PRODUCT BRIEF

AXIAD

AXIAD MESH

# Identity Risk Management (IdRM) at Enterprise Scale

More digital identities are at work in today's organizations than at any other time in history. They include multiple human identities for on-prem and SaaS applications, as well as non-human identities used for machines, containers, workloads, and virtual infrastructure of all kinds. And the business-level causes of this "identity boom" aren't going anywhere:

- Many organizations use multiple identity providers (IDPs), along with identity governance (IGA) and privileged access (PAM) solutions
- Increasing use of machine identities, including personal devices, production devices, corporate devices and security controls
- Ongoing digital transformation efforts will continually create new sources, distributors and consumers of enterprise identities

The unintended consequence of this identity boom? Uncontained identity sprawl: identities have become the fastest growing and most under-protected attack surface in most modern organizations.

Axiad Mesh is an identity risk management (IdRM) solution that leverages identity fabric technologies to provide a unified view of disparate identity sources. It highlights and measures risks and assists cybersecurity and IAM teams in managing these risks before they're swamped by them. And it facilitates inter-team communication and remediation.

## Identify and Quantify Risky Identities, and Then Fortify Them

- Discover human and non-human identities across your enterprise
- Create a singular view of identity risk, despite organizational or functional silos
- Discover and fill gaps in identity profiles
- Pull insights from existing identity tools and platforms
- Calculate risk scores based on consistent, repeatable frameworks
- Determine the "blast radius" of potential identity compromises
- Get out-of-the-box insight on how to manage and mitigate identity risks
- Take action: communicate remediation details across teams

New to IdRM? Download our free e-book, The Definitive Guide to Identity Risk Management, to learn how IdRM addresses the problems presented by our ongoing identity boom.

# CORE CAPABILITIES

- **Identify Your Risky Identities.** Identities are the #1 attack surface for modern adversaries: 90% of organizations experienced an identity-based incident last year[1], and nearly 80% of enterprise breaches come from phishing or compromised identity credentials[2]. The first step in resolving these challenges is identifying and mapping your organization's extended use of human and non-human identities, whether known and trusted or born from "shadow IT" practices. Axiad Mesh categorizes risk types in your organization as a starting point, and then discovers at-risk identities used in on-prem or cloud-based infrastructures.
- **Quantify Your Identity Risks.** Identities are not as simple as they appear: they're complex, stateful, contextual elements that are the foundation of every security program. This is true even as they dynamically morph and change. Identities can be "stale" and un-updated, or inconsistent between systems, or completely devoid of correlation, context and confidence. Axiad Mesh correlates identities against known-good sources and provides consistent scoring to prioritize risks at an enterprise scale. This breaks down silos, removes surprises, and ensures teams can bring the right resources to bear at the right time.
- **Fortify Your At-Risk Identities.** Identities—and the credentials and authentication processes that support them—can be weak or strong or any condition in between. Axiad Mesh gives insight into weak identity controls, credentials and practices. It enriches existing cybersecurity tools and gives actionable identity data to operational teams, facilitating fast remediation. Axiad Mesh shows these teams how to harden identities against increasing attacks and threats.

[1] Study: 90 Percent of Organizations Experienced an Identity-Related Incident in Last Year

[2] Revealing the threat landscape with the 2024 Elastic Global Threat Report

See for yourself how Axiad Mesh identifies hidden identity risks, quantifies risks for better prioritization and management, and fortifies identities against impending attacks.

Book a Demo


*AXIAD Mesh provides risk leaders with enterprise-wide views of identity-specific risks, as well as tools needed to remediate them*

