Software Analyst®
Cyber Research

FEBRUARY 2025

FRANCIS ODUM

SECURING THE IDENTITY ATTACK SURFACE

A DEEP DIVE INTO THE NEW BATTLEFIELD OF IDENTITY SECURITY

axiad AUTHMIND HYDDEN SILVERFORT slash/id ACALVIO

TABLE OF CONTENTS

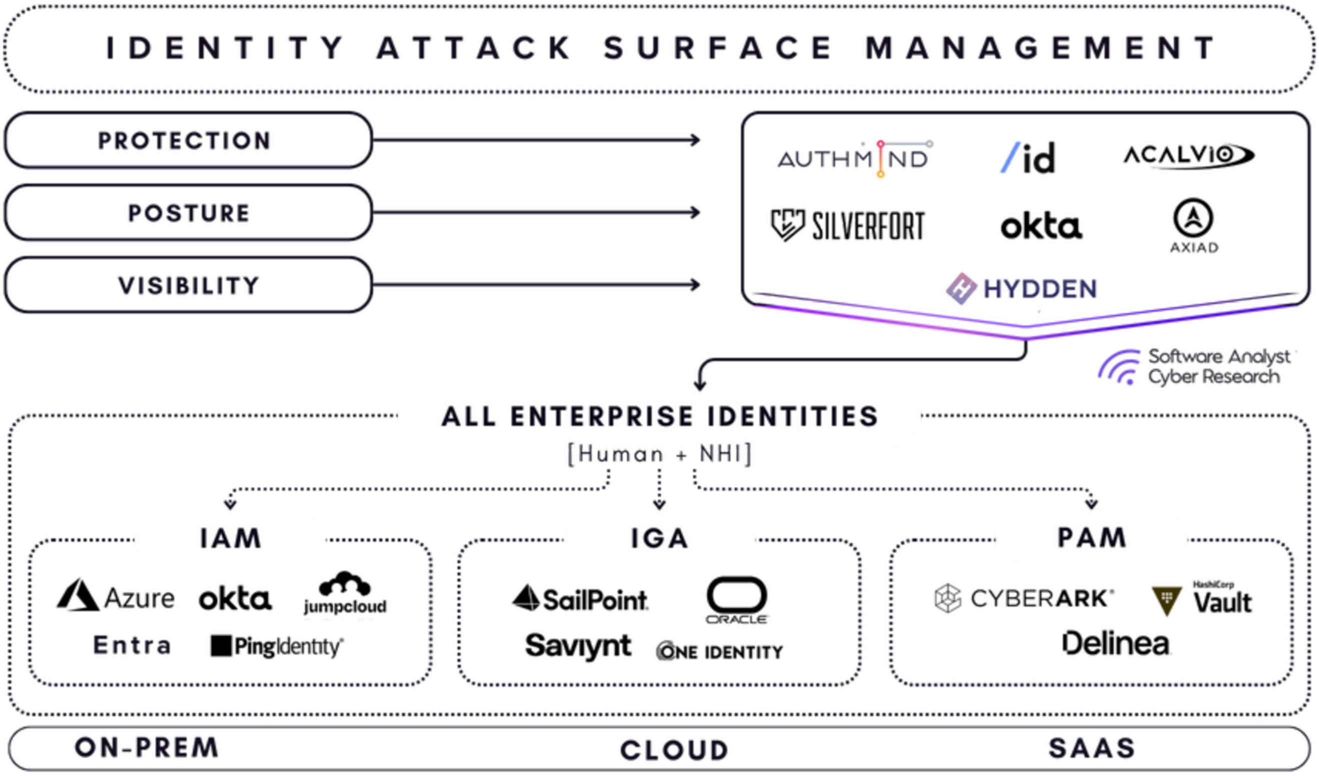
INTRODUCTORY BLURB

Over the past two decades, the most successful identity security vendors—each nearing a billion in revenue—have been built around Identity Access Management (IAM), Identity Governance and Administration (IGA), and Privileged Access Management (PAM). This trend has given rise to giant leaders like Microsoft Identity, Okta, CyberArk, and SailPoint, with the latter poised for an IPO.

The next generation of identity security companies will unify IAM, PAM, and IGA, addressing the silos and security gaps that have emerged as enterprise stacks evolve with AI and LLMs. As organizations scale, identities—spanning both human and non-human identities (NHI)—has become one of the most exploited and overlooked attack surfaces in cybersecurity.

This report dissects the Identity Attack Surface, exposing how threat actors exploit identity weaknesses and what enterprises must do to defend against them.

KEY SUMMARY



The focus of this report: This report explores how enterprises can secure their identity attack surface using multiple approaches. I have written extensively on the identity governance ecosystem and non-human identities (NHIs). However, this report focuses on three key methodologies for how enterprises can go about monitoring, managing and securing their identity attack surface

Structure of the report: The rise of the identity attack is leading organizations to realize the importance of closing gaps within their existing identity solutions. This report aims to discuss how enterprises can leverage this 3-step process:

1. **Visibility** provides the foundational understanding of the identity landscape.
2. **ISPM** proactively enforces hygiene and proper configuration to reduce vulnerabilities.
3. **ITDR** actively monitors and mitigates threats as they arise, complementing proactive management strategies.

WHY IDENTITY?

Why The Identity Attack Surface? The concept of an attack surface has long been recognized in security. However, its application to identity security is a relatively recent development that is gaining momentum. Identity Attack Surface Management (IASM) has emerged as a response to the growing realization of gaps within legacy identity vendors. The objective is to provide enterprises with full visibility into their legacy identity stacks, enforce posture controls, protect identities and drive remediation efforts based on informed insights.

How IASM is the next battlefront in Identity security: Over the past decade, organizations have focused primarily on managing access control (IAM), identity governance (IGA), and privilege management (PAM) solutions. These solutions hold a vast number of identities, yet they all provide very different solutions across a wide spectrum of architectures. These solutions don’t easily integrate amongst each other. This has led to organizations to have silos and many failed identity projects, resulting in numerous breaches. The next platform in security will have strong visibility, posture and protection mechanism.

The frequency and prevalence of identity attacks have surged over the years, due to weaknesses in identity systems, emphasizing the need for IASM. Attackers are increasingly leveraging techniques that bypass existing controls, forcing enterprises to adopt more advanced security measures.

.

- **90%** of organizations experienced an identity-related breach in the past year, with 93% of these breaches being preventable through improved controls.
- **37%** of organizations reported that implementing MFA for all users helped prevent or mitigate the effects of incidents. Other effective measures included regular reviews of access to sensitive data **(42%**) and privileged access **(50%).**
- The MITRE ATT&CK framework reveals that **50%** of observed attack tactics in the wild target identity, emphasizing the necessity for unified security visibility.
- **75%** of detections are malware-free (a malware-free attack enables adversaries to operate under the radar and navigate seamlessly across endpoint and cloud domains).

Key report takeaways: Stronger visibility empowers organizations to take proactive, coordinated remediation steps. By breaking down silos between security teams, organizations can adopt the most secure and future-proof strategies to remediate vulnerabilities.

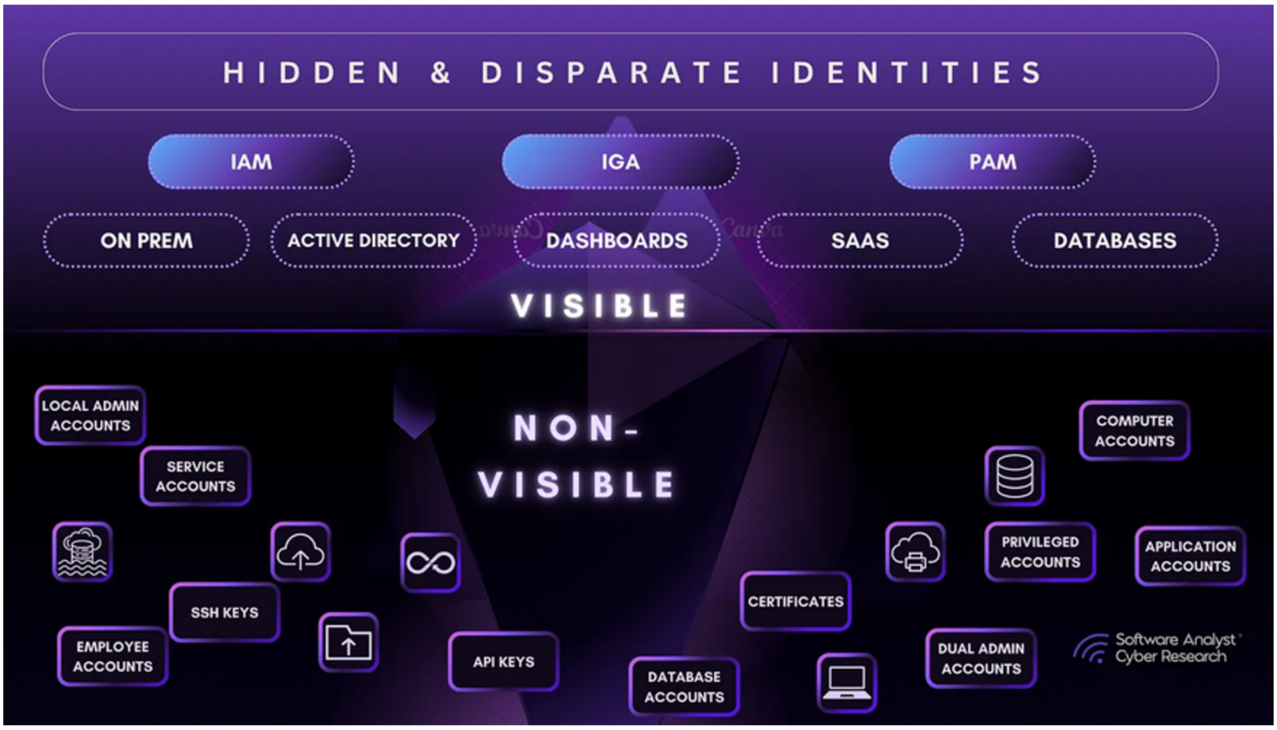
Identity security problem is a data problem: Identity security fundamentally hinges on data integrity. Despite frameworks like OCSF, Okta's IPSIE, and CAEP improving interoperability, they fail to fully normalize and correlate identity data across HR systems, traditional IAM solutions, and cloud-native identity platforms. This fragmentation weakens security postures, making enterprises vulnerable to identity-based threats. Organizations must proactively establish a unified identity data foundation, ensuring seamless correlation and governance. As these standards evolve, enterprises that prioritize structured identity data management will be better positioned to enhance security and streamline compliance

