyber threats.

Here are some concepts associated with identity security:

- **Identity and access management (IAM):** This specialty automates the assignment and review of access, so that only the right people get fine-grained access to only the right data and applications, at the right times, for the right reasons.
- **Privileged access management (PAM):** This subset of IAM focuses on protecting the privileged accounts of those users whose work requires them to access databases, backend systems, and other sensitive places.
- **Access management (AM):** This has to do with authentication, granting various identities access to applications through such technologies as single sign-on (SSO) and multifactor authentication (MFA).

Identity security extends these concepts so organizations can improve and automate their processes to validate least-privilege access, make sure that access is reviewed appropriately, and be certain that separation of duty policies are in place and enforced. It's all about accountability, transparency, and risk mitigation.

Untangling Identity Misconceptions

As outlined in the preceding section, identity security encompasses a number of related concepts. Think of it as being greater than the sum of its parts, because any one of these concepts on its own doesn't get the whole job done effectively or efficiently.

For example, identity security may sound like access management, in that it incorporates such services as SSO and MFA. Those

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

three-letter services are essential to identity security, particularly the task of authenticating the identity of a person or entity seeking access.



REMEMBER

But authentication is only the first step. Think of an airline boarding pass. Show it at the gate along with your valid ID card or passport, and you're authenticated as a passenger. The next question is, where are you authorized to sit? First class or coach? Which boarding group are you in? Are you entitled to a complimentary meal? Your boarding pass provides the proper authorization.

In the context of identity security, authorization is the process of verifying what an authenticated user is allowed to access — what specific applications, files, and data. Authentication happens first, with the help of such verifiers as passwords, personal identification numbers (PINs), biometrics, and security questions. Then comes authorization, based on settings and policies established by the organization. Here are two common methods of authorization:

- **Role-based access control (RBAC):** Access is determined by the user's role in the organization. RBAC helps people within specific roles get the access they need to succeed, but nothing beyond what their role needs.
- **Attribute-based access control (ABAC):** This is more granular than RBAC, and it adds in user-specific attributes such as name, ID, and security clearance. ABAC attributes might also include time of access, location of data, and current organizational threat level.

Recognizing Why Identity Security Is Vital

Cyberattacks and identity-based threats are more prevalent all the time, with an ever-increasing impact on organizations. Business impacts include lost revenue, damaged reputation, and the costs of containment. These continually worsening impacts make identity security increasingly critical.



TIP

Compliance requirements are an ever-growing concern, too; organizations need all the help they can get not just meeting compliance needs, but also proving compliance in ways that are auditable. Identity security tools are incredibly helpful in that regard.

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.



REMEMBER

Ultimately, identity security is essential for staying secure and remaining compliant — but it also opens the door to greater business productivity that enables growth. Technology can only propel business success if it's accessible to the people who need to use it and identity security facilitates that access while keeping out those who shouldn't have access.

Benefiting from Modern Identity Security

What are the selling points of identity security? One giveaway is right there in the name: security. That's a good reason, but it's far from the only one. Here are some of the key benefits:

- **Reduced operational costs:** A solid identity security program automates the labor-intensive processes of identity governance and administration. Access certifications, access requests, password management, and provisioning — all can be automated for dramatically lower operational costs. Users gain self-service options to handle their own needs, reducing some access tasks from hours to minutes. IT staff can reduce costs as much as 15 percent, while spending less time on administrative tasks and more time adding value in other ways.
- **Improved compliance and audit performance:** Strong identity security helps you verify that the right controls are in place to ensure compliance with a host of security and privacy regulations — the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and the Sarbanes–Oxley Act (SOX), to name some of the most impactful ones. Audits and compliance are far less of a hassle with the right tools in place.
- **Upgraded efficiencies:** Everyone's better off when users have easy access to the applications and data they need to succeed. They become more productive, more quickly, even as their roles change.
- **Reduced risk and stronger security:** Yes, we promised security was one of the reasons. Identity security offers a centralized view into who has access to what. With the help of automation, it quickly spots inappropriate access, weak controls, or policy violations, and then addresses and remediates the issues.

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Exploring identity lifecycle management
- Provisioning access for users
- Setting up policies and controls

Chapter 2
Building an Identity Security Program

What does it take to create a modern identity security program? It starts with a full picture of the lifecycle of an identity, creating it and evolving it and, when the time comes, bidding it farewell. It's a matter of provisioning access, establishing policies and controls, and ensuring that the effort meets the needs of not just security but other enterprise compliance mandates. This chapter spells out the specifics.

Managing the Lifecycle

Think of digital identities as though they're living things. That may seem like a sci-fi kind of thought, but identities do have lifecycles. They begin, they evolve, their needs change, and eventually, their time is up. Managing that lifecycle is a key component to an identity security program. And it's a component that can be a time-consuming manual pain or an efficient and largely automated or self-service process.


TIP

A modern, unified identity security program will automate the management and control of what otherwise would be complex challenges. A lifecycle-driven approach can work wonders for automated provisioning and deprovisioning for the organization's joiners, movers, and leavers.

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

It's an approach that empowers business users to request and manage access to resources, without causing hassles for the information technology (IT) team. It should offer visibility and control of access, whether you're looking at employees, contractors, or even nonhuman users such as bots, service accounts, and so on. It should be able to evolve, appropriately changing access as a user's role changes. And the compliance team should be able to easily gather what it needs when responding to audits.

Here's how a modern system handles automated provisioning:

- Account creation and access to apps and data are automated.
- Granting of birthright access and entitlements are data-driven and accurate.
- The system knows when users join, move, or leave.
- A least-privilege access model is enforced, with visibility into any overprovisioning or orphan accounts.

And here's how access requests are handled:

- Users can make a request for new access, for themselves or others, from a catalog of roles and entitlements that's automatically built and refreshed.
- Generative artificial intelligence (AI) helps build easy-to-understand entitlement descriptions to inform approvers who must determine if this request is appropriate.
- AI-driven recommendations based on activity help inform determinations about what access should be granted.
- The system captures justification for access requests, helping enable good decision-making and providing an audit trail.
- Temporary, time-bound access is easy to create.
- One interface shows the progress of approval requests.

Provisioning Users


REMEMBER

A key step in identity security is *user provisioning*, which is the process of creating a user's digital identity and access privileges for various resources that might live on-premises, in the cloud, or in a hybrid environment. User provisioning takes into account

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

a person's name, job role, department, plus various attributes, entitlements, memberships, and other data.

Some aspects of user provisioning are self-service, while other things may be discretionary, including getting access to data and apps. After mandatory authorizations are taken care of, access in some cases may be granted based on workflow requirements. And ideally, much of the process is automated and handled by software that applies established rules.


TIP

Provisioning must change as user roles and business needs change. As an employee moves from one role to another or takes a temporary assignment, some access will need to be removed, while access to other resources must be added.

The opposite of provisioning is *deprovisioning,* which is when access and privileges are revoked based on role changes or perhaps when an employee leaves. Deprovisioning is super-important, because even if a fantastic employee departs under the best of circumstances, if that person's account goes dormant, it could become a gateway to cyberattacks.

Best practices in user provisioning include centralized identity security processes and policies. Automating the process is key, reducing the risk of over- or under-provisioning that can happen with manual systems. The principle of least privilege should be the guiding light in a modern identity security solution because it assures that users get only the access they need to do their job. Risk-based authentication can automatically block users if troubling actions are spotted.


REMEMBER

Auditing and reporting are essential elements, too, because security concerns often coincide with compliance requirements. Internal auditing and reporting are proactive ideas that support both compliance efforts and the best security posture. The right identity security program can document risk mitigation controls and coordinate a host of compliance activities that get a good handle on audit deficiencies and breaches. More on that in the next section.

Establishing Access Controls

In the context of identity security, it's not just people who have identities. Connected devices and AI can have identities, too, to name a couple possibilities. With increasingly complex

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

multi-cloud environments, various kinds of cloud resources must interact constantly. Modern, unified identity security must extend to cloud infrastructure and cloud identities.



REMEMBER

That's where *entitlement management* becomes vital. Identity security includes defining the entitlements assigned to systems, applications, data, and cloud services — the permissions and boundaries that declare what they have access to and what actions they're allowed to take. Given the always-changing nature of cloud environments, entitlement management needs fine-grained visibility and control, with automatic adjustment and detection of excessive entitlements. As always, least privilege is the aim.

Role-based access control (RBAC) makes provisioning simpler by connecting identities with defined roles in the enterprise. If a person is approved for a role or task, specific permissions and access rights are automatically granted. If they leave that role, access is automatically adjusted or removed.

Policy-based access control (PBAC) or *attribute-based access control* (ABAC) enforces policies based on such characteristics as department, location, manager, and even attributes such as the time of day, the identity's normal behavior, relationships with third parties, and actions requested. Attributes can be drawn from a variety of data sources — not just identity tools but also human resources applications and enterprise resource planning (ERP) systems. It allows a granular approach to access.

One more key concept to build into identity security efforts is *separation of duties* (sometimes called *segregation of duties*, or SoD). The principle holds that no single user should be allowed total control over certain kinds of activities or processes or sensitive systems. Completing a sensitive process should require more than one person's involvement.

For example, the person who authorizes check payments shouldn't be the same person who signs the check electronically. That kind of hard-and-fast rule is known as *static enforcement. Dynamic enforcement* means controls are determined in real time, with users needing to get approval from a different authorized person to perform a task.

SoD is a good practice for many reasons, including accounting and cybersecurity concerns. That's why it's actually a compliance requirement, including being one provision of the Sarbanes–Oxley Act (SOX).

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Using AI to supercharge identity processes
- Tapping into AI for detecting threats
- Automating with the help of AI

Chapter 3
Tapping into AI and Automation

Artificial intelligence (AI) is touching all kinds of work in all types of enterprises — allowing powerful results and eliminating mundane tasks. It's no surprise AI-driven identity security is the key to automated and centralized control over access to data, applications, systems, and cloud infrastructure, along with providing 360-degree visibility into risk. This chapter shows how AI supercharges identity security.

Streamlining Identity Processes

AI-driven data intelligence can automate the discovery, management, and control of user access. It makes the process of discerning access faster and more reliable, and it also makes it easier to discover and respond to potential threats.



TIP

For business managers, identity teams, and application owners, AI helps build and optimize an always-adapting access model. The identity data you already have turns into insights for modeling the correct access for each identity and for decision support. And by tackling the tedious tasks, it allows greater focus on higher-risk access.

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

AI helps risk management professionals be more proactive in spotting risky access and doing something about it. It gives identity security professionals comprehensive visibility they need to ensure compliance. And for end users, it provides access they need to be as productive as possible on Day 1, adapting to constant changes, while ensuring least privilege.



TIP

Take the work of writing descriptions for entitlements as just one example. These descriptions are essential, but they can be a time-consuming pain to create. As SailPoint Identity Security Cloud demonstrates, generative AI can help. Automatically created descriptions can improve access reviews and come in handy in governance and compliance.

AI can also be a game-changer in employing role-based access control (RBAC). In the past, role design relied on a time-intensive, manual effort. With a modern identity security program, AI can take on that task. It can look at a sea of users, divide them into peer groups, and then proactively spot who has anomalous access. AI can automatically build roles by identifying clusters of like access, and then assigning the right level of access needed for each role defined. It can then identify outliers and fix their risky access.

In the process, AI builds an access model that maximizes productivity with the least amount of privilege. From there, it uses machine learning (ML)–powered continuous role analysis and recommendations to maintain the model, automatically analyzing to discover new and specialized roles, all in a way that minimizes administrative involvement.

The access model also is essential in beefing up security beyond the employed workforce. Managing the identity lifecycle of all identities, but especially nonemployees and machines, can be difficult and time-consuming, so it's ripe for the benefits of a centralized, AI-driven system.



TIP

The SailPoint solution helps organizations efficiently track and control access for machines and people who aren't full-time employees, such as contractors, vendors, or business partners. The solution streamlines collaboration between internal and external teams to collect and manage identity details, ensuring that the right people get the right access when they need it — and that access is removed when they don't. This practice reduces

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

security risks, improves compliance, and makes managing non-employee identities faster and easier.

The road to modern, unified identity security also involves onboarding the applications that a system will govern. Typically, two types of applications are supported. Access applications are those that provide context for access rights, requests, and access policies. Enterprise applications are those that need identity security functions to manage access to accounts on them. They may be on-premises or software as a service (SaaS) platforms.


TIP

Application onboarding discovers enterprise applications that can be added to the identity security program and assists with streamlining and accelerating the onboarding and configuration process of those applications. This practice ensures that the applications are subject to the full array of identity security capabilities accelerating an organization's time-to-value.

Detecting Threats

The proverbial needle in a haystack is what you might think of as an "outlier" in the haystack — nearly impossible to find. The same goes for identity outliers, but spotting them is essential for securing a modern, data-driven environment.


TIP

That's another way that AI and ML can be helpful. They're incredibly powerful technologies for looking through the haystack of identities and seeing who stands out, with patterns that deviate from the norm.

Not all outliers are nefarious, of course. An identity outlier could be a privileged user with higher access levels than most, a system account that's handling automated tasks, or someone who's taken on a short-term assignment with different access needs. But sometimes an outlier is a compromised account or an insider threat, either of which might have veered from acceptable behavior into malice.

ML technologies learn from vast identity data and can spot even subtle patterns with incredible precision. ML is skilled at detecting toxic access combinations that could open the door to data theft or fraud. And it spots threats very quickly, which minimizes the window of opportunity for threat actors.

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.



REMEMBER

You'll want an outlier dashboard offering a broad perspective of the outlier landscape. Such a feature gives each outlier a risk score, with risk thresholds that are based on organizational risk tolerance. This task has clearly moved beyond human capabilities. Identifying an outlier is a complex consideration, based on numerous factors such as entitlement count, role uniqueness, rare access, and similarities/differences compared to peers.

Expect this work to happen constantly, in real time. If a threat is detected, the system should automatically revoke access. A variety of direct and indirect remediation tactics can reduce outlier threats. And it's possible to make a strategic decision to ignore an outlier based on unique factors related to the particular identity.

Automating with Agentic AI

There are countless ways to employ agentic AI to automate the work of identity security, above and beyond the AI examples cited earlier. Solution providers continually search for tedious customer tasks that can be turned over to automated intelligent agents for their assistance, guidance, and natural-language interactions.

Minimizing manual intervention is one of the primary aims. The work of identity security is essential, but it's also vital for the business to keep security requirements from becoming a productivity bottleneck. AI streamlines processes to grant appropriate access quickly.

As outlined earlier, agentic AI can also do things that humans simply cannot do at the necessary scale. Constantly watching for identity outliers and threats effectively — this is where AI is absolutely essential. Increasingly, so is creating and continually adapting access models.



TIP

Streamlining identity processes into centralized management leads to stronger access governance, which makes the compliance team smile. AI-driven insights help spot risky access and certify that access is correct and in alignment with identity security and regulatory requirements. A 360-degree view allows business-friendly reports that satisfy regulators. Proving separation of duties is another feather in the regulatory cap.

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Avoiding common pitfalls
- Building an identity security road map and following the path

Chapter 4
Ten Tips for Improving Identity Security

Losing sleep wondering whether your current security practices are up to the task? Ready to take your enterprise to the next level of identity security maturity? Read on for ten tips to help your organization improve identity security.

- **Moving past passwords:** Passwords have been around as long as there have been secure accounts on computers. But they really can't guarantee security because they're vulnerable to breaches, even if you build in biometrics or other extras. Ultimately, securing a login provides no protection from inappropriately defined access — identity security is the perimeter you must build and defend.
- **Embracing least privilege:** The best defense is an assurance that no person or entity can access anything beyond what they need to succeed in their given role. The concept of least privilege minimizes risks by ensuring users have only absolutely necessary permissions. This limits attack surfaces, thwarts insider threats, and enhances compliance with policies and regulations.
- **Thinking beyond IT:** Security is everyone's business — not just information technology (IT) security teams but also application owners, all the way up to executives. Identity security protects from threats that can halt operations and cause horrific financial and reputational damage. But when done right, it also opens the door to greater productivity by all and facilitates not just privacy compliance but financial regulatory compliance as well.

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Setting a vision:** The vision for your identity security program should be informed by trends shaping the future of identity security and the maturity of your program today. Dive in knowing what else you also hope to gain for end users, IT staff, compliance specialists, and the business overall. Identity security benefits operations, competitiveness, and the success of the business. That's some real return on investment.
- **Checking your posture:** A smart journey begins with a maturity assessment that spells out your current identity posture. Most organizations are still near the start of their identity journey, with manual processes and fragmented technologies. Head to `www.sailpoint.com/identity-security-horizons` to assess your identity maturity.
- **Getting quick wins:** Any change management specialist will tell you that quick wins help with adoption. That can mean starting small, perhaps tackling one department, and then expanding from there. Just remember to also establish long-term goals.
- **Choosing tools and partners:** I mention "fragmented" technologies earlier. What you need is the opposite: unified identity security, a platform that centralizes access, offers 360-degree visibility, and taps into artificial intelligence (AI). Partners also can help you make the most of your program, with planning and advisory services as well as implementation help.
- **Checking the list:** To get from here to where you need to be, make a checklist that guides your planning and helps you select the right solution. Explore how you'll build a business case, how solutions handle access requests, how they automate provisioning, how they're leveraging AI and machine learning, what they do for password management, and how they're set up for separation of duties. For more checklist ideas, check out `SailPoint's Ultimate Guide to Unified Identity Security Checklist`.
- **Measuring success:** With any process improvement, you'll never know how successful you are without metrics. Try counting how many access control actions you're able to automate. Or the percentage of resources you streamline and the resulting cost savings. Or how much you reduce time to provision access.
- **Digging deeper:** This is a short book, and I've included all the insights that would fit. You'll find a lot more resources and learning opportunities by visiting `www.sailpoint.com` and clicking the Resources tab.

These materials are © 2025 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

SailPoint

Secure every identity. Manage all access.

Welcome to the core of enterprise security





sailpoint.com



Enhance identity security for safety and efficiency

As cyber threats continue to grow, modern identity security is how organizations thrive. It effectively deters attacks while improving efficiency and costs. It's the secret for satisfying both the risk/compliance team and users, all while supercharging productivity and innovation to please business leaders. *Modern Identity Security For Dummies* is your guide for building stronger identity security, managing identity lifecycles, getting the right access to the right people, and using AI to detect threats and streamline processes.

Inside...

- Understand what identity security means
- Discern authentication and authorization
- Explore the benefits of identity security
- Manage the full identity lifecycle
- Establish the right controls for access
- Automate processes with agentic AI
- Build an identity security roadmap

Steve Kaelble is the author of many books in the *For Dummies* series, and his writing has also been published in magazines, newspapers, corporate annual reports, and coffee table books. When not immersed in the *For Dummies* world or writing articles, he engages in healthcare communications.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-34982-1
Not For Resale



for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.