# MAINTAIN PROPER IDENTITY HYGIENE

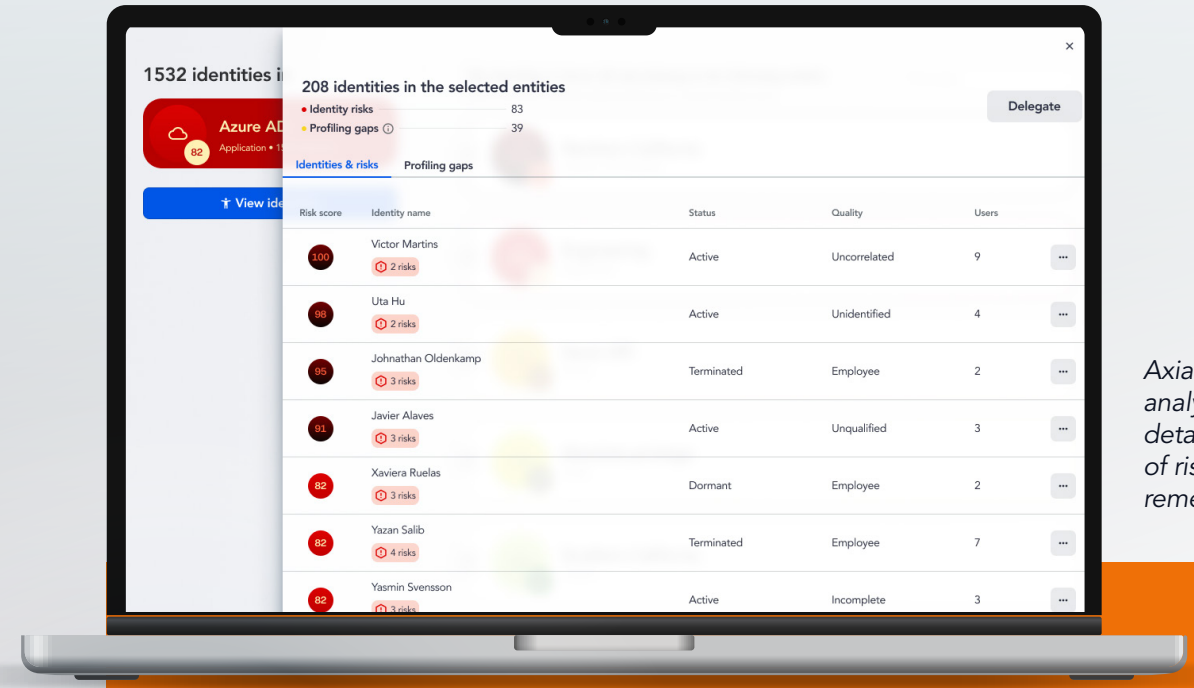
As a recent report from Gartner on identity hygiene states[3],

"You can't protect what you don't know about, and what you don't know about can cause pain and grief when you least expect it."

[3] Prioritize IAM Hygiene for Robust Identity-First Security

To avoid the "pain and grief" of identity-based attacks, practitioners are refocusing on their security roots and pursuing practices of "good identity hygiene." Axiad Mesh does this by automatically detecting and flagging issues like excessive permissions, weak or non-deployed MFA, or identities with inconsistent and questionable status. Once the manually or automatically detected identities are gathered, Axiad Mesh merges their attributes to assign risk scores that highlight inconsistencies and vulnerabilities. This is the first step in maintaining identity hygiene.

From that point, Axiad Mesh enriches the work of other tools in your identity stack like IdP, PAM or IGA solutions. It supports automated workflows to remediate discovered risks without manual intervention, while integrating with management systems like Axiad Conductor for automatic remediation if needed.




*Axiad Mesh allows security analysts to dive into risk details, determine root cause of risk, and delegate remediation*

Get your complimentary copy of the Gartner report, Prioritize IAM Hygiene for Robust Identity-First Security, and learn how a renewed focus in identity hygiene can address escalating identity attacks.

# MITIGATION REQUIRES CORRELATION

Understanding and managing identity risk begins with correlation. Advanced identity correlation is a process that works across fragmented systems, whether HR or IT operations or SOC, and provides a unified view of an organization's identities. It can show you when a human identity has been flagged as Terminated in HR systems but still retains privileges and access in operational systems.

Once correlated, "problem" identities become immediately obvious and highly actionable. Gaps in human and non-human identity profiles can be filled in and clarified. Risk scores can be assigned to individual identities, functional units, working teams, or application groups, breaking down silos and leading to faster remediation with less downtime.

With Axiad Mesh, raw identity data is ingested and correlated from multiple sources to create actionable insight:

Microsoft Entra ID

aws

okta

Ping Identity

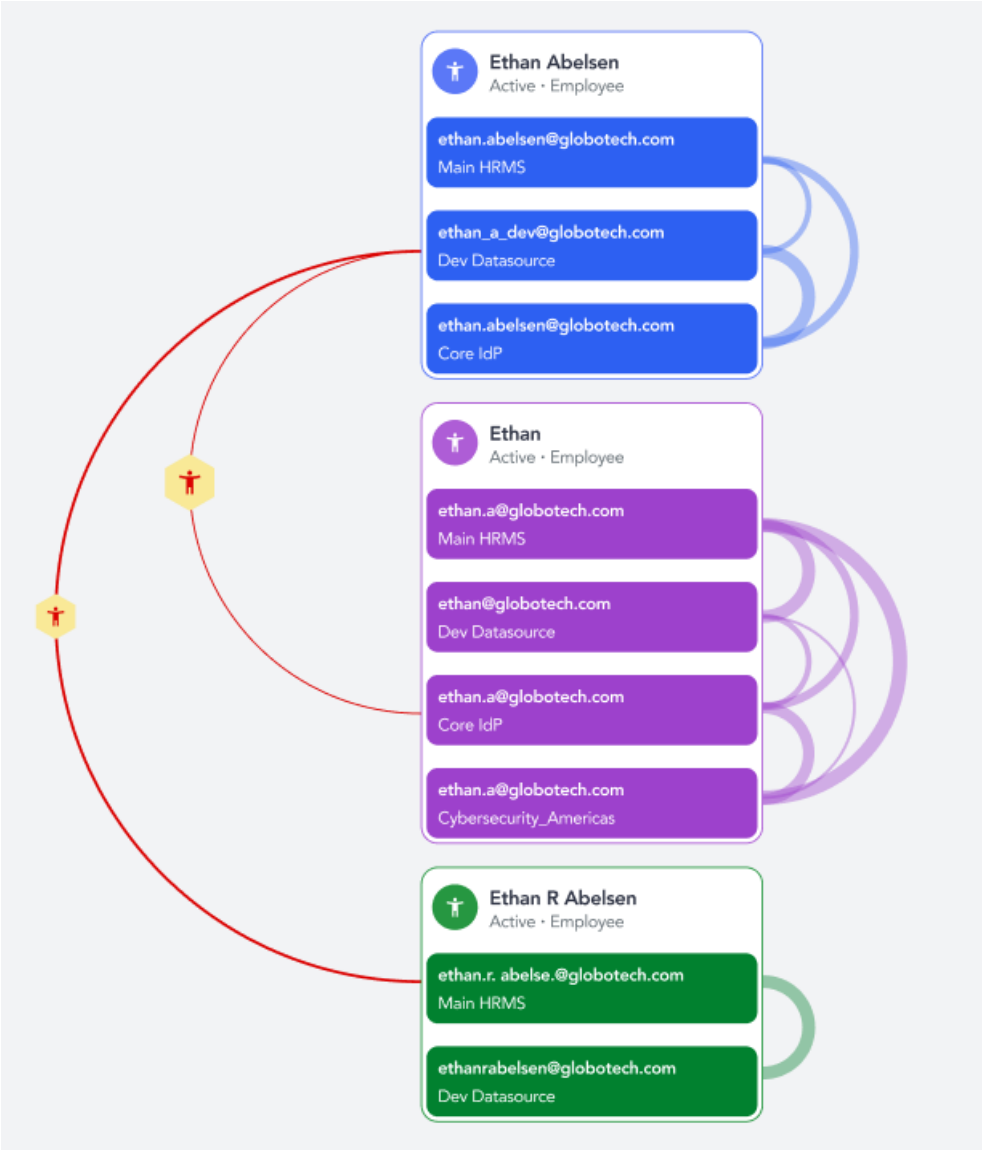
Venafi

trinet

appviewX

workday.

SailPoint



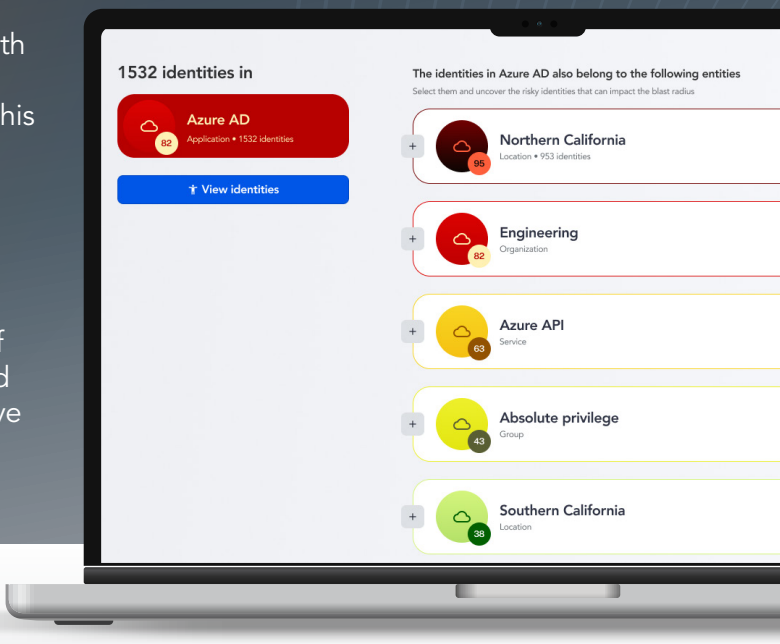

*The root of IdRM is simplified correlation of identity attributes and linkages across different identity sources and teams*

# INSIGHT ACROSS TEAMS AND FUNCTIONS

Individual identities can be robust or risky. But taken together, whole groups of weakly protected identities can lead to significant business or organizational problems. In February of 2024, Change Health experienced not only the largest data breach of the year but what would prove to be the largest breach ever of protected health care data, impacting over 100 million customers. The company had been acquired by UnitedHealth Group (UHG) in a 2022 deal valued at $13 billion. According to forensics reports, the attack was successful because Change Health was not using multifactor authentication to secure identities in one of their critical systems. Unfortunately, this level of deep risk insight across companies is rarely available for due diligence teams, and never obvious.

**Axiad Mesh provides the kind of deep, risk-based insight** into the state of identities and their protection mechanisms that are crucial to understanding nested, deeply integrated risks. No one can claim this degree of identity insight between Change Health and UHG would have stopped the attack, but few can argue it would have been beneficial.

*Risky identities often exist in multiple systems or groups. Axiad Mesh allows deep discovery and insight gathering across systems.*




# PLATFORM-NEUTRAL INTEGRATIONS

Everyone's identity ecosystem is deep and varied. Identity providers like Microsoft, Okta and Ping need to work side-by-side with IGA tools. PAM solutions, PKI providers, and hardware security token vendors need to efficiently interoperate in complex, frequently changing ecosystems. To provide value in these environments requires less focus on "being the default platform" and more focus on providing deep, useful integrations that are nevertheless easy to achieve and maintain.

Axiad Mesh has been built with an integration-first philosophy that enriches all the identity tools in your arsenal. Axiad Mesh leverages:

- The Open Cybersecurity Schema Framework (OCSF) to integrate with identity providers, as well as the directories and security policies in external sources like GitHub
- Continuous Access Evaluation Profile (CAEP) and the Risk Incident Sharing and Coordination (RISC) from the OpenID Foundation's Shared Signals Working Group

This allows Axiad Mesh to plug into your current identity stack and start providing actionable risk insights with real value on Day One.

Axiad's expertise in integrating signals and capabilities across the identity ecosystem is the prime enabler of Mesh insights and risk mitigations

IAM SYSTEMS

Microsoft okta Ping Identity FORGEROCK ONE IDENTITY

HARDWARE AUTHENTICATIONS

yubico IDEMIA THALES FEITIAN WE BUILD SECURITY

ENDPOINTS

iOS linux mac OS

PAM

CYBERARK BeyondTrust Delinea

PKI SYSTEMS

Microsoft ENTRUST KEYFACTOR Atos

IGA

SailPoint SAVIYNT

MACHINE IDENTITIES

appviewX Venafi

Axiad Mesh provides immediate insight into the state of your organization's extended identity risks.
Visit www.axiad.com/axiad-mesh/ to try or to learn more.

WWW.AXIAD.COM

101 Metro Drive, Suite 560 San Jose, CA 95110 United States

AXIAD