Key representative vendors are discussed and highlighted throughout this report. These vendors represent this market ecosystem and the evolution toward visibility, posture and protection. There are many more vendors on the market that provide something similar or adjacent. One of the most successful has been CrowdStrike's achievement of $400M+ in revenue in less than 4+ years after their acquisition of Prempt in 2020. However, SACR selected these vendors after thorough product review and collaborated with them to successfully bring the research to market.

- Hydden
- Silverfort
- Authmind
- Acalvio
- SlashID
- Axiad

SILOED GAPS IN IDENTITIES TODAY

What you see is just the beginning—beneath the surface, enterprises manage thousands of hidden identities, from users to non-human entities, each a potential attack vector. At the surface, enterprises rely on IAM, PAM, and IGA to manage identities—but beneath, a vast, fragmented web of disparate identities remains unseen. Service accounts, API keys, machine identities, shadow IT, and ephemeral credentials operate in the dark, expanding the Identity Attack Surface beyond traditional controls. Without visibility into these hidden layers, organizations are exposed to silent threats lurking below the surface.



THE MODERN ATTACK SURFACE IS IDENTITY-CENTRIC

To help us better understand the role of identity in the modern attack surface. We need to dissect and analyze — both:

1. Identity security management
2. Attack surface management

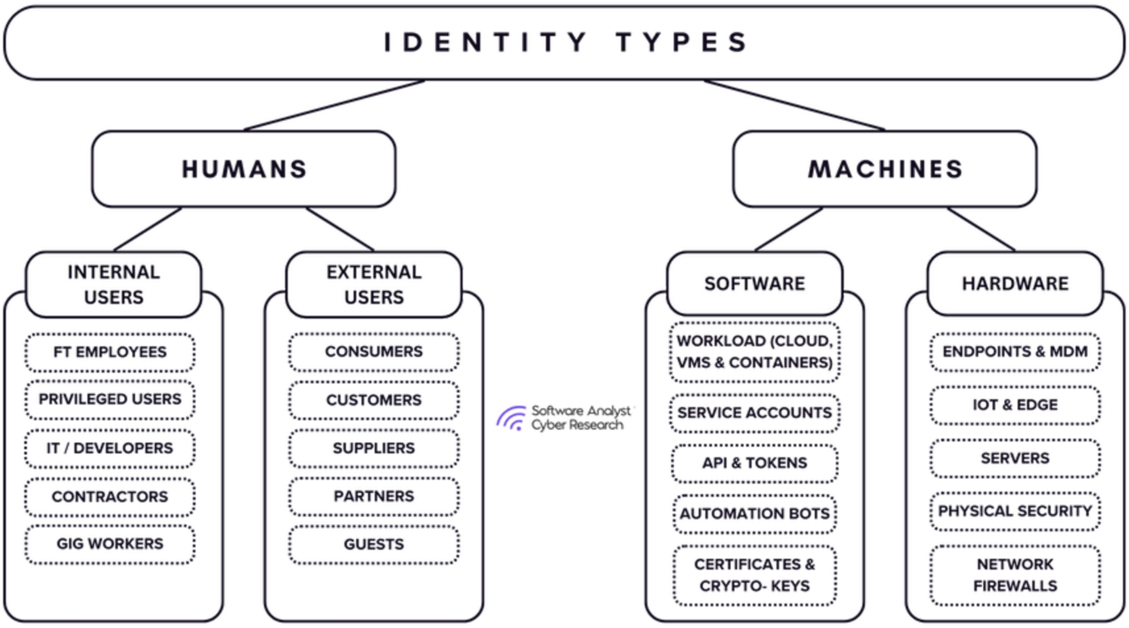
Let's begin with breaking down identity into its foundational principles.

An identity is any entity within an enterprise that can be authenticated and authorized to perform actions within an IT system. We have two primary categories:

- Human Identities ("People")
- Non-Human Identities ("Machines")

Modern identity security management should takes a holistic approach, ensuring that both human and non-human identities are properly authenticated, authorized, and monitored to prevent unauthorized access, privilege abuse, and identity-based threats. It encompasses three critical areas:

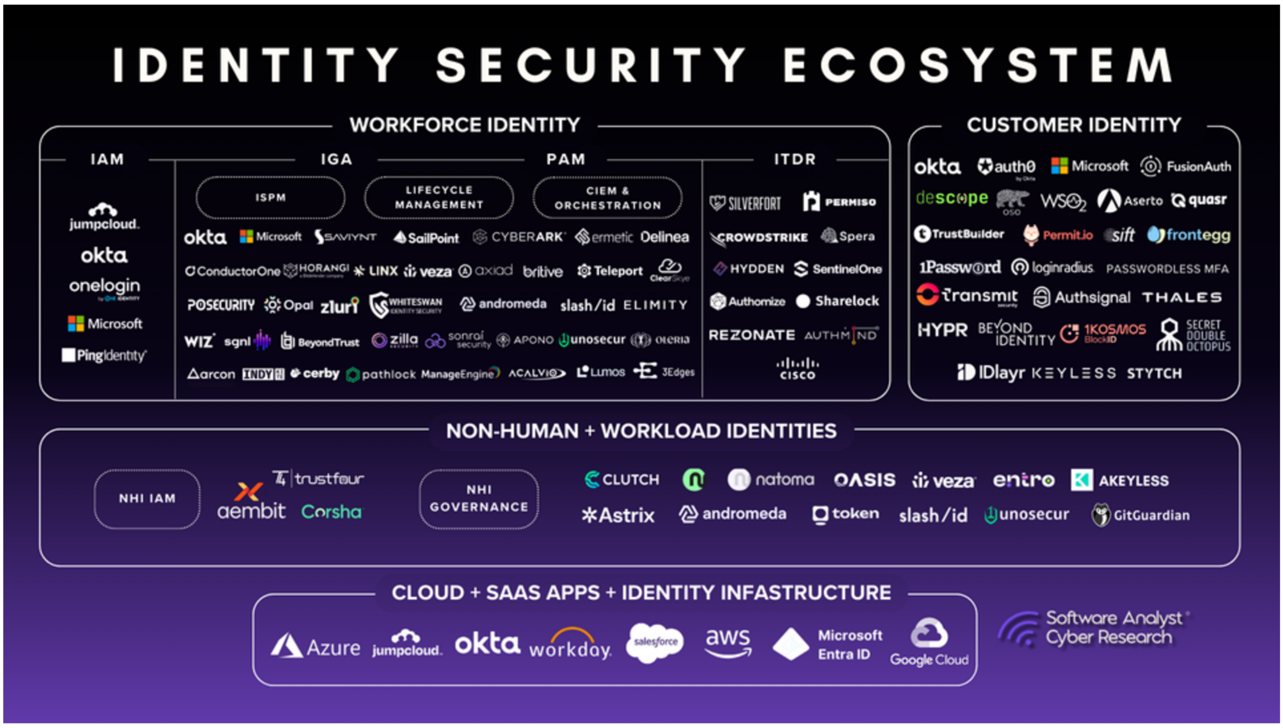
THE MODERN ATTACK SURFACE IS IDENTITY-CENTRIC



1. **Human identities**, including employees, contractors, and partners, who require strong authentication, least privilege access, and governance to mitigate risks like credential theft and insider threats.
2. **Non-human identities (NHIs)**, such as service accounts, bots, and API keys, that often have excessive privileges and require robust secrets management, rotation policies, and machine identity protection to prevent exploitation.
3. **Digital identities,** which include user accounts, roles, permissions, and credentials that define access and are susceptible to privilege escalation, misconfigurations, and sprawl if not properly managed

MODERN IDENTITY ECOSYSTEM CONTINUES TO EXPAND

The identity ecosystem continues to explode and grow, as can be seen in the market map below:

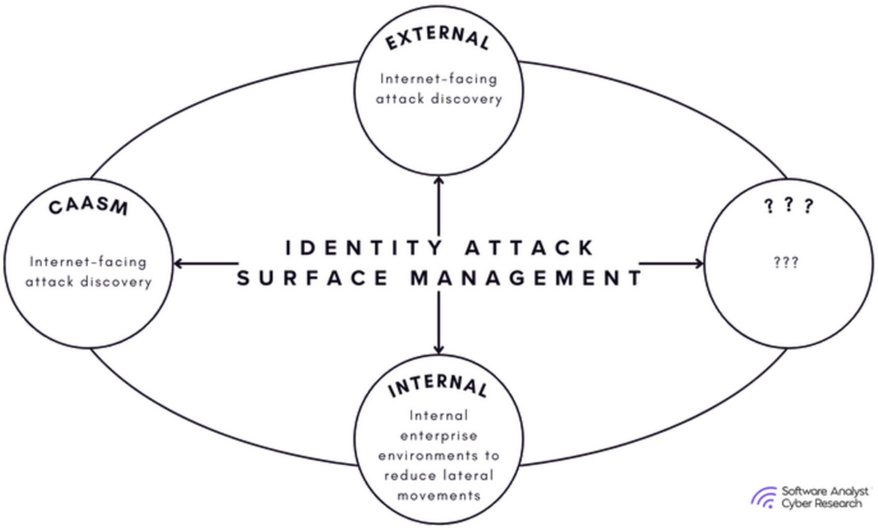


I have written extensively on the identity governance ecosystem and non-human identities (NHIs). However, we want to delve into the attack surface built around this ecosystem today.

ATTACK SURFACE MANAGEMENT (ASM)

Attack Surface Management (ASM) involves the continuous discovery, inventorying, classification, and risk assessment of an organization's digital assets to minimize exposure to potential cyberattacks. It includes identifying all external and internal points that could be exploited by attackers, understanding their vulnerabilities, and taking proactive steps to secure them. Historically, ASM has been categorized into the following types:

1. **EASM (External Attack Surface Management):** Focuses primarily on internet-facing assets for a company, continuously discovering and monitoring misconfigurations, shadow IT, and vulnerabilities to minimize external exposure.
2. **Traditional ASM (Attack Surface Management)**: Focuses on internal networks, endpoints, and identities, detecting insider threats, lateral movement risks, and unpatched vulnerabilities to strengthen internal security.
3. **CAASM (Continuous Attack Surface Management):** Provides a unified, real-time view of an organization's entire attack surface by integrating security tools, prioritizing risks, and automating remediation.


EXTERNAL
Internet-facing attack discovery
CAASM
Internet-facing attack discovery
IDENTITY ATTACK SURFACE MANAGEMENT
? ? ?
???
INTERNAL
Internal enterprise environments to reduce lateral movements
Software Analyst Cyber Research

BRINGING IT TOGETHER: IDENTITY CENTRIC (ASM)

After reviewing the key identity categories, it is evident that a significant portion of modern enterprise architecture is identity-driven across both human and machine identities. Traditional Attack Surface Management (ASM) focused on external and internal assets such as servers, applications, cloud environments, and endpoints. However, identity has become the primary attack vector in modern cyber threats, cutting across all boundaries. Additionally, Identity is the new perimeter i.e. Traditional ASM focused on networks and endpoints, but in cloud and hybrid environments, attackers bypass these and directly target credentials, privileges, and identity misconfiguration.

Credential stuffing, phishing, session hijacking, and privilege escalation attacks are now dominant in modern breaches (e.g., Okta and Uber breaches).

For example, Identity-based attacks have become central to the MITRE ATT&CK framework, with nearly half of its tactics relying on exploiting identity vulnerabilities. From initial access via credential theft to privilege escalation, persistence, and lateral movement, adversaries increasingly target weak authentication, excessive permissions, and mismanaged identities. Credential Access, a tactic entirely identity-focused, highlights the growing risk of stolen, cracked, or intercepted credentials. Attackers leverage identity-based reconnaissance, adversary-in-the-middle attacks, and privilege abuse to compromise organizations at scale. As identity becomes the new perimeter, SOC teams must integrate Identity Risk Management (IdRM) and Identity Threat Detection & Response (ITDR) to map and mitigate these attack vectors in real-time. Strengthening identity security is critical to closing gaps before they can be exploited.

Key parallels between traditional ASM and identity attack surface management (IASM) include :

1. **Asset Discovery → Identity Discovery:** Just as ASM maps exposed IT assets, IASM maps identities and their entitlements across cloud, SaaS, and on-prem environments.
2. **Attack Path Analysis → Identity Risk Analysis:** Traditional ASM traces exploitable attack paths; while IASM maps identity attack paths to identify privilege escalation risks.
3. **Continuous Monitoring → Identity Drift & Exposure:** ASM tracks asset changes, whereas IASM monitors identity and permission changes to prevent unintended exposure.

INTRODUCING IDENTITY ATTACK SURFACE MANAGEMENT (IASM)

IASM is the process of discovering, monitoring, and managing all identity-related vulnerabilities and risks within an organization. As the attack surface expands with the addition of new employees and applications creating new identities, enterprises struggle to manage them effectively, increasing the likelihood of attacks. Identity ASM or IASM extends visibility into identities, making ASM more holistic and adaptive to modern threats.

The end goal of IASM is to proactively limit exposure by preventing unauthorized users from compromising identities and gaining access. Just as ASM solutions analyze potential attack paths and identify key targets attackers may pursue, IASM provides centralized visibility into all identities, wherever they exist, focusing on securing identity-related assets against exploitation.

USE CASES

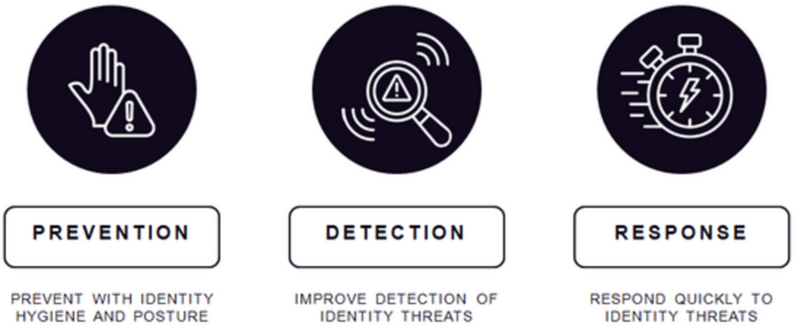
IASM cuts across traditional boundaries by:

1. Providing complete coverage of the identity lifecycle, identifying configuration states and hygiene across all identity types (B2E, B2C, Machine).
2. Enforcing security policies across solutions to align security policies across all existing products.
3. Proactively identifying threats early while offering holistic risk assessments.
4. Detecting exposed credentials, risky access patterns, and potential identity-based attack vectors that malicious actors could exploit.
5. Identifying dormant accounts, excessive privileges, and exposed credentials across cloud services, third-party applications, and development environments.
6. Prioritizing and resolving identity-based risks based on identity data source context and telemetry.

EXISTING IDENTITY SECURITY FRAMEWORKS

PREVENTION, DETECTION AND RESPONSE

As identity-based attacks have become the primary entry point for cyber threats, many industry frameworks emphasize prevention techniques, detection mechanisms, and response capabilities for a comprehensive identity security strategy. While these frameworks collectively help reduce attack surfaces, more structured approaches are needed to address identity-specific threats.



PREVENTION

PREVENT WITH IDENTITY HYGIENE AND POSTURE

DETECTION

IMPROVE DETECTION OF IDENTITY THREATS

RESPONSE

RESPOND QUICKLY TO IDENTITY THREATS

IASM INTERCONNECTS WITH EXISTING IDENTITY CATEGORIES

Many existing identity solutions focus on isolated aspects of identity security:

- IAM, which focuses on the authentication layer
- IGA, which focuses on account lifecycle management
- PAM, which focuses on privileged users, secrets, and vaulting

While traditional IAM tools offer some identity management capabilities, they often operate in isolation and have significant limitations. Modern identity security requires a more comprehensive approach. Traditional solutions face several key challenges: they cannot effectively aggregate and normalize identity data across diverse platforms, they lack enterprise-wide contextual awareness for informed remediation, and they cannot provide standardized risk assessments across the organization.

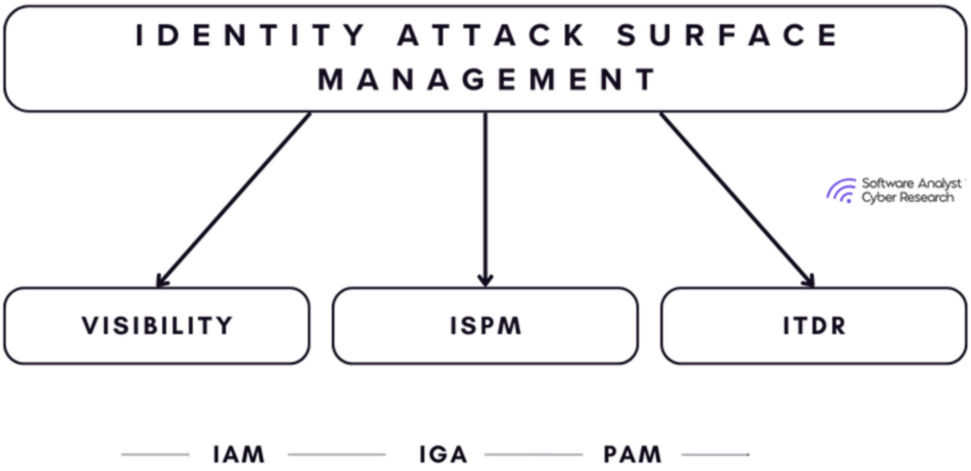
Most importantly, they fail to provide a holistic view of an organization's identity attack surface and cannot effectively prioritize identity-related risks that could lead to major security breaches.

Most of these solutions remain siloed, focused solely on the key areas they were designed to protect. IASM serves as a foundational layer that spans IAM, IGA, PAM, and ZTNA, enabling teams to take remediation actions and strengthen existing identity security implementations.

The fundamental identity security problem is a data problem. Despite efforts to improve interoperability through frameworks like OCSF, RISC, IPSIE, and CAEP, a significant gap remains in the identity security landscape. While these standards facilitate some integration between IAM systems, they lack the comprehensive capabilities needed to fully normalize and correlate identity data across the modern enterprise ecosystem, which spans human resources systems, traditional IAM solutions, and cloud-native identity management platforms. As these frameworks and standards gain traction in the industry, organizations will be required to comply. To maintain a strong security posture, they must also adopt the right technologies to secure all identities within their infrastructure, ensuring every identity is properly managed and protected.

COMPONENTS OF IASM

1. **Discovery and visibility**
2. **Posture and hygiene**
3. **Protection and remediation**


IDENTITY ATTACK SURFACE MANAGEMENT
Software Analyst Cyber Research
VISIBILITY
ISPM
ITDR
IAM
IGA
PAM

DISCOVERY & VISIBILITY

Visibility is the foundational pillar of IASM, as you cannot secure what you cannot see. Identity discovery and inventory are essential, as securing the attack surface depends on making all identities within an organization's ecosystem visible, including both human and non-human identities (NHIs).

The lack of identity visibility leads to shadow identities, orphaned accounts, over-privileged access, and an expanded attack surface. Visibility provides organizations with a real-time inventory of all identities, their relationships, and their associated permissions. Thus, visibility should encompass the following:

- Discovering and identifying all human and machine identities to gain a clear, real-time view of who is accessing what resources.
- Inventorying and cataloging identity types, permissions, and their associated attributes across all IT assets.
- Mapping access privileges for each identity to enforce least-privilege principles and detect over-privileged accounts and unused permissions.
- Mapping permissions and relationships: Understanding the relationships between identities and the assets they can access, such as cloud resources, applications, or data stores.
- Ongoing and continuous monitoring of all identities, including new identities being created, rather than relying on static visibility, as most solutions on the market do.

The IASM process follows a comprehensive structured workflow, progressing from discovery to visibility and ultimately to controls. Unlike traditional static assessments, this approach ensures continuous, ongoing discovery across the enterprise's fragmented identity infrastructure. The system provides detailed reporting and dashboards for different stakeholders, all built on a unified data foundation that consolidates and analyzes all identity-related information.

Many of these solutions focus on:

- Querying target systems and applications using their APIs
- System and identity log parsing and analysis
- Event-driven data capture

This data is then used to continuously monitor and track configuration and permission changes to detect identity-based threats.

ASSESSING VENDOR'S CAPABILITIES IN IMPROVED IDENTITY VISIBILITY

Comprehensive Identity Discovery: The first job of an IASM solution is to discover and ingest identity information from across the enterprise. This process requires integration with a wide range of systems where user identities and identity information are created, stored, and managed.

Example Case Study: Cloud Identity Exposure - A Fortune 500 company identified thousands of orphaned service accounts across its AWS and Azure environments. By leveraging automated identity discovery tools, it reduced its exposed attack surface by 40% in three months.

1. **Breadth To Depth of integrations and connectors**
    - The solution should integrate with various applications and services with strong connectors including:
        - **Human Resource Management Systems (HRMS)** – Managing workforce identities and access.
        - **Enterprise and Cloud Identity Directories** – Centralized repositories for user authentication and authorization.
        - **Traffic Monitoring & Directory Logs** – Providing visibility into identity usage and anomalies.
        - **Privileged Access Management (PAM) & Identity Governance and Administration (IGA)** – Controlling and auditing privileged and general user access.

- **Identity Providers (IdPs)** – Supporting digital identity management and single sign-on (SSO) across cloud-based and legacy on-premises environments.
- **Security & Networking Solutions** – Including XDR, SASE, and other perimeter defense tools that integrate identity data for enhanced security.
- **SIEM & SOAR Platforms** – Aggregating and correlating identity-related security events for threat detection and response.
- **Machine Identity Management Solutions** – Governing non-human entities like bots, workloads, and service accounts.
- **Certificate Lifecycle Management Services** – Ensuring the integrity and renewal of cryptographic credentials.
- **SaaS & API-Based Services** – Extending identity governance across both cloud and on-premises applications

2. Identity scanning capabilities

An effective solution must:

- Continuously monitor identities across cloud, on-premises, and hybrid environments
- Detect and inventory IAM accounts from providers like Microsoft, Okta, and JumpCloud.
- Identify both human and non-human identities, including API keys, bots, and service accounts.
- Uncover shadow identities and unauthorized access points, mitigating hidden risks within the identity attack surface.

3. Inventory of all identities

A comprehensive inventory of identities enables teams to:

- Identify groups, departments, platforms, applications, and regions with the highest risks, helping determine root causes and prioritize resources effectively.
- Normalize the data: Data normalization is essential for Identity and Risk Management (IdRM) solutions that integrate with various information sources. While systems like HRMS, enterprise directories, and PAM solutions may store user data differently (e.g., names, addresses, titles, business units, locations), normalization converts this into a standard format. This standardization is crucial for correlating, aggregating, and analyzing identity data across disparate sources.

4. Identity graph to correlate and map identity-to-asset relationships

- To enhance visibility, organizations must be able to map which identities have access to which resources. Using graph-based security models, vendors should enable organizations to visualize identity-based attack paths and illustrate relationships between identities, groups, roles, entitlements, credentials, secrets, and other entities.

- Leverage external standards for context: Solutions should integrate with industry frameworks and standards, including the Open Cybersecurity Schema Framework (OCSF), Risk Identification and Site Criticality Toolkit (RISC), and the Continuous Access Evaluation Protocol (CAEP). Additionally, emerging standards like the Interoperability Profile for Secure Identity in the Enterprise (IPSIE) should be considered.

5. Analyze and assign risk scores

- Risk Scoring capabilities: Risk scoring capabilities are essential in identity security because they provide a quantifiable measure of the likelihood that an identity is compromised or poses a security risk. By assigning risk scores to users, service accounts, and access requests based on behavioral analytics, historical activity, and contextual factors, organizations can prioritize their security efforts. Risk scores enable the enforcement of dynamic, risk-based access controls. For example, a high-risk score could trigger additional authentication measures, limit privileges, or initiate automated incident response workflows, thereby reducing the chance for identity misuse.
- Real-Time Identity Monitoring: A robust database should be able to scan, capture and map identities. This functionality helps organizations detect anomalies in login patterns, permission changes, and access behavior.
- Detecting Orphaned & Unused Accounts: The system should also be able to perform regular audits and remove inactive accounts. It should also identify external identities (e.g., contractors, vendors) that no longer require access.

VISIBILITY CAN'T BE STATIC, BUT CONSTANT

Visibility into identities must be continuous and dynamic, rather than static. Organizations need to implement scanning mechanisms that monitor repositories frequently, as new identities and development processes are continuously introduced. Continuous, automated account discovery capabilities are essential for detecting when new accounts are created. Some of these capabilities can be integrated with cloud providers to identify newly created identities.

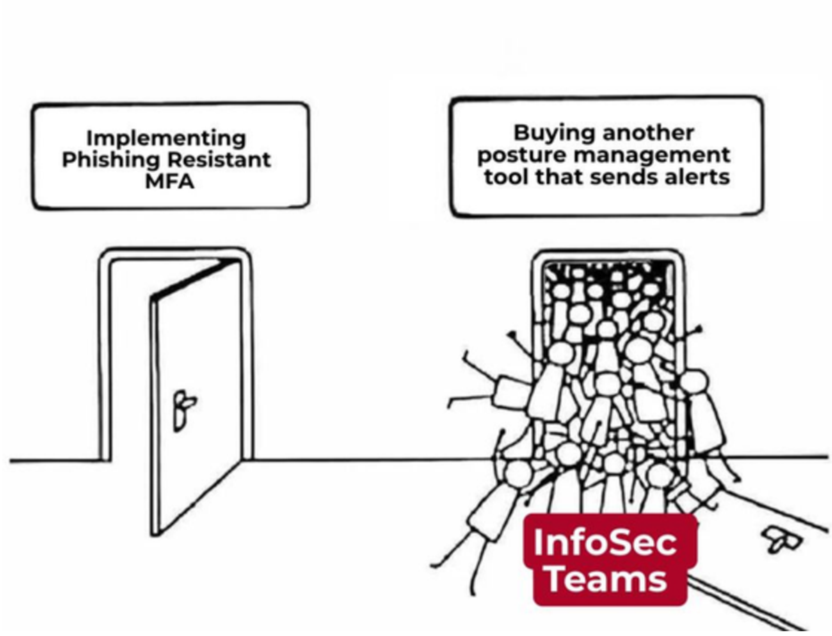
POSTURE & HYGIENE

This sub-category emphasizes maintaining a robust security baseline by assessing and improving the configuration and hygiene of identities. ISPM ensures that identities are correctly provisioned, regularly updated, and aligned with the principle of least privilege.

Challenges with IAM and Identity projects

Some of the major challenges in identity security can be tied to a perspective shared by Bojan Simic:

“Every major cybersecurity report clearly points out that authentication and identity verification attacks account for the vast majority of breaches. Unfortunately, we still see most InfoSec teams "taking the pill" by investing in more alerting and discovery of problems instead of truly working to get rid of the source of the problem. Sometimes this requires a bit of surgery. The good news is that phishing resistant authentication is deployable across all user groups within the enterprise. This can enable organizations to massively improve security and user experience. This will also help them achieve their Zero Trust/BeyondCorp identity assurance goals. - Full post here”


Implementing Phishing Resistant MFA
Buying another posture management tool that sends alerts
InfoSec Teams

How to prevent identity issues - Key Components

- **Identity Misconfiguration Detection:** Identifying issues such as overly permissive roles, weak passwords, and misaligned access policies.
- **Compliance and Governance:** Ensuring that identities adhere to internal policies and regulatory requirements (e.g., NIST, GDPR, HIPAA).
- **Lifecycle Management:** Regularly decommissioning stale or orphaned accounts to minimize exposure.
- **Access Reviews:** Conducting periodic reviews to validate that permissions align with job roles.

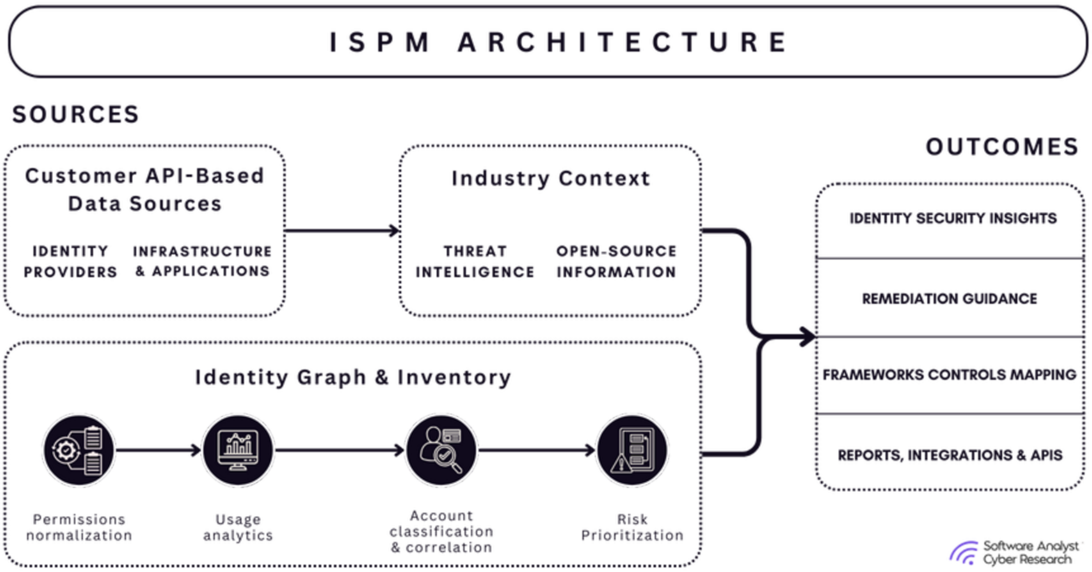
WHY SEPARATE VISIBILITY FROM POSTURE

Separating Visibility from Identity Security Posture Management (ISPM) is crucial for effective identity security. This distinction allows organizations to thoroughly identify and understand their identity landscape and relationships (Visibility) first, before implementing security policies and controls (ISPM). Visibility focuses on discovery and awareness, providing a comprehensive understanding of all identities and their interconnections within the organization. Meanwhile, ISPM centers on governance and enforcement, ensuring the identity landscape remains secure by minimizing misconfigurations, enforcing least privilege access, and eliminating over-provisioning.

By prioritizing visibility, organizations can take proactive and coordinated remediation steps based on a deep understanding of their identity landscape. Breaking down silos between security teams fosters collaboration, leading to comprehensive solutions that provide secure and future-proof remediation actions.

IDENTITY SECURITY POSTURE MANAGEMENT (ISPM)

Identity Security Posture Management (ISPM) has emerged as a critical approach for enterprises. ISPM is a proactive framework designed to enhance and maintain the security posture of an organization's identity infrastructure, preventing breaches and unauthorized access. It involves continuous monitoring and analysis of identities, access rights, and authentication processes across the entire digital ecosystem.


ISPM ARCHITECTURE
SOURCES
Customer API-Based Data Sources
IDENTITY PROVIDERS
INFRASTRUCTURE & APPLICATIONS
Industry Context
THREAT INTELLIGENCE
OPEN-SOURCE INFORMATION
Identity Graph & Inventory
Permissions normalization
Usage analytics
Account classification & correlation
Risk Prioritization
OUTCOMES
IDENTITY SECURITY INSIGHTS
REMEDIATION GUIDANCE
FRAMEWORKS CONTROLS MAPPING
REPORTS, INTEGRATIONS & APIS
Software Analyst Cyber Research

Similar to Cloud Security Posture Management (CSPM) but within an identity context, ISPM proactively identifies vulnerabilities and minimizes the identity attack surface for both human and non-human identities. Customers prioritize addressing known security gaps over-generalized threat detection due to concerns about noise and false positives. The insights from the visibility component should drive action to correct posture issues and fortify defenses against identity risks. Example Case Study: Preventing Overprivileged Access- A healthcare provider detected over 5,000 overprivileged accounts with access to sensitive patient data. After deploying an identity posture management solution, it reduced excessive permissions by 70%, mitigating the risk of insider threats.

HOW ORGANIZATIONS SHOULD FIX IDENTITY POSTURE & HYGIENE ISSUES

Identity Security Posture Management (ISPM) provides organizations with a systematic approach to continuously assess, manage, and remediate identity risks. This ensures that security gaps are proactively addressed before they can be exploited. By integrating ISPM into their identity security strategy, organizations can automate access reviews, enforce least privilege policies, detect misconfigurations, and eliminate identity sprawl. ISPM strengthens authentication controls, monitors non-human identities, and implements risk-based access policies, ultimately reducing the attack surface and improving overall security posture.

With ISPM in place, organizations can effectively tackle the following identity hygiene challenges:

1. **Detect & Fix Identity Misconfigurations**: ISPM solutions help security teams proactively detect and fix identity misconfigurations that could lead to unintended privilege escalation or lateral movement. This includes identifying misconfigured IAM roles, overly permissive policies, and wildcard permissions that grant excessive access. Organizations should implement network segmentation strategies to prevent unauthorized identity access to sensitive assets unless explicitly required. Regular IAM audits uncover potential weaknesses before exploitation
2. **Strict Enforcement of Multi-Factor Authentication (MFA):** Mandatory MFA for all privileged and external accounts as well as for companies moving to implement stronger authentication processes is critical. Cybercriminals continuously exploit weak or stolen credentials, making MFA an essential safeguard against unauthorized access. Organizations should move beyond legacy MFA implementations and adopt passwordless authentication wherever possible to reduce the attack surface for phishing-based credential theft. As adversaries refine their tactics, adaptive authentication mechanisms that factor in risk-based signals should be prioritized.

3. Principle of Least Privilege (PoLP): One of the most effective ways for organizations to strengthen their identity security posture is by enforcing the Principle of Least Privilege (PoLP). Identity sprawl and over-permissioned accounts have made organizations vulnerable to privilege escalation attacks. Security teams must ensure that every identity—human or non-human—has only the necessary permissions required to perform its function, nothing more. Implementing just-in-time (JIT) access further minimizes standing privileges, reducing the risk of persistent overexposure. Dynamic access control frameworks, such as role-based access control (RBAC) and attribute-based access control (ABAC), should be leveraged to grant permissions based on contextual signals rather than static entitlements.

4. **Managing, monitoring and reducing Identity Sprawl:** Unchecked identity sprawl leads to thousands of unnecessary or duplicate accounts, increasing the attack surface. To mitigate this risk, enterprises should actively merge duplicate accounts, remove unused roles, and decommission inactive identities. Automated tools should continuously scan and flag over-provisioned accounts, ensuring access remains tightly controlled as business needs evolve.

Case Study Outcomes for ISPM: Framework control mapping to the following frameworks

1. NIST - It could be linked to NIST AC-2(3)(d) to disable unused accounts or AC-2(11), AC-6-7 to remove unused permissions
2. There are other key compliance frameworks around SOX | SOC2 | PCI-DSS | ISO 27001 | CIS

Okta ISPM's powered by its Spera acquisition has robust resources and capabilities around resolving ISPM compliance issues.

HOW ISPMS SOLVE FOR IDENTITY COMPLIANCE STANDARDS

	PROBLEM	SOLUTION	SAMPLE USE CASE
NIST CYBERSECURITY FRAMEWORK	INACTIVE ACCOUNTS WITH ELEVATED PERMISSIONS REMAIN ACTIVE, VIOLATING NIST AC-2(3)(D).	MONITORS AND AUTOMATICALLY REMEDIATES INACTIVE ACCOUNTS WITH ELEVATED PERMISSIONS, ENSURING COMPLIANCE WITH NIST STANDARDS.	AUTOMATICALLY DISABLES DORMANT ACCOUNTS IN A CLOUD ENVIRONMENT TO ALIGN WITH NIST AC-2(3)(D).
SOX COMPLIANCE	OVER-PERMISSIONED ACCOUNTS IN FINANCIAL SYSTEMS LEAD TO UNAUTHORIZED CHANGES, RISKING SOX COMPLIANCE.	IDENTIFIES AND REMOVES EXCESSIVE PRIVILEGES IN FINANCIAL SYSTEMS, REDUCING SOX COMPLIANCE RISKS.	REMEDIATES OVER-PERMISSIONED USER ROLES IN ERP SYSTEMS TO AVOID UNAUTHORIZED FINANCIAL TRANSACTIONS UNDER SOX.
AICPA SOC	THIRD-PARTY VENDOR ACCOUNTS WITH EXCESSIVE PRIVILEGES COMPROMISE SOC2 TRUST PRINCIPLES.	ANALYZES THIRD-PARTY ACCOUNTS FOR OVER-PERMISSIONING AND APPLIES LEAST PRIVILEGE PRINCIPLES TO ALIGN WITH SOC2 REQUIREMENTS.	REDUCES THIRD-PARTY ACCESS PRIVILEGES IN SAAS APPLICATIONS, MAINTAINING SOC2 CONFIDENTIALITY REQUIREMENTS.
ISO 27001	LACK OF CONTINUOUS MONITORING OF IDENTITIES INCREASES THE RISK OF UNAUTHORIZED ACCESS, VIOLATING ISO 27001 ANNEX A.9.	PROVIDES CONTINUOUS POSTURE ANALYSIS AND IDENTITY RISK REMEDIATION TO ENSURE COMPLIANCE WITH ISO 27001 RISK MANAGEMENT.	AUDITS AND CORRECTS ADMINISTRATOR PERMISSIONS IN PAYMENT PROCESSING SYSTEMS TO MEET PCI-DSS REQUIREMENTS.
PCI DSS COMPLIANT	OVER-PERMISSIONED ADMINISTRATOR ACCOUNTS EXPOSE CARDHOLDER DATA, VIOLATING PCI-DSS STANDARDS.	FLAGS AND REMEDIATES ADMINISTRATOR ACCOUNTS WITH UNNECESSARY PERMISSIONS TO PROTECT CARDHOLDER DATA.	IDENTIFIES ACCESS RISKS IN SHARED STORAGE SYSTEMS AND APPLIES CONTROLS TO MEET ISO 27001 STANDARDS.
CIS	MISCONFIGURED USER ACCOUNTS DO NOT ADHERE TO CIS BENCHMARKS FOR SECURE IDENTITY PRACTICES.	IDENTIFIES AND FIXES MISCONFIGURATIONS IN USER ACCOUNTS TO MEET CIS BENCHMARKS FOR SECURE PRACTICES.	FIXES MISCONFIGURED IDENTITY POLICIES ON CRITICAL SERVERS TO ADHERE TO CIS BENCHMARKS.

PROTECTION AND REMEDIATION

Lateral movement case study

71% of ransomware attacks leverage credential access tactics, and more than 80% of cyberattacks involve compromised credentials. This makes lateral movement a common attack method, highlighting how attackers exploit stolen identities to move undetected across networks.

Even with visibility and strong identity hygiene, attackers continuously evolve their techniques to bypass security controls and compromise identities within enterprises. This underscores the importance of continuous monitoring of identities and their activities, as behavioral monitoring and anomaly detection enable early threat identification. These signals help administrators spot potential compromises early, triggering alerts when suspicious patterns emerge.

Lateral movement has become one of the most widely used techniques in cyberattacks. This method enables adversaries to escalate a localized breach into a full-scale organizational compromise. To counter this, enterprises must implement layered protection mechanisms. This report focuses on two major technologies for modern identity protection:

1. Identity Threat Detection and Response (ITDR)
2. Deceptive technologies leveraging honeytokens

IDENTITY THREAT DETECTION AND RESPONSE (ITDR)

Use Cases

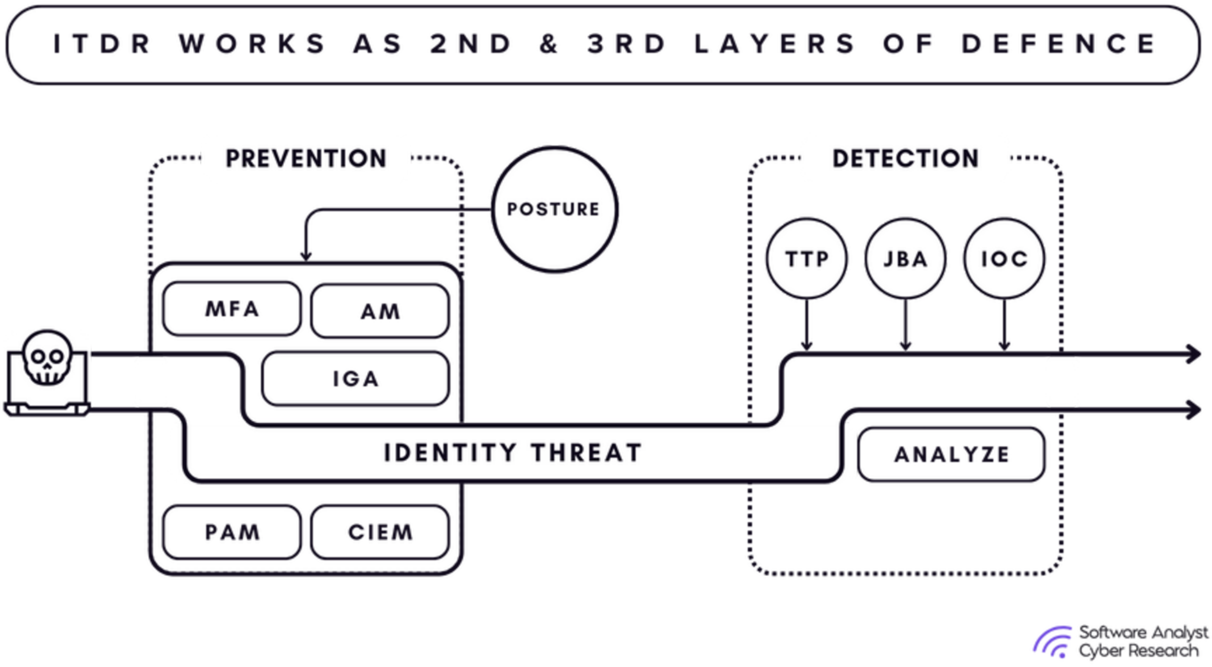
The reality is that traditional security solutions, such as Endpoint Detection and Response (EDR), Privileged Access Management (PAM), and network segmentation, have failed to stop lateral movement. These solutions either lack visibility into authentication activity or only protect privileged accounts, leaving standard user accounts vulnerable. Additionally, Active Directory (AD) inherently trusts valid credentials, making it unable to differentiate between a legitimate user and an attacker using stolen credentials. This fundamental limitation leaves organizations exposed to identity-based threats.

Enter ITDR. ITDR directly addresses these blind spots by continuously monitoring authentication requests, detecting anomalies in user behavior, enforcing real-time multi-factor authentication (MFA) verification, and blocking unauthorized access before attackers can pivot to additional resources. ITDR solutions analyze user behavioral anomalies, authentication protocol changes, and external risk signals to detect identity threats. Some solutions leverage IOCs, TTPs, MIT&RE framework and risk analysis to differentiate between normal and malicious activity. By integrating natively with IAM infrastructure, ITDR integrates directly with IAM and proactively blocks threats before access is granted. ITDR ensures comprehensive protection across all authentication protocols, including command-line access tools like PsExec and Remote PowerShell, which are frequently abused for lateral movement. Given that 24 billion compromised credentials are circulating on the dark web, proactively detecting and disrupting lateral movement attacks in real time is no longer optional—it is a necessity for a robust identity security strategy.

Additionally, MFA and ITDR work in tandem to enhance security. Strong MFA, supported by posture and hygiene solutions, allows ITDR to validate access attempts automatically, minimizing false positives and reducing the SecOps workload. With MFA, ITDR can block identity threats in real time, ensuring that only verified access attempts are allowed.

When selecting an Identity Threat Detection and Response (ITDR) solution, organizations must evaluate its coverage, detection accuracy, and response capabilities. An effective ITDR platform should integrate seamlessly with all identity and access management (IAM) solutions, whether on-premises or in the cloud, ensuring comprehensive protection across Active Directory (AD), cloud identity providers (IdPs), VPNs, and SaaS applications. It must accurately identify a broad spectrum of identity threats, including credential theft, lateral movement, and privilege escalation, while offering real-time mitigation rather than relying solely on reactive alerts.

Real-time threat detection leverages machine learning and anomaly detection to identify unusual authentication patterns, such as impossible travel logins, credential stuffing attacks, and unauthorized lateral movement within hybrid environments. Behavioral analytics for high-privilege accounts further enhance security by continuously monitoring privileged user sessions and enforcing risk-based conditional access controls.


ITDR WORKS AS 2ND & 3RD LAYERS OF DEFENCE
PREVENTION
POSTURE
MFA
AM
IGA
PAM
CIEM
IDENTITY THREAT
DETECTION
TTP
JBA
IOC
ANALYZE
Software Analyst Cyber Research

DECEPTIVE TECHNOLOGIES AND ITDR

Deceptive technologies, such as honeytokens and honey accounts, play a critical role in Identity Threat Detection and Response (ITDR) by providing early detection of identity-related attacks. Enterprises leverage deception to protect identities across on-premises and multi-cloud environments, addressing key gaps in traditional ITDR approaches.

Traditional detection methods struggle to distinguish between legitimate and malicious usage of valid accounts, leaving blind spots in Active Directory (AD) logs, domain controllers, and endpoint detection response (EDR) systems. Attackers frequently exploit stolen credentials, including SAML/JWT tokens and offline attacks like Kerberoasting, as well as emerging zero-day identity threats that bypass conventional security measures. By deploying deceptive identities within credential caches and creating honey accounts, organizations can lure adversaries into revealing their presence without relying solely on log correlation.

The NSA and Five Eyes intelligence agencies recommend honeytokens as an effective strategy for detecting AD compromises, as they provide strong indicators of unauthorized access. Vendors like Acalvio's Identity Protection enhance ITDR by deploying honeytokens that remain attractive to attackers while integrating seamlessly with security operations. This approach extends beyond AD to multi-cloud environments, where identity remains a top attack vector. Cloud-based adversaries increasingly exploit IAM misconfigurations, API-based attacks, and privilege escalation techniques to gain unauthorized access.

More enterprises are deploying honeytoken traps alongside their ITDR solutions. Honeytokens in cloud environments—including IAM roles and deceptive access keys—provide real-time threat intelligence by alerting security teams to unauthorized activity before an attack escalates.

For example, CrowdStrike partners with Acalvio to enable comprehensive ITDR with a defense-in-depth strategy that combines traditional detection methods with deception technology. Their autonomous deception farms simplify deployment at scale, securing enterprises with thousands of endpoints and complex identity environments. A real-world case study highlights how a honeytoken exposed a malicious insider who attempted to manipulate user provisioning scripts—an attack that bypassed other security controls but was immediately detected through deception.

REMEDIATION CAPABILITIES

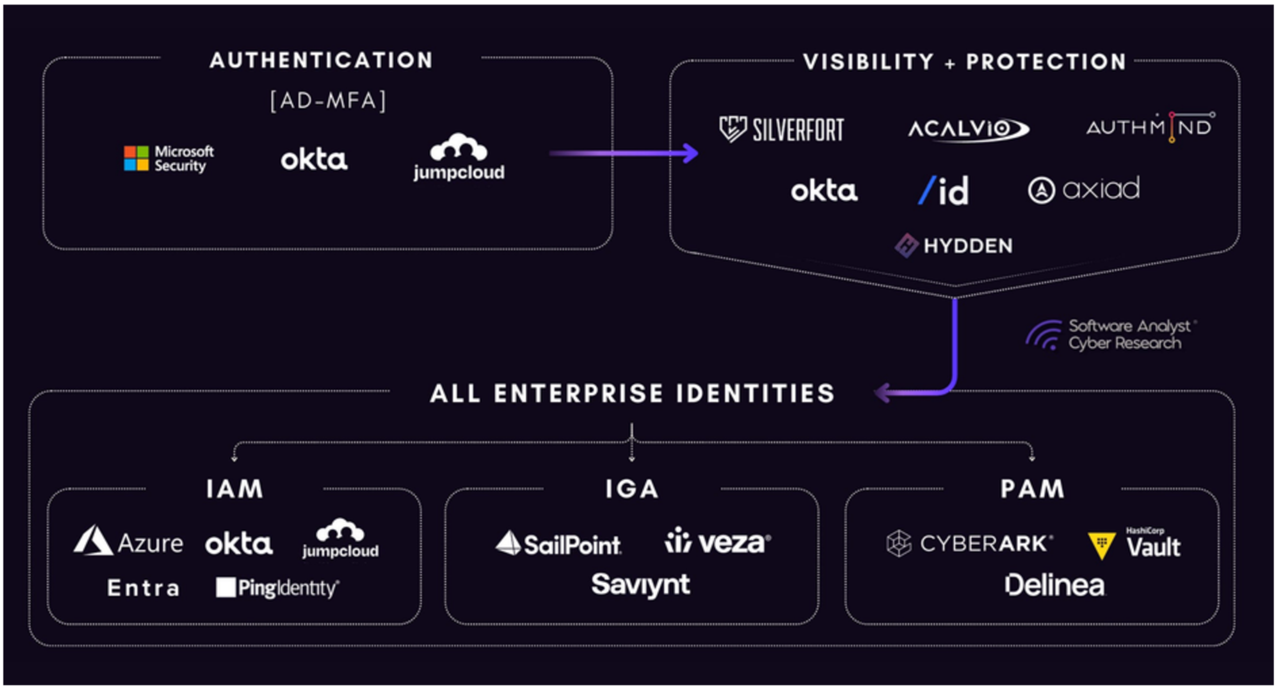
Effective remediation is a critical component of identity protection, ensuring that detected threats do not escalate into full-blown security breaches.

Remediation is the final and often most important step in the security process, encompassing visibility, posture, and protection. All identity security technologies should incorporate strong remediation capabilities. Upon detecting an identity compromise, an automated incident response mechanism should take immediate action, such as locking compromised accounts, triggering step-up authentication via MFA, and integrating with SOC and SIEM platforms for threat correlation and response orchestration. For ITDR vendors, sending alerts to a SIEM or data lake is often considered table stakes. Additionally, forensic analysis and post-incident reporting play a critical role in strengthening identity security by providing detailed audit logs that allow security teams to investigate attack patterns and proactively mitigate future risks.

For example, in a real-world ITDR deployment, a financial institution’s security system detected an unauthorized administrator login attempt from a foreign location at 5 AM. The ITDR platform immediately flagged the anomaly, triggered an automated account lockdown, and enforced MFA re-authentication, effectively preventing a privilege escalation attack. Other key aspects of an effective ITDR response include automated threat containment and security posture adjustments, as discussed earlier. Upon detecting a suspicious authentication attempt, ITDR solutions must immediately disrupt active identity threats through mechanisms like session termination, universal logout, and privilege revocation. This case highlights how ITDR’s real-time monitoring, automation, and identity analytics enable organizations to proactively block identity-based attacks before they escalate.

Beyond immediate mitigation, ITDR also enhances long-term security posture by feeding threat intelligence back into identity hygiene and risk management practices. It enables organizations to reduce the IAM attack surface by revoking excessive permissions, adjusting role-based access, and ensuring continuous identity monitoring.

IDENTITY ATTACK SURFACE REPRESENTATIVE VENDORS



VISIBILITY & POSTURE

- Hydden
- Axiad
- Silverfort

PROTECTION & REMEDIATION

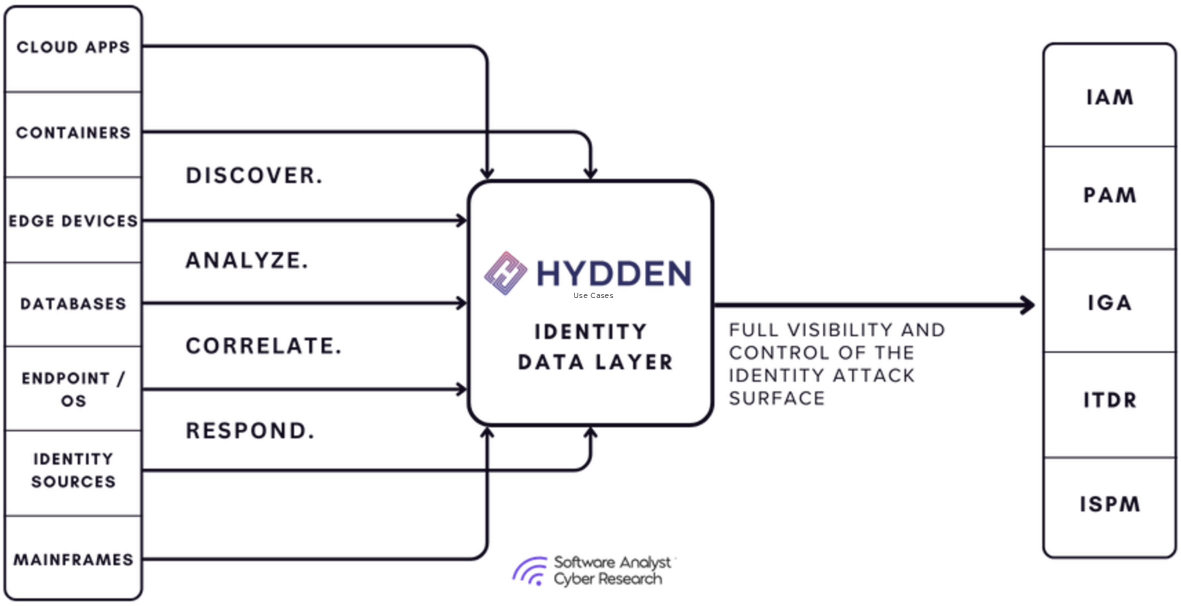
- Silverfort
- Authmind
- SlashID
- Acalvio

Note: *this isn't a fully holistic list of hundreds of vendors providing adjacent solutions, but a few vendors selected as representative vendors.*

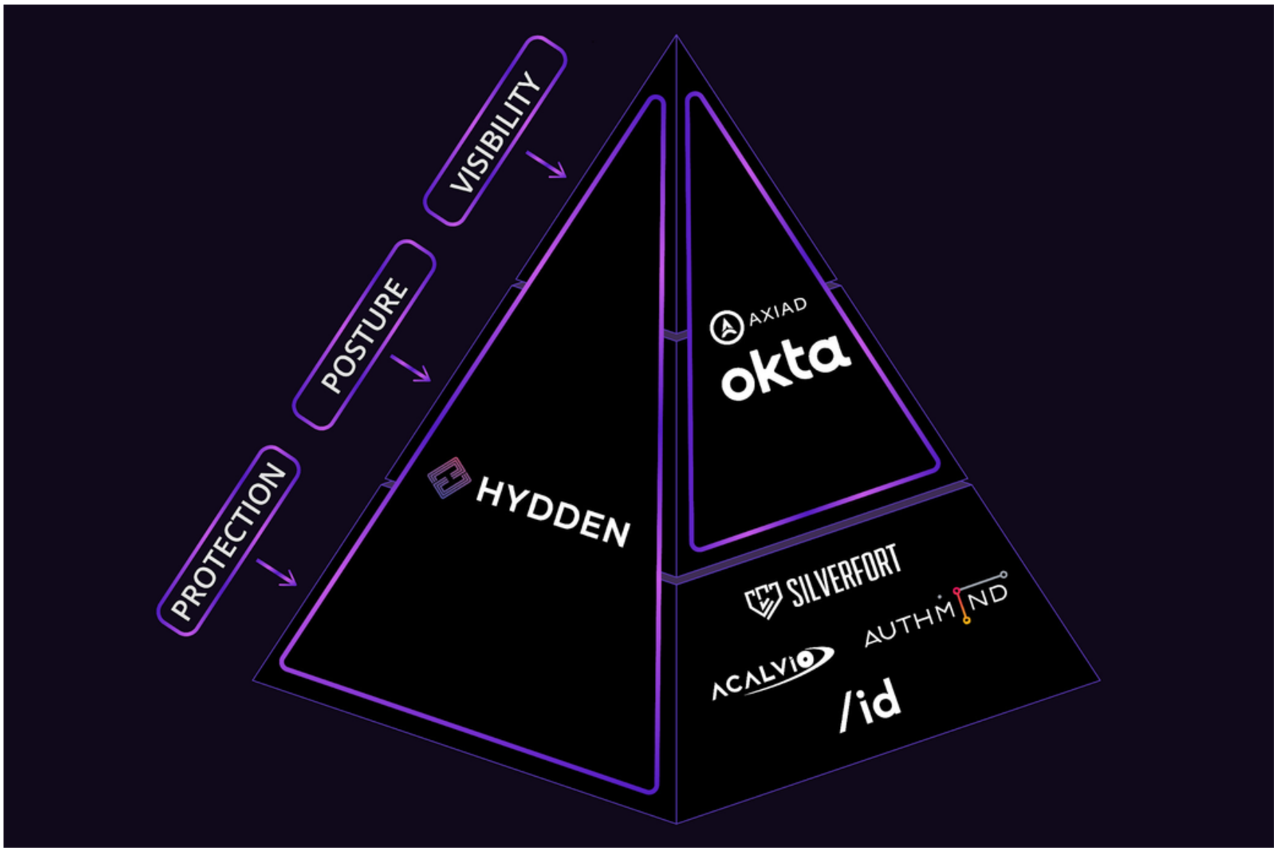
HYDDEN

IDENTITY FOCUSED ON IDENTITY SURFACE PROTECTION

Hydden is an emerging vendor with strong capabilities in enhancing the visibility and discovery of all identities across existing identity solutions today. They focus on identity attack surface management by mapping non-human identities (NHI) and human identities across the enterprise. Hydden helps organizations identify orphaned accounts, misconfigured identities, and security gaps in multi-cloud, on-prem, and hybrid environments.



The system automates threat detection and risk scoring based on predefined security rules and frameworks (e.g., NIST CSF v2.0). Users can classify identity risks on a scale from 1 to 10 and customize them based on historical threats (e.g., password spraying, orphaned accounts).



RISK CLASSIFICATION & THREAT SCORING

Dynamic risk scoring, identified earlier in the report, is critical for successful vendors that produce outcome driven results. Hydden showed an impressive capability around assigning contextual identity risk scores, classifying identities based on exposure, misconfigurations, and access patterns.

This enhances threat modeling capabilities by prioritizing security responses based on attack likelihood and impact. If an anomaly is detected, the system flags suspicious activity, such as unauthorized travel logins or excessive permissions. Hydden's risk engine not only assigns a threat score but also provides confidence levels and contextual relationships (e.g., linking identities to SaaS applications, AD entitlements, and MFA status).

HYDDEN & CYBERARK PARTNERSHIP

Hydden recently struck a partnership with CyberArk for privileged access management (PAM) and vaulting credentials.

Hydden enhances CyberArk Privileged Access Manager (PAM) by providing 100% visibility into the entire identity attack surface. By creating a unified data layer, Hydden continuously tracks and analyzes identity security posture and threat indicators, ensuring that every privileged identity is securely managed, vaulted, and monitored in real time. With Hydden's privileged identity discovery, CyberArk customers can automatically detect and vault all accounts that should be, but are not yet, secured within CyberArk Safes.

CyberArk Privileged Access customers utilize this analysis to ensure every identity is securely managed and continuously monitored for any external changes by Hydden. A few notable things from this partnership include:

1. **Automated Account Classification** – Hydden classifