AXIAD

Essential Guide to Managing Risk with Identity Visibility and Intelligence

Protecting the Enterprise with an Identity Visibility and Intelligence Platform (IVIP)

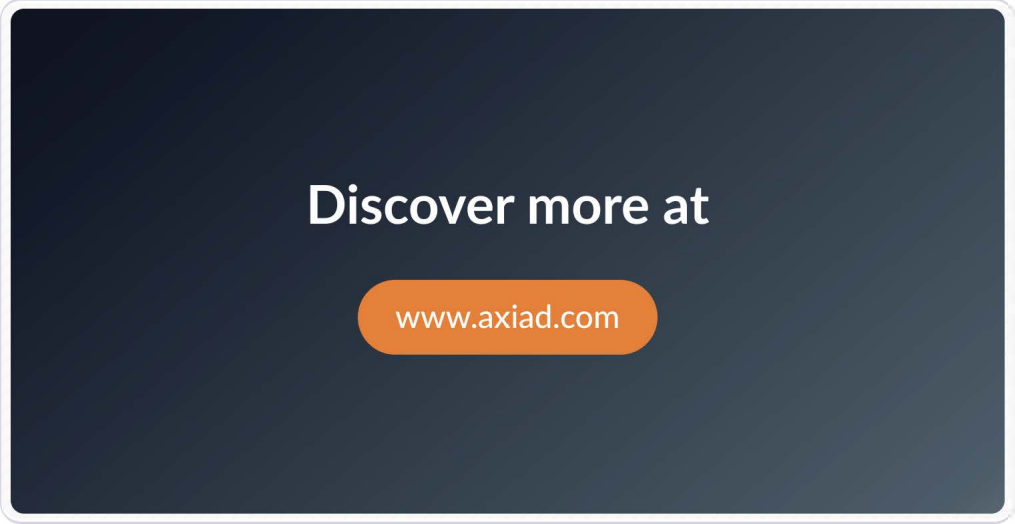
A comprehensive guide to understanding, implementing, and maximizing the value of IVIP for enterprise identity security

About Axiad

Axiad is an identity security company tackling the growing threat of compromised and weak identity credentials, which drive over 70% of enterprise breaches. The sprawl of human and non-human identities across organization silos creates security blind spots that existing tools fail to secure.

Axiad tackles this problem head-on with Axiad Mesh—the first Identity Visibility and Intelligence Platform—detecting identity risks and poor credential hygiene across siloed identity, security, human resources, SaaS, and enterprise resource management systems.

The Axiad Mesh IVIP provides actionable insights to remediate security gaps in the identity attack surface and prepare organizations for postquantum cryptography. Axiad makes identity visibility and intelligence across the entire identity attack surface simple, effective, and real.



Essential Guide to Managing Risk with Identity Visibility and Intelligence

Protecting the Enterprise with an Identity Visibility and Intelligence Platform (IVIP)

© 2025 Axiad. All rights reserved.

Published by Axiad

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the prior written permission of the publisher.

Table of Content

Foreword by David Canellos, CEO of Axiad 6

Introduction 8

Chapter 1: The Identity Visibility Crisis 10

Identity: Today's Pivotal Attack Surface 10

The Visibility Gap 12

Four Reasons Why Identity Visibility Is So Hard 13

The Answer: Unified Identity Visibility and Intelligence 15

Chapter 2: Understanding IVIP 17

What Is IVIP? 17

Key IVIP Capabilities 20

Chapter 3: Where IVIP Fits in the IAM Landscape 22

IVIP Supercharges IAM Prevention Activities 23

IVIP Supports Incident Response 24

What Other Tools Can't Do 24

Chapter 4: Who Should Care About IVIP? 25

Security Practitioners 25

Identity Management Leaders 26

CIOs and CISOs 27

Chapter 5: Discovering Your Identity Attack Surface 28

Discovering and Ingesting Identity Information 28

Correlating Identities 29

Generating Quick Wins 31

Chapter 6: Quantifying Your Identity Risks 32

Risk Scoring for Individual Identities 33

Using MITRE ATT&CK to Quantify Risk 34

Outcome-Driven Metrics 35

Chapter 7: Reducing and Hardening Your Attack Surface 36

Fortifying Identities 36

Overcoming Fear of Fortifying 37

Using AI to Fortify Identities 38

Chapter 8: Selecting the Right IVIP Solution 39

A Brief Checklist 39

Assess the Vendor 42

About Axiad Mesh: The First IVIP 43

Foreword

by David Canellos, CEO of Axiad

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

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

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

Current IAM systems were simply not designed to address these emerging risks. A more comprehensive approach to identity security is necessary—one that provides unified visibility across all identity systems and delivers the intelligence needed to prioritize and remediate risks.

This is precisely why Gartner introduced the Identity Visibility and Intelligence Platform (IVIP) category in 2025. And it's why we built Axiad Mesh—to deliver on the IVIP vision before it even had a name.

This guide introduces the fundamental concepts of IVIP and explains how it addresses the visibility gaps that have plagued IAM programs and security teams for years. You'll learn how a unified, intelligence-driven approach can not only protect identities but also strengthen your organization's overall security posture.



David Canellos
CEO, Axiad

Introduction

Today, countless identities are continually dispersed across an enormous variety of systems and platforms. Industry analysts call this "the identity boom."

This guide outlines how the current identity visibility crisis has been shaped by modern computing trends; provides guidance on how to achieve unified visibility across fragmented identity systems; describes how identity information can be discovered, correlated, analyzed, and quantified; and offers a roadmap to using an Identity Visibility and Intelligence Platform to assess risks and reduce the fastest-growing attack surface: your enterprise identity ecosystem.

Chapters at a Glance

Chapter 1, "The Identity Visibility Crisis," discusses why identity security is so challenging and outlines the visibility gaps that existing IAM tools cannot address.

Chapter 2, "Understanding Identity Visibility and Intelligence Platforms," explains what IVIP is, why Gartner created this category, and how it differs from traditional IAM tools.

Chapter 3, "Where IVIP Fits in the IAM Landscape," explains how IVIP solutions strengthen AM, PAM, CIEM, IGA, and other IAM functions without replacing them.

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

Chapter 5, "Discovering Your Identity Attack Surface," discusses how IVIP solutions discover, ingest, and correlate identity data across the enterprise.

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

Chapter 7, "Reducing and Hardening Your Identity Attack Surface," highlights how IVIP helps organizations improve remediation and attack surface hardening.

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

CHAPTER 1

The Identity Visibility Crisis

In This Chapter

- Review why the identity attack surface is the pivotal battleground for threat actors and security teams today
- Examine why existing IAM tools create visibility gaps
- Understand the scope of the identity visibility crisis

> "You can't protect what you can't see."
>
> — *Security industry maxim*

Identity: Today's Pivotal Attack Surface

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

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

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

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

The proof?

Statistics show that identities and identity-related information are key tools in most major cyberattacks today:

- The 2025 Verizon Data Breach Investigations Report identifies credential misuse as the dominant method attackers use to compromise organizations.
- The Identity Defined Security Alliance reports that 91% of organizations experienced one or more identity-related breaches in the last year.
- Of the 14 tactical areas described in MITRE's ATT&CK framework, five include multiple techniques for compromising and exploiting identities.

The Visibility Gap

Despite major IAM advances—significant investments in IGA, PAM, CIEM, and access management tools—residual blind spots persist. Organizations have spent billions on identity security, yet still struggle to answer basic questions like:

- "Who has access to our most critical systems?"
- "How many dormant accounts exist across our environment?"
- "Which service accounts have excessive privileges?"
- "Are all our identities protected by MFA?"

The problem isn't a lack of tools. The problem is that each tool operates in its own silo, creating fragmented visibility that leaves security teams flying blind.

Key Definitions

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

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

Four Reasons Why Identity Visibility Is So Hard

1. Identity Information Is Scattered Everywhere

Identity information includes user identities and their attributes, accounts, entitlements, credentials, and secrets like keys and tokens used for validation and encryption.

In a typical enterprise, these items are scattered across:

- Directories and identity management systems
- Password and secrets managers
- Workstations, servers, and other devices
- On-premises applications
- Cloud platforms
- "Shadow IT" cloud applications and services

Because so many identities are poorly tracked, most organizations have no way to assemble a complete picture of the identity information for any person or machine.

2. Silos Disrupt Prevention and Remediation

IT and security teams devote much time and effort to finding and remediating vulnerabilities, misconfigurations, and issues that expose identity information. Unfortunately, they perform most of these activities in silos—identity management systems, cloud operations systems, endpoint management tools, software development environments.

> **⚠ CAUTION**
>
> Teams waste time and effort on tasks that are seemingly urgent but are actually a low priority for the enterprise as a whole. At the same time critical risks are ignored because the impact of the problem is unseen. Without unified visibility, you can't prioritize effectively.

3. Advanced Technologies Have Increased Complexity

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

4. Machine Identities Change the Game

Machine or non-human identities (NHIs) are a special case of advancing technologies that increase identity management challenges. Machine identities vastly outnumber human identities with industry estimates ranging from 45:1 to as high as 100:1 in large enterprises.

TECH TALK

Machine identities can be software entities such as workloads, service accounts, APIs, AI entities, automation tools, and robotic process automation (RPA) services or physical devices, including workstations, servers, personal devices, internet of things (IoT) devices, and industrial systems.

The Answer: Unified Identity Visibility and Intelligence

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

There is a way. Gartner calls it an Identity Visibility and Intelligence Platform (IVIP).

IVIP is a new technology category that enables security and identity management teams to:

- Discover and consolidate identity data across connected and disconnected systems
- Enable advanced identity analytics to understand relationships and expose hidden privilege paths
- Improve integrated identity, security, and business controls
- Remove ambiguity for distributed teams by quantifying risk levels
- Shrink the identity attack surface demonstrably over time
- Support Zero Trust implementation
- Enable automated remediation with appropriate human oversight

DON'T FORGET

IVIP doesn't replace your existing IAM investments. It makes them more effective by providing the unified visibility layer they've always lacked.

CHAPTER 2

Understanding Identity Visibility and Intelligence Platforms

In This Chapter

- Learn what IVIP is and why Gartner created this category
- Understand key IVIP capabilities
- Consider why IVIP is the foundation for an identity fabric

> "What we know matters... but who we are matters more."
>
> — *Brené Brown*

What Is IVIP?

In July 2025, Gartner formally introduced Identity Visibility and Intelligence Platforms (IVIP) as a distinct category in the Hype Cycle for Digital Identity.

According to analysts, IVIPs are:

> "Products that provide rapid integration and visibility for identity and access management (IAM) relevant data, typically paired with advanced analytics (often AI-enabled) capabilities. This innovation provides a single view of IAM data, activity/events, relationships, configuration and posture to enable rapid improvement of all other integrated IAM controls and capabilities supporting both improved security and business enablement."

In simpler terms:

IVIP gives you the visibility your IAM stack never could.

The emergence of this category addresses several converging forces:

- The explosion of non-human identities: Machine-based identities now significantly outnumber human users
- The inherently siloed nature of IAM: The adoption of cloud and SaaS blew up the enterprise perimeter
- Credential abuse as the top attack vector: Attackers consistently exploit weak credentials
- The shift from episodic to continuous IAM: Continuous visibility has become essential
- The impossibility of Zero Trust without visibility: You must know what identities exist

IVIP Is Not Another Directory

It's important to understand what IVIP is not. As Gartner explicitly states, these platforms are distinct from a traditional user or metadirectory.

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

DON'T FORGET

IVIP acts as an intelligence layer that makes sense of the identity data you already have scattered across your environment. It doesn't replace IGA, PAM, or CIEM— it makes them all more effective.

Key IVIP Capabilities

Unified Identity Discovery

Automatically discover and catalog every identity across your enterprise—from Active Directory and Azure AD to AWS, GCP, SaaS platforms, and on-premises systems.

Intelligent Risk Scoring

AI- and ML-powered analytics continuously assess identity risk based on permissions, behavior, access patterns, and toxic combinations.

Real-Time Posture Intelligence

Monitor identity configuration and security posture in real-time across all IAM controls. Detect drift and misconfigurations when they occur.

Non-Human Identity Visibility

Finally gain control over the identity explosion: service accounts, API keys, OAuth tokens, certificates, cloud roles, and AI agents.

Rapid IAM Integration

Connect your existing IAM stacks—CMDB, HRMS, IGA, PAM, CIEM, directories, and SaaS apps—in days, not months.

Advanced Analytics and Reporting

Transform raw identity data into executive-ready insights with risk scores and financial risk analysis.

Automated Remediation

Don't just identify risks—fix them. Trigger automated workflows and orchestrate access reviews directly through your existing IAM controls.

TIP

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

CHAPTER 3

Where IVIP Fits in the IAM Landscape

In This Chapter

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

> "Coming together is a beginning, keeping together is progress, and working together is success."
>
> — *Henry Ford*

IVIP Doesn't Duplicate Existing IAM Processes

IVIP does not duplicate or displace existing components of IAM. Rather, it ingests and analyzes data from many identity-centric sources and IAM systems, enriches the data, and provides tools, reports, and risk scores that can be used by security practitioners and managers across many IAM disciplines.

IVIP Supercharges IAM Prevention Activities

Industry analysts divide IAM defenses into "prevention" and "detection and response" layers. Activities in the prevention layer are concerned primarily with identity hygiene and identity security posture management (ISPM).

Reducing the Identity Attack Surface

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

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

IVIP solutions give identity management and security teams expanded visibility that crosses silos, as well as new analytic tools. These features help them find and remediate more vulnerabilities and policy violations.

IVIP Supports Incident Response

IVIP solutions can assist SOC analysts and incident responders in containing attacks and remediating the conditions that allowed them:

- If a user's passwords have been compromised, IVIP could find other identities and accounts associated with the same user
- If an attack exploits a particular vulnerability, IVIP can show other places with the same issue
- If IVIP detects sudden privilege escalation, it can alert analysts to potential account manipulation

What Other Tools Can't Do

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

- Ingest, normalize, and correlate data from multiple identity sources
- Provide contextual information from across the enterprise
- Assess risk using a consistent methodology across the enterprise
- Provide a global picture of identity risk posture
- Provide financial impact analysis of identity risk

DON'T FORGET

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

CHAPTER 4

Who Should Care About IVIP?

In This Chapter

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

> "By 2028, 70% of chief information security officers (CISOs) will utilize an identity visibility and intelligence platform (IVIP) to shrink their IAM attack surface."
>
> *— Gartner Strategic Planning Assumption*

Security Practitioners

IAM Teams

Most people in IAM spend time managing processes for onboarding and provisioning users, granting appropriate entitlements, ensuring privileged users are protected, and monitoring user access.

These teams can use IVIP solutions to identify:

- Users with excessive privileges
- High-risk accounts (orphaned or dormant)
- Users associated with multiple uncorrelated identities
- Identity information stored in insecure locations
- Violations of identity security policies

OT, IoT, and DevOps Security Teams

People responsible for security in operational technology (OT), industrial control systems (ICS), IoT devices, and development operations (DevOps) often lack tools for systematically managing machine identities. IVIP solutions can help them uncover identity-related risks.

Identity Management Leaders

IVIP solutions can help chief identity officers, VPs of IAM, and enterprise security architects:

- Improve the productivity and effectiveness of their teams
- Identify and isolate identity risks across on-premises, multi-cloud, and hybrid infrastructures
- Prioritize remediation activities based on global risk comparisons
- Share identity information and promote collaboration among teams
- Increase consistency of IAM processes across business units

CIOs and CISOs

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

- Accelerate cloud transformation by identifying and reducing identity-related risks
- Mitigate staff shortages by increasing productivity of existing teams
- Prevent many identity-related attacks and contain others more quickly
- Assess business acquisition targets for identity risk issues
- Document compliance with identity-related frameworks and standards
- Assess, quantify, and report to the CEO and board on risk levels

Who Needs IVIP?

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

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

CIOs and CISOs who want to secure the organization's identity attack surface to protect its intellectual property and brand

CHAPTER 5

Discovering Your Identity Attack Surface

In This Chapter

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

> "Things don't turn up in this world until somebody turns them up."
>
> *— James Garfield, 20th President of the United States*

Discovering and Ingesting Identity Information

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

- Human resources management systems (HRMS)
- Enterprise and cloud identity directories
- Privileged access management (PAM) and identity governance (IGA) products

- Cloud-based and legacy identity providers (IdPs)
- Security products such as XDR and SASE tools
- SIEM and SOAR products
- Machine identity management solutions
- Certificate lifecycle management services
- SaaS applications and API-based services

IVIP solutions can also discover identity information from places where it shouldn't be, such as unauthorized shadow IT services and identity dump sites on the Dark Web.

DON'T FORGET

What makes IVIP solutions different from other security analytics products is optimizing discovery, ingestion, and normalization for identity-related information. All the analytic power in the world won't help unless you have comprehensive data in standardized formats.

Correlating Identities

The next step is correlating identity information from all relevant systems to generate a comprehensive and definitive identity for each person and machine in the enterprise.

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

- All known identities and their organizational units
- Suspected additional identities ("shadow identities")
- Attributes, including technical information like devices, IP addresses, location
- Credentials, entitlements, and permissions
- Policies and controls

Drilling Down to Uncover Issues

By correlating identity information and providing tools to drill down into details, an IVIP solution can enable identity management teams to immediately identify security issues and policy violations.

Discovering and comparing identity information can point to identities that are problematic because they are:

- Stale or dormant – unused for a long time, probably unnecessary
- Inconsistent with similar identities – lacking attributes typical of similar roles
- Uncorrelated with any other identity – without provenance, more likely to belong to threat actors

Generating Quick Wins

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

- Reducing risk and company spend by highlighting identity-related vulnerabilities
- Saving identity and security teams hours otherwise spent collecting data
- Determining the organization's current identity security compliance level and financial risk

CHAPTER 6

Quantifying Your Identity Risks

In This Chapter

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

> "You can't run a business without taking risks."
>
> — *Millard Drexler*

Quantify to Compare and Prioritize

An organization takes a great step forward when it can comprehensively map identity information and identify the risks. But the essential next step is to be able to quantify the risks so security teams can:

- Compare and rank identities so the highest-risk ones can be remediated first
- Aggregate and visualize risk by platforms and groups
- Calculate enterprise-wide identity risk all the way up to the entire organization

TIP

You should have a common scale for identity risks across your enterprise. The best way to rank them is usually with numerical risk scores—for example, on a scale of one to 10 or one to 50.

Risk Scoring for Individual Identities

The risk to an enterprise associated with an individual identity is determined by:

- The identity's exposure to compromise
- The controls in place to protect it (or lack of them)
- The extent of its access to critical resources (its "blast radius")
- Its likelihood of being targeted by threat actors
- Indicators of compromise activity outside the organization

IVIP solutions can assess risk based on many factors:

- Being privileged (access to critical applications, data, or infrastructure)
- Being orphaned, stale, dormant, or never used
- Being overprivileged relative to peers' identities
- Missing key attributes (e.g., no manager for people, no owner for workloads)

- Missing credentials or using weak passwords
- Using phishable or easily spoofed credentials
- Having missing, misconfigured, or inconsistently applied controls
- Being associated with compromised identities

Using MITRE ATT&CK to Quantify Risk

The MITRE ATT&CK framework highlights many adversary tactics and techniques that focus on exploiting weaknesses in identity security. About half of ATT&CK tactics rely heavily on compromising identities:

Initial Access

Using legitimate credentials to access accounts through misusing valid accounts, phishing, and exploiting external-facing services.

Persistence

Maintaining long-term access by modifying credentials, permissions, or group memberships to preserve access.

Privilege Escalation

Gaining higher-level permissions using compromised credentials and exploiting misconfigurations in role assignments.

Credential Access

Getting access to credentials through brute force, credential dumping, keylogging, and phishing.

Lateral Movement

Moving across systems using remote services with valid credentials and exploiting trust relationships.

Outcome-Driven Metrics

Outcome-driven metrics (ODMs) focus on results rather than outputs.

Key ODMs for measuring IAM attack surface progress include:

- Reduction in orphan/dormant accounts – Eliminates legacy access that threat actors can exploit
- Increased use of phishing-resistant credentials – Eliminates weak credentials
- Reduce financial annual loss expectancy – Using FAIR framework analysis
- Compliance audit pass rates – Ensures continuous compliance
- Reduction in access-related security incidents – Indicates improved security posture

CHAPTER 7

Reducing and Hardening Your Identity Attack Surface

In This Chapter

- Examine the ways that IVIP helps organizations improve and automate remediation
- Understand how to overcome "fear of fortifying"
- See how IVIP can leverage AI to fortify identities

> "Hardening is the practice of making a system or application more secure than its default configuration."
>
> *— Darril Gibson*

Fortifying Identities

Global Visibility and Prioritization

IVIP enables identity and security teams to find identity-related risks they would have overlooked, and to prioritize remediation tasks both within groups and globally. It helps them see the groups with the most risk so they can determine root causes and apply resources where they will have the greatest impact.

Enriching Remediation

When SOC and identity management teams receive alerts about vulnerabilities, they often spend considerable time gathering information to determine if the alert is a false positive. An IVIP solution can enrich the data analysts use to make these decisions, providing critical context and recommendations so analysts can make judgments faster and more accurately.

Automating Remediation

IVIP solutions can be configured to send alerts and contextual information to SOC and identity management teams. In appropriate circumstances, IVIP systems can perform remediation automatically:

- Revoke permissions
- Revoke certificates
- Suspend credentials
- Force new credential issuance
- Revoke just-in-time access to applications or platforms

Overcoming Fear of Fortifying

Managers responsible for identity and security management sometimes develop a "fear of fortifying"—a reluctance to fully automate remediation because they might disrupt business processes. These are valid concerns.

However, it is important to balance the "risk of breaking internal things" with real external risks. Ways to smooth the path toward reliable automated remediation include:

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

Using AI to Fortify Identities

As IVIP solutions mature, they will incorporate AI in more activities:

- Gather and analyze more data to make better remediation decisions
- Recommend appropriate permission levels based on peer groups
- Generate punch lists to guide identity teams
- Detect overprovisioning by comparing identities for similar users
- Correlate types of identity risks with observed security incidents
- Suggest additional monitoring and controls for greatest impact
- Propose immediate remediation for detected high-priority events

TIP

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

CAUTION

Organizations that try to systematically reduce and harden their identity attack surface without IVIP are essentially flying blind, or at least severely visually impaired.

CHAPTER 8

Selecting the Right IVIP Solution

In This Chapter

- Review a checklist of criteria for selecting an IVIP solution
- Understand how to assess IVIP vendors

> "Make good choices."
>
> — *Your mother*

How to Find Your IVIP Solution

An IVIP solution acts like a unifying layer for the disparate elements of an identity management program. It gathers data from all corners of the identity ecosystem, provides a forum to share information, and generates plans to make identities safer.

A Brief Checklist

Ability to Leverage Existing Investments

IVIP should not duplicate or displace existing IAM tools. You should be able to leverage the full value of current investments, prevent overlapping processes, and avoid affecting computing infrastructure performance.

A Wide Range of Integrations

IVIP solutions should discover and ingest identity information from a wide range of sources.

Look for products that:

- Offer out-of-the-box integrations with popular IAM and security tools
- Work with APIs and frameworks such as OCSF, RISC, IPSIE, and CAEP

Enterprise-Wide Visibility

Many identity security issues can be detected only by creating a comprehensive picture of identity information across the entire enterprise. Ensure solutions can normalize, correlate, analyze, map, and search all that information together.

Enterprise Scalability

IVIP must ingest and correlate large amounts of data from the start and scale to handle massive volumes over time. Analysis and remediation need to be performed quickly so teams can stay ahead of threat actors.

Meaningful Risk Scores

IVIP solutions should create risk scores that are easy to interpret, reflect a wide range of meaningful factors, and can be used to rank and compare risk levels of both individual identities and groups.

Value for Many Teams

Look for IVIP solutions with tools to help all groups—IAM teams, SOC analysts, auditors, identity leaders, and executives—visualize risks, drill down on details, understand relationships, and analyze financial risk impact.

Assess the Vendor

IVIP is evolving rapidly. Look beyond current features to assess the vendor's ability to meet your requirements over time:

- Does the vendor have a track record of integrating multiple IAM technologies?
- Is the vendor a thought leader and innovator in this field?
- How does the vendor's vision and roadmap align with your needs?
- Does the architecture support scalability and flexibility?
- Is the vendor committed to interfaces and standards that future-proof your investment?
- Does the vendor have a great track record in customer support—and are customers happy?

DON'T FORGET

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

About Axiad Mesh: The First IVIP

While Gartner defined the IVIP category in July 2025, Axiad has been pioneering IVIP capabilities since launching Axiad Mesh in 2024. We saw the visibility gap long before it had a name—and built the platform to solve it.

Why Axiad Mesh Leads the IVIP Category

First to Market

While competitors are scrambling to add IVIP features, we've already been delivering unified identity intelligence. Our customers already have the visibility advantage analysts say will take others years to achieve.

Purpose-Built, Not Bolt-On

Axiad Mesh was architected from day one as a visibility and intelligence layer. We're not an IGA, ITDR, or ISPM tool with dashboards added—we're a true IVIP that makes every other IAM tool in your stack more effective.

PKI Intelligence Built-In

As a leader in PKI credential management, we bring unique certificate and cryptographic visibility for NHIs that other IVIPs lack. Discover every crypto asset, track ownership, and prepare for post-quantum cryptography—all from one platform.

Deployment at Scale

Start seeing value in days, not months. Our deployment methodology accelerates time-to-value and ensures adoption success.

Integrate, Don't Rip and Replace

Native integrations with the tools you already use. We don't replace your stack —we unify it, normalize it, and make it intelligent.



Get Your Free FAIR Identity Risk Analysis

LIMITED TIME OFFER

See your identity risk quantified in financial terms. Axiad Mesh will analyze your environment and deliver a comprehensive FAIR assessment showing probable loss exposure, risk prioritization, and investment recommendations—at no cost.

Your Free Report Includes:

- Financial Risk Quantification – Probable annual loss exposure in dollar amounts
- Risk Prioritization – Top identity risks ranked by financial impact
- ROI Projections – Expected returns on identity security investments

Visit Axiad Website

No software purchase required • Completely confidential



The First Identity Visibility and Intelligence Platform

© 2026 Axiad. All rights reserved.

axiad.com