LEARNING MADE EASY

SailPoint Special Edition

Adaptive Identity Security

for dummies®
A Wiley Brand



Leverage AI to identify risk fast

Govern human, machine, and AI identities with ease

Safeguard your enterprise with modern security

Brought to you by

SailPoint

Eric Butow

About SailPoint

SailPoint (Nasdaq: SAIL) is defining the new era of adaptive identity security. In a world where non-human identities now significantly outnumber humans, our AI-powered platform unifies identity, security, and data intelligence to protect today's enterprise from advanced identity-based threats. We deliver the identity solution that spans both the breadth of identities and the depth of context needed to drive real-time access with confidence. Built on principles like zero-standing privilege and contextualized risk, our SailPoint platform transforms identity from a point of vulnerability into a powerful security advantage. Trusted by many of the world's leading organizations, SailPoint secures the enterprise with intelligent, autonomous identity security.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.



Adaptive Identity Security

SailPoint Special Edition

by Eric Butow

for dummies®
A Wiley Brand

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Adaptive Identity Security For Dummies®, SailPoint Special Edition

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

Copyright © 2026 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 www.dummies.com/custom-solutions. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-45826-4 (pbk); ISBN 978-1-394-45827-1 (ebk); ISBN 978-1-394-45828-8 (ebk)

Publisher's Acknowledgments

Editor: Elizabeth Kuball
Acquisitions Editor: Traci Martin
Senior Managing Editor: Rev Mengle
Client Account Manager: Jeremith Coward
Content Refinement Specialist: Umeshkumar Rajasekhar
Special Help: *Susie Spencer, Jaishree Subramania*

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Table of Contents

INTRODUCTION 1
About This Book 1
Foolish Assumptions 2
Icons Used in This Book 2
Where to Go from Here 2

CHAPTER 1: **Realizing Why Old-School Security No Longer Works** 3
Understanding the New Battleground: Your Identity 4
Counting Your Digital Population: Humans, Machines, and AI 4
Flying Blind: Why Traditional Security Tools Can't Keep Up 5
Installing Real-Time Governance for Humans and Autonomous Agents 6
Establishing Identity as the Foundation of Trust and Insurability 7

CHAPTER 2: **Defining Adaptive Identity: Security That Thinks** 9
Discovering Adaptive Identity 10
Moving from Snapshots to a Live Video Feed 11
Thinking with Context: Who, What, When, Where, and Why 12
Getting Ahead of the Attacker 13
Understanding Core Principles for the Agentic Economy 14

CHAPTER 3: **Introducing the Four Essential Elements of Adaptive Identity** 15
Capturing the Shift to Always-On Governance 16
Securing Your Digital Workforce 17
Ending Standing Privilege Access 18
Bridging Identity and Threat Detection in the SOC 19

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

CHAPTER 4: **Implementing an Adaptive Identity Strategy** 21
Building for Trust and Automated Response 22
Discovering and Mapping Every Identity 23
Establishing Real-Time Governance 23
Enforcing Dynamic, "Right Now" Access 24
Connecting Identity to Your Security Ecosystem 26

CHAPTER 5: **Ten Hallmarks of a Truly Adaptive Identity Strategy** 27

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Introduction

For organizations today, it's not just humans who need access to company resources. You now have three distinct access groups:

- **Humans** include the people in, or interacting with, your organization.
- **Machines** are nonhuman entities like service accounts and applications that require access to systems.
- **Autonomous artificial intelligence (AI) agents** access your business data and tools to do their work.

Each of these is an *identity*, which is broadly defined as a digital representation of an entity that requires access to organizational resources.

SailPoint's platform helps organizations govern access across all these identity types by defining and managing access with precision. Through adaptive identity security, SailPoint provides the guardrails for secure, controlled, compliant, and predictable access.

About This Book

This isn't just a book — it's your field guide to building a modern, adaptive identity security strategy using the best practices in the industry. So, grab your favorite beverage, sit in your comfy chair, and get ready to explore the world of adaptive identity.

Adaptive Identity Security For Dummies, SailPoint Special Edition, breaks down key components of managing your human, machine, and AI agents in a simple and digestible manner. Topics you'll find in this book include the following:

- Why old-school security no longer works today
- What adaptive identity is and how it makes your business more secure
- The four essential elements of adaptive identity

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- How to implement an adaptive identity strategy that works for your business
- What makes for a truly adaptive identity strategy

Foolish Assumptions

In writing this book, I made a few assumptions about you, the reader:

- You're someone who manages identity security on the daily.
- You want to have control over which agents have access to your data and systems.
- You know that you need to manage your agents and security better, but you have a lot of questions you need answered.

Icons Used in This Book

To make things easier and ensure that you don't miss important details, I use icons throughout this book. Here's what the different icons look like and mean:



TIP

The Tip icon is a small piece of advice that may save you time and make your adaptive identity journey easier.



REMEMBER

This book covers a lot of details and information, so every now and then you see a Remember icon to remind you of the most important details. When you're reading every juicy detail of the book, the Remember icon just helps resurface some of those tidbits.

Where to Go from Here

This book can help you discover more about identity security, but if you want resources beyond what this book offers, check out the SailPoint website — it's a comprehensive resource hub for the latest in adaptive identity and enterprise security. Just head to `www.sailpoint.com`.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Scouting the new battleground of your identity
- Canvassing your digital population
- Discovering why traditional security tools no longer do the job
- Managing the security of autonomous agents
- Establishing trust and security using identity

Chapter 1
Realizing Why Old-School Security No Longer Works

It wasn't that long ago that traditional identity and access management (IAM) was safe: a world where users were primarily human, roles were stable, and access didn't change all that often. Governance? That happened with quarterly reviews, annual certifications, and manual cleanup when it was needed.

This model was built for clarity, predictability, and scale. It was measured in thousands of users and applications. Blue skies and fields of daisies.

Now the skies are stormy and the daisies have blown away. Artificial intelligence (AI) has arrived, and now there's an explosion of nonhuman identities (NHIs) that far outpace human ones. The speed at which access is granted, used, and exploited has been supercharged. Decisions are made at machine scale. AI has enabled specific cyberattacks. And the regulatory pressures are only growing.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

To weather the storms, you need to be prepared, not scared. In this chapter, I start by introducing you to what an identity is and the different types of identities. Next, you see why traditional security tools aren't built to manage all these identity types. Then you find out how modern identity management tools use real-time governance to manage and secure human and non-human identities. I conclude by explaining how employing a modern, adaptive identity strategy calms the storms and makes access to your organizational resources predictable and trustworthy.

Understanding the New Battleground: Your Identity

An *identity* is the central and authoritative digital profile in an organization. This single entity aggregates all distinct accounts, access rights, and attributes across enterprise systems and applications.

The definition of "who" is being rewritten as we speak, with machine and AI agent identities quickly overwhelming human ones. Every one of those identities, whether human, machine, or AI agent, represents a path to your critical data and systems.

Today's modern enterprises are grappling with the explosion of identities, especially the growing dominance of non-human identities. Organizations just like yours are now dealing with a vast digital workforce that operates and makes decisions at a scale beyond human capacity to manage it.

A comprehensive security strategy must see, govern, and secure all of your identities without exception. What about your existing security tools, you ask? Hang tight, because you'll see why they're not fit for modern use in the section "Flying Blind: Why Traditional Security Tools Can't Keep Up."

Counting Your Digital Population: Humans, Machines, and AI

I talked about humans and machines, which sounds like we're living in the world of *The Matrix,* but when it comes to your enterprise security, you need to know the three identities:

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Humans** are the employees or non-employees such as contractors or vendors interacting with your organization.
- **Machine identities** are the service accounts and application programming interface (API) keys that require access to systems to perform their functions.
- **AI agents** (along with machine identities) are the NHI itself; these are autonomous identities that can execute hundreds to thousands of actions per task to achieve a specific goal.

The identity fabric feels almost like a busy airport, with humans, bots, APIs, containers, workloads, and AI agents coming in, staying sometimes for only a few seconds, and then going out again.

This massive digital population isn't just sitting idle. Every day, these identities are creating, sharing, and interacting with an explosive amount of data — documents, spreadsheets, code repositories, and cloud storage. Traditional tools simply cannot see into this "dark data," leaving you exposed.

Flying Blind: Why Traditional Security Tools Can't Keep Up

Today's networks are now borderless — they extend from the cloud to your company's partners to your employees' homes. What's more, there's an average of 45 digital identities for every single human user. And that number is only expected to increase exponentially — some experts say it could reach 1 human to 100 or even 1,000 NHIs in the next few years (yikes).

The explosion in the number of identities isn't the only issue. Security tools must also act quickly because privilege is now created dynamically by agents, APIs, and continuous integration/continuous development (CI/CD) pipelines. This high-speed environment creates three critical gaps:

- **Exposure:** Access exists longer than it should, relative to how quickly it's used.
- **Detection:** Risky or dastardly behavior is identified only after execution from logs and reviews.
- **Control:** Security enforcement can't reliably interrupt misuse in real time.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

And, you guessed it, adding AI into the mix amplifies all three gaps. Agents that act automatically and probabilistically can generate unintended actions on unintended data. These actions often chain across systems, spreading misconfigurations or over-privilege instantly.

So, what's the problem with many current security tools? They're "identity blind." They can't distinguish between legitimate and malicious access because they can't tell *who* is behind the access request. That leads to bad juju: Ninety percent of all data breaches involved a compromised identity.



REMEMBER

Current security tools treat identity and security as separate disciplines, but the only way forward to unify them is by using identity context to make smarter and faster security decisions.

Installing Real-Time Governance for Humans and Autonomous Agents

The governance models within traditional identity security tools are completely overwhelmed by AI and machine identities. When you add all the agents, bots, service accounts, workloads, and credentials into the mix, the governance problem becomes unsolvable by humans. No, really — it's mathematically impossible to validate access meaningfully at that scale.

Traditional security tools are built for periodic governance, such as quarterly reviews, but that's as obsolete as an eight-track player is today. Instead of static roles, binary access decisions, and scheduled reviews, adaptive identity brings a bounty of modern features:

- Continuous signal ingestion across identities, behaviors, and environments
- Real-time risk evaluation with every new piece of data that comes in, including entitlements and relationships
- The ability to make dynamic, per-action authorization decisions
- Mid-session enforcement that interrupts risk as it happens
- Continuous, verifiable evidence for every decision

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

This modern approach answers the central identity question as AI adoption grows: "Should this identity perform this action, in this context, right now — and can we prove why?"

Establishing Identity as the Foundation of Trust and Insurability

Everyone in your company needs to be able to trust that the right people have the right access to the right data. (Your leadership expects no less.) A mature and adaptive identity strategy brings resilient infrastructure, simplifies and maintains compliance, and operationalizes the Zero Trust cybersecurity model that's encapsulated by its slogan: "Never trust, always verify."



TIP

If you're trying to convince leaders that an adaptive identity strategy is worth using, remind them that doing so will set up favorable cyber-insurance terms to save the company money. I cover what adaptive identity security is in Chapter 2.

When you're moving from obsolete identity security tools to a modern adaptive identity solution, this new approach comes with four fundamental changes (translate this to significant risk reduction benefits):

- Identity is evaluated continuously with each action.
- Access is governed during execution.
- Zero Standing Privilege (ZSP) and Least Standing Privilege (LSP) are enabled through Just in Time (JIT) and Just Enough Access (JEA).
- Every access decision produces traceable, explainable records.



REMEMBER

What are all these acronyms, anyway? They're cybersecurity frameworks you need to know, so let's cover them (or review them in case you need a refresher):

- **Zero Standing Privilege:** Identities have no default privileges. Access is granted only temporarily for a specific task and is gone the moment a task is done.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Least Standing Privilege (LSP):** Identities are granted the absolute minimum "always-on" access needed for basic, low-risk daily tasks. Any sensitive or elevated tasks require temporary, dynamic access.
- **Just in Time:** This is the mechanism for ZSP and LSP. It dynamically grants privileges to human, machine, or AI identities for a limited time, only when needed and revokes permissions immediately after the task is completed.
- **Just Enough Access:** This principle ensures that any access granted — whether standing or temporary — is the bare-minimum required to do the jobs. No more, no less.

This is all to provide both the feeling and the knowledge that you can trust and ensure that the right people and non-humans have the right access at the right time. But wait, shouldn't you use human-centric policies to do that? After all, humans need to control the security tools, don't they?

Yes and no. You can't apply human-centric policies to non-human machine and AI agents and expect them to work the way you want them to. That's why an adaptive identity solution gives you the power to manage these agents responsibly:

- **Visibility:** You can't secure what you can't see. The first step is to discover and catalog every machine and agent identity across all your cloud and on-premises environments.
- **Ownership:** Every agent needs a human owner who's accountable for its actions and its access rights. This creates a clear line of responsibility.
- **Lifecycle:** Like humans, machines and AI agents have a lifecycle. These need to be provisioned securely, their access must be certified periodically, and they must be properly decommissioned. This entire lifecycle must be governed and auditable.
- **Real-time authorization:** Identities should operate under the principle of least privilege. This means granting access with JIT and JEA authorization based on policy, context, and the specific task.

In sum, the goal of an adaptive identity system is to keep up with agent builders without becoming the bottleneck, while making all identities, including machines and AI agents, visible, owned, governable, and safe in real time.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Introducing adaptive identity and the SailPoint platform
- Moving from static identity governance to continuous evaluation
- Learning how to think with context
- Implementing strategies to defeat attackers
- Knowing the core principles for today's agentic economy

Chapter 2
Defining Adaptive Identity: Security That Thinks

You've felt the fundamental shift. Now we're at a pivotal moment in enterprise security created by agentic artificial intelligence (AI) — that is, AI that can act independently and make its own decisions — pressure-testing traditional identity security models like never before. AI isn't just a tool anymore, but an active participant in decision-making and operations.

For enterprise organizations like yours, security must adapt, or you'll find your business on the corporate "endangered species" list. (The choice really is that stark.) For years, SailPoint has been at the forefront of putting identity as the core of security. But now AI has pushed that discussion to higher prominence.

You can guess why: AI has rewritten the very definition of "who" in enterprise security. Adaptive identity is the new standard for

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

enterprise security because that identity adapts deftly to the challenges AI agents pose.

In this chapter, I start by going into detail about how SailPoint approaches adaptive identity in its platform. Specifically, you see how this modern approach bridges identity, data, and security by using deep context to inform every security action. Then you find out why adaptive identity requires continuous, real-time governance. Next, you see how adaptive identity thinks with much broader context to keep access under control.

This change in enterprise security is vital to keeping out attackers, and I follow up by telling you how attackers think and how adaptive identity foils their dastardly deeds. Finally, I wrap up with a discussion of the core principles in today's agentic economy.

Discovering Adaptive Identity

Adaptive identity is an advanced security strategy that continuously evaluates and adjusts access decisions based on real-time behavior, context, and risk. At its core is integrative identity context, which brings together identity, data, and security signals in your network.

This isn't just about replacing traditional identity and access management (IAM) — it's about a new approach that protects enterprises against credential-based attacks, token hijacking, and unauthorized lateral movement.



REMEMBER

Lateral movement happens when attackers use stolen credentials or hijacked sessions to blend in with legitimate user activity. Then they can pivot across your network or cloud tenants to escalate their privileges and wreak havoc.

A true adaptive identity solution has four defining characteristics:

- **It's built on context.** Identity-first, data-first. Both identity and data context inform security actions.
- **It uses dynamic access models.** SailPoint includes support for modern just-in-time approaches — including real time — because static privileges are no longer sufficient with traditional IAM solutions.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **It's integrated with security operations.** Breaches and threats can be addressed inside the security operations center (SOC) with real-time response and remediation.
- **It has intelligence embedded.** SailPoint weaves AI and machine learning into its very fabric to protect and respond to risk.

These aren't just theoretical concepts — they're the core design principles of the SailPoint adaptive identity platform.

Moving from Snapshots to a Live Video Feed

Access isn't static, it's dynamic. All agent interactions — agent–agent, agent–user, and agent–tool — needs to be evaluated by your identity security platform in real time. AI has made that shift vital, and it's becoming more common to see media reports of AI agents that accessed or shared inappropriate data.

Despite all the change that AI and other machine agents have brought to enterprise security, many organizations are still governing the same way they did 15 years ago: high-volume, point-in-time, human-driven certification campaigns.

It's like taking snapshots of governance, but this approach is dangerous in the age of AI. What's needed is continuous evaluation of identity access and risk signals, like a live video feed that shows risk as it's happening.

The SailPoint platform offers a maturity journey that allows organizations to move from traditional access governance to one that's continuous, intelligent, adaptive, and real time.

Your cybersecurity likely isn't starting from zero. You probably already have certification programs, auditors, and governance processes in place. So, what does that mean for your existing governance when you adopt the SailPoint platform?

Certifications will continue to exist, but their role must fundamentally change. Access governance can no longer be defined by high-volume, checkbox-driven reviews. It has to evolve into an operational security system that acts as that live video feed.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

But that evolution happens in phases. Not everyone needs to reach the final phase immediately. Your company may stop halfway or move faster in one area than another. Every business is different, but the goal is the same: Each phase moves you closer to policy-driven, risk-aware, machine-scale governance.

Thinking with Context: Who, What, When, Where, and Why

Access is dynamic because access paths aren't ladders you can climb anymore — they're webs that have indirect relationships, inherited rights, and fleeting privileges contained in the lattice. That's because in the modern workplace, users and machines move fluidly across roles, context, geographic locations, and risk states — often within a single session.

This results in a mismatch because traditional and modern IAM approaches answer different questions. Traditional IAM answers the question, "Who are you and what are you allowed to access?"

What's more, traditional IAM governance models fall short of today's business needs in several ways:

- **Volume:** Reviewers are routinely asked to evaluate hundreds or even thousands of line items in a single batch of risk assessments. The human brain looks for the fastest way to complete the task. After all, if the line items you find are okay, the rest are, too, right? (Spoiler alert: No.)
- **Focus:** At the point of certification, the same person who approved the access request certifies it. The lack of policy or roles, as well as human-derived decision-making at the point of policy administration and certifications, results in over-provisioned, over-privileged, standing access.
- **Context (and the lack thereof):** Reviewers are asked to answer a deceptively simple question: "Should this access still exist?" And yet most reviewers don't have context. They don't know who needs access to what, what the entitlement actually does, and how access was granted. And they certainly don't have environmental context like access history and changing conditions.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

» **Timing:** Certifications either run too often and exhaust the business (as well as the people in them), or they don't run often enough and miss massive amounts of change — and risk. For environments where access changes often, sometimes hourly, point-in-time reviews are always behind reality.

A modern platform evaluates the context of every access request by looking at signals like user behavior, data sensitivity, location, and time of day to create a risk score. Based on the score, the system can approve a low-risk request, require multifactor authentication for a medium-risk one, or block a high-risk attempt and create a security alert.

Getting Ahead of the Attacker

As you've read this chapter so far, you've likely had the sense that identity is the new attack surface and a modern adaptive identity platform is the key to staying one step ahead of attackers. However, in many organizations — probably even yours, which is why you're reading this book — there's a fundamental disconnect in how to manage that surface.

The disconnect comes because the identity and governance teams and the security and SOC teams work off of different data, use different tools, and speak different languages. It's this gap that attackers exploit every day, because the time lost translating information between these teams is time the attacker uses to move deeper into your network.

Another structural defect is that, as defenders, we're trained to see the world in siloed asset lists of users, entitlements, and applications. It's impossible to surface the hidden connections between these lists. But an attacker doesn't see your business that way at all. They see a map. They see a graph of relationships.

When an attacker sees a low-level service account, they see that the account, though a series of forgotten, nested permissions, has a direct pathway to your production database — or your CEO's inbox. That's the path of attack.

This is the attacker's advantage. An adaptive identity platform is designed to remove that advantage, giving you the same clarity to see the hidden paths to your critical data — and close them.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Understanding Core Principles for the Agentic Economy

A modern adaptive identity platform like SailPoint leverages predictive AI to anticipate and spot risks from digital agents and automatic responses to create an AI immune system. That is, AI creates self-governing guardrails, prevents breaches, and is ethically aligned without human intervention.

This approach creates an *agentic economy*, where autonomous AI agents act on their own and as primary decision-makers. They execute tasks, negotiate contracts, and transfer value with minimal human oversight.

I can already feel your unease about having AI take over from humans, but SailPoint has established six foundational principles that help ensure a secure, compliant, and trustworthy AI ecosystem:


REMEMBER

- **Clear human ownership:** Every AI agent must have a designated human owner who is responsible for its actions.

  Accountability is critical because no agent should be allowed to change its owner on its own while trying to achieve its goal.
- **Real-time agent ledger:** Every action the agent takes must be recorded in a real-time ledger, which provides an auditable record for compliance and forensic analysis.
- **Continuous risk evaluation of all agent interactions:** All agent interactions need to be evaluated for risk in real time with privileges automatically adjusted to prevent misuse.
- **Real-time authorization:** A zero trust approach is enforced for every action, granting the minimum privilege required for a task only for the time it is needed.
- **Cryptographic verification:** Every critical agent interaction needs to be cryptographically verified to ensure the integrity and authenticity of all communication.
- **Agent moral code:** As a final safeguard, a moral code provides a set of core ethical and operational rules, guiding agent actions to ensure alignment with company values and policies.

These tenets are the bedrock of a modern identity security strategy for the agentic era and create a North Star for the SailPoint Agentic Fabric, which I talk more about in Chapter 4.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Moving to always-on governance
- Safeguarding your digital workforce
- Terminating standing privilege access
- Connecting identity and threat detection in the SOC

Chapter 3
Introducing the Four Essential Elements of Adaptive Identity

Think of adaptive identity not as a single feature, but as the complete, intelligent safety system in a modern car. It's built on four essential elements that work together to protect the occupants:

- **Element 1 (Always-On Governance):** The Traction Control System, which is always monitoring the wheels for slip and making constant, tiny adjustments to maintain grip.
- **Element 2 (Unified Identity Security):** The Central Computer, which knows about every part of the car — the engine, the brakes, the airbags, the passengers — and governs them from one place.
- **Element 3 (Ending Standing Privilege):** The Automatic Emergency Braking, which doesn't keep the brakes on all the time, but applies them instantly just in time to prevent a collision.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Element 4 (Bridging to the security operations center, or SOC):** The Onboard Diagnostics, which instantly alerts the driver (the SOC team) with specific information the moment a problem is detected.

In this chapter, I talk about each of the four elements, starting with the shift from static to always-on governance. Next, I talk about ensuring all your identity types — your digital workforce — are secured. Then I cover the concept of standing privilege — or "always on" access — and why ending this risky practice is one of the best things you can do for your security. Finally, you find out about building a bridge between identity and threat detection in the SOC.

Capturing the Shift to Always-On Governance

In the past, governance was an event — a scheduled review, an annual audit. These events were built around a simple joiner-mover-leaver (JML) model of an employee's lifecycle. Access was granted when they joined, adjusted when they moved roles, and revoked when they left.

This model is no longer enough.

Today, access is not a simple path; it's a web of temporary permissions, shared credentials, and machine identities that are created and destroyed in minutes. Waiting for a scheduled "event" to review this activity is like trying to stop a coordinated heist using a security camera that takes only one picture a day.

Always-on governance shifts from scheduled events to a state of constant watchfulness. It's designed to make intelligent decisions between the traditional JML milestones. By using real-time signals, it can ask crucial questions at any moment:

- Has this user's risk level suddenly changed?
- Is this machine identity suddenly trying to access something outside its normal pattern?
- Did this session just become compromised?

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Instead of just cleaning up yesterday's access, always-on governance allows you to respond to risk the second it appears, making your security proactive, not reactive.

Securing Your Digital Workforce

In practice, periodic reviews service compliance more than control and risk management. Indeed, static compliance addresses yesterday's risk and not the security chaos created when machine and artificial intelligence (AI) identities — bots, service accounts, and agents — aren't part of a governance strategy.

And yet non-human identities (NHIs) already outnumber humans in many environments. Non-human identities — including machine identities like service accounts and cloud workloads, alongside autonomous task-executing large language model (LLM)–based AI identities — hold increasing privileges.



REMEMBER

If your machine and AI identities are managed separately from human identities, this siloed approach creates massive blind spots, inconsistent policies, and the inability to get a clear picture of access across the organization. It's not a matter of if a breach will happen, but when.

The only effective solution, like SailPoint provides, is to bring all identity types — human, machine, and AI — under a single, unified governance platform. Governance defaults to Zero Standing Privilege (ZSP) and Least Standing Privilege (LSP), allows Just in Time (JIT) access for need, and applies Just Enough Access (JEA) for scope.

When an agent expresses high-risk intent, such as a destructive or cross-boundary operation, a human in the loop uses an approval and curation tool to curb excessive agency but maintain speed.

This approach makes your life far easier: You get a complete 360-degree view of all your identities, simplified management, and the ability to apply consistent, intelligent security controls for your entire workforce. How does that compare to what you're doing now?

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Ending Standing Privilege Access

I talked about machine and AI identities holding increasing privileges in the previous section. When you hear "privileged access," your mind may think of the IT admin with the keys to the kingdom. Though that was so in the past, privilege is everywhere today.

It's not just in your infrastructure and on-premises data centers. It's in your software as a service (SaaS) applications. In your multi-cloud centers. In your critical data environments. And they're all held by AI agents making automated decisions and service accounts running your core business processes.

Privileged access is one of the biggest drivers of security risk. Most organizations try to solve this in pieces, but SailPoint's modern platform manages privileged access in one of three ways:

- **Least privilege**: The goal with least privilege is to minimize the blast radius of mistakes or compromises by ensuring that every identity has only the access it needs. SailPoint maintains least privilege over time, not just during audits.
- **Zero Standing Privilege:** This means no identity has access it isn't actively using. SailPoint helps ensure that powerful privileges exist only when needed and only for as long as needed.
- **Zero Trust:** This framework is built on a philosophy that's a twist on an old Russian proverb, "Trust, but verify." In the case of zero trust, the mantra is, "Never trust, always verify." Zero Trust presumes no access is implicitly trusted, and access by every agent must be continuously authorized.

In practice, this approach looks like short-lived elevation, transient credentials for services and agents, allow-listed tools for AI, and approvals when risk or intent crosses a boundary. This doesn't mean standing access can't remain for some things. For example, end-user email access can remain standing where appropriate, but the SailPoint approach shifts decisively toward short-lived, scoped privilege, especially for NHIs.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Bridging Identity and Threat Detection in the SOC

SOC teams need a lot to do their jobs. They need identity telemetry and an identity graph that shows where risk sits and the potential blast radius. They also need drift and privilege use that's mapped to known attacker techniques such as lateral movement and escalation patterns. If that's not enough, they need control levers to interrupt threats mid-session. (Didn't know your SOC team did all this? Consider showing your appreciation by buying them their favorite beverage.)

Pairing identity threat detection and response (ITDR) with adaptive identity's control plane reduces time-to-contain as well as backs investigations with decision lineage so your SOC team's response is both fast and explainable.

SailPoint pushes rich identity context and agent activity logs to your security information and event management (SIEM) and security orchestration, automation, and response (SOAR) platforms to compress investigations from days to only minutes.

By integrating deeply with your security tools, an adaptive identity platform like SailPoint can:

- **Automate rapid containment.** When a threat is detected, access can be automatically revoked in real time.
- **Trigger intelligent responses.** Based on risk signals, the system can step up authentication requirements or downgrade privileges instantly.
- **Provide clear decision history.** It gives your SOC team a complete, auditable record of every decision, compressing investigation times from days to mere minutes.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Creating a partnership based on trust and automated response
- Uncovering and charting all your identities
- Installing real-time governance
- Applying dynamic access
- Linking identity to your security ecosystem

Chapter 4
Implementing an Adaptive Identity Strategy

We're at a pivotal moment in enterprise security. The inflection point is agentic artificial intelligence (AI) that's an active participant in decision-making and operations.

For enterprise organizations, the shift that must happen is placing identity at the absolute center of your business and security strategy. An adaptive identity strategy is what makes this shift possible.

This chapter summarizes what it takes to implement your adaptive identity strategy with SailPoint. I start by discussing how SailPoint has built a modern adaptive identity platform based on trust and automated responses. Then I talk about how this platform discovers and maps each identity.

Next, I tell you about how SailPoint establishes real-time governance, followed by a discussion about how SailPoint applies

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

dynamic access to your data. Finally, I explain how SailPoint links identity to your security ecosystem.

Building for Trust and Automated Response

Adaptive identity is about securing enterprises efficiently and effectively in a dynamic world. At its core is integrative identity context: the ability to bring together identity, data, and security signals to provide clarity, control, and scale across every enterprise identity.

The SailPoint platform is built on a specialized foundation designed to govern the new world of AI and automation. Think of it as a dedicated agentic fabric called, unsurprisingly, SailPoint Agentic Fabric, that's built on three core principles:

- **Agents are a new and unique form of identity.** They possess autonomy and persistent decision-making capabilities that transcend traditional access models.
- **Agents can't be governed in isolation, because they interact with humans, machines, and data.** Their risks are interconnected.
- **SailPoint provides a unified control plane to govern all these identity types together.** This ensures consistent policy enforcement and lifecycle management across your entire digital ecosystem.

The number-one question that comes to mind, especially when you think about trust, may be this: "How do I ensure that an AI agent doesn't inadvertently give an employee unauthorized data access or access unauthorized data themselves?" After all, a human user could effectively bypass their own access restrictions by using an AI agent as a proxy to open the cookie jar.

SailPoint's platform, with its integrated Data Access Security capabilities, helps prevent over-permissioning by identifying when human identities get new entitlements or access to sensitive data resources through AI agents. This approach ensures least-privilege tenets are upheld across your company's entire digital workforce.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Discovering and Mapping Every Identity

Organizations were struggling with the sheer volume of identities long before the rise of AI agents. (I see you nodding your head.) But when you add agents, machines, and data into the mix, you have a lot more stuff to govern that just landed in your lap. (No, I'm not spying on you.)

All of this is happening while you're getting pressure to innovate with AI, even though your leaders can't explain what they want with AI, only that they fear being left behind. Hopefully, your leadership understands the need to do so safely so they don't end up on the front page of *The Wall Street Journal* for all the wrong reasons.

SailPoint is built to solve three core challenges your company is facing:

- You want clear and actionable visibility into the permissions for applications and data that humans, machines, and AI agents have.
- You want to drive efficiency and automation to give human and non-human identities the right access to reduce your audit burden.
- You need confidence to embrace the adoption of an agentic identity strategy, and I hope this book is helping you feel assured about the outcome of that strategy.

Establishing Real-Time Governance

To make real-time governance a reality, a critical partnership must be formed between your agent-building teams (the people creating your powerful AI agents) and your identity security teams (the sentinels of your organization's access and data). If you don't have this partnership, then you can't establish real-time AI agent governance. Full stop.

If you're all rowing in the same direction, you can take advantage of real-time governance, which is a key component of SailPoint's adaptive identity strategy. Their vision is access that evolves from periodic, human-driven reviews to a continuous, intelligent,

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

adaptive, contextual, and ultimately autonomous system of risk management.

Mr. Spock would say it's logical to presume your organization is using static governance now. SailPoint has a process for transitioning to a real-time governance model that your organization can implement today. This is achieved by:

- **Rapidly connecting your applications:** Gaining visibility by quickly bringing your critical applications under the governance umbrella.
- **Defining smart access policies:** Establishing clear, intelligent rules for who can access what, and under what conditions.
- **Putting AI to work for you:** Using AI to enrich your access data, making it easier for everyone to understand what an entitlement actually does.
- **Shining a light on your data:** By binding identity and data context, enterprises can ensure that actions — human or digital — are governed by the same permissions and policies. This is essential in a world where agents act on behalf of humans.
- **Bringing everyone along:** Educating stakeholders — from auditors to the CIO — on how this modern approach to governance reduces risk and improves efficiency.


TIP

As SailPoint developed its platform, it worked with auditors to define what access governance meant in the age of access certifications.

After you finish the real-time governance installation process and implement the policies you mapped out, you start bringing non-human identities (NHIs) under control, reduce risk, and secure access.

Enforcing Dynamic, "Right Now" Access

A core feature of an adaptive identity system is replacing "always-on" privileges with dynamic, "right now" access. It acts like an air traffic controller, if you will, for your security tools.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

One important way the SailPoint platform does this is by supporting the Shared Signals Framework (SSF). SSF is a security identity standard that allows different security solutions to talk to each other instantly, sharing and consuming security events and alerts in real time. This framework significantly reduces the time it takes to detect, respond to, and remediate identity-related threats.

This real time, event-driven architecture supports zero trust principles — encapsulated by the maxim "never trust, always verify" — by enabling dynamic access decisions based on the current identity context. There are five components of SSF:

- **Subject:** A user, device, group, or organization about which you want to communicate security events
- **Event:** A security-related occurrence pertaining to a subject, such as when a user's device is no longer compliant
- **Transmitter:** A component within the infrastructure that broadcasts events to other components
- **Receiver:** A security component within the framework that receives and acts on events
- **Stream:** The secure pathway that protects event signals from being tampered with in transit

By incorporating this data and correlating it with identity data, you can detect and respond to threats not just at the point of authentication, but even when the user is in session.

For example, imagine your endpoint security tool detects that an employee's laptop is compromised.

- **Without SSF:** That alert sits in one system. Your identity platform has no idea anything is wrong.
- **With SSF:** The endpoint tool instantly sends a signal — a "distress call" — to every other tool. The identity platform catches this signal and can immediately take action, such as blocking access, forcing a re-login, or even logging the user out of all sessions.

This real-time communication is what enables a platform like SailPoint to make intelligent, contextual decisions about whether someone should have access *right now*.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Connecting Identity to Your Security Ecosystem

The SailPoint Agentic Fabric is built upon a proven foundation designed to deliver intelligence, extensibility, and scale. SailPoint integrates with your existing security tools and executes remediation in several ways:

- It pushes rich identity context and agent activity logs to your security information and event management (SIEM) and security orchestration, automation, and response (SOAR) platform.
- It instantly triggers actions, such as revoking entitlements or disabling the agent identity.
- It integrates with endpoint security to terminate a malicious process, or frictionless controls within the browser session to prevent and redirect actions that fall outside of policies.

And that's not all, SailPoint's connectivity framework delivers thousands of integrations for your SaaS and legacy applications. These integrations provide the ability to discover your full application landscape, onboard new applications, help secure access to your most critical applications, and apply consistent compliance at scale — across your entire landscape. (Now that's all.)

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Chapter 5
Ten Hallmarks of a Truly Adaptive Identity Strategy

As you get ready to discuss the SailPoint adaptive identity platform with your team, leaders, and perhaps helpful SailPoint reps who are ready to chat with you, keep in mind the ten hallmarks of a truly adaptive identity strategy:

- **An adaptive identity strategy is identity-centric, not perimeter-focused.** This is the foundational concept of this book — the security battleground has shifted from the network to the identity.
- **An adaptive identity strategy governs every identity, human, machine, and artificial intelligence (AI) agent.** A true strategy leaves no identity behind, providing consistent governance for employees, non-employees, AI agents, and service accounts.
- **An adaptive identity strategy operates in real time, all the time.** It replaces periodic, after-the-fact reviews with continuous, automated governance that acts the moment a risk appears.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **An adaptive identity strategy unifies identity, data, and security.** It evaluates the context of the identity, the classification of the data, and the real-time security posture to make smarter, more precise access decisions at a scale humans cannot match.
- **An adaptive identity strategy eliminates standing privilege.** It's built on a principle of "just in time" or "right now" access, ensuring no one has access they don't currently need.
- **An adaptive identity strategy is deeply integrated into your security ecosystem.** It doesn't operate in a silo. Instead, it acts as the connective tissue, sharing signals with and receiving intelligence from your other security tools.
- **An adaptive identity strategy is designed to govern actions, not just access.** It looks beyond what an identity can access and focuses on controlling what it can and should do with that access, especially for non-human agents.
- **An adaptive identity strategy is predictive, not just reactive.** It uses data and AI to anticipate and resolve access risks — like a risky separation of duties or a compromised identity — before they ever turn into security incidents.
- **An adaptive identity strategy delivers true zero trust by helping you "verify everything."** It provides the core "never trust, always verify" engine that makes a true zero trust strategy possible by continuously validating every access request.
- **An adaptive identity strategy turns security from a roadblock into a business accelerator.** It gives you the confidence to unleash AI and drive rapid innovation without compromising your security posture.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

SailPoint

Legacy identity won't survive the AI era.
Set a new standard.

You've read the book, now see how to put adaptive identity into practice. With AI projects barreling forward, you can't rely on security that was built for the past. Unify identity, security, and data into a single control plane to confidently secure the rapid influx of AI agents and modern threats.

Put adaptive identity into practice.

sailpoint.com



Secure your agentic future with adaptive identity from SailPoint

Organizations are now dealing with a vast digital workforce that operates and makes decisions at a scale beyond human capacity. SailPoint, a trusted authority in identity security, addresses the challenges posed by the explosion of human and non-human identities; leverages AI to enable real-time, adaptive security; and provides actionable insights for implementing an adaptive security strategy.

Inside...

- Know the new front line: your identity
- Understand adaptive identity
- Secure your digital workforce
- Get ahead of attackers
- Unify access to your identities and data
- Modernize your security
- Make security a business enabler



Eric Butow is the owner of Butow Communications Group (BCG) in Jackson, California. BCG offers writing, online marketing, and website development services. Eric has authored or co-authored 59 books so far, most recently *AI ChatBots For Dummies* and *Instagram & Facebook All-in-One For Dummies*.

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

ISBN: 978-1-394-45826-4
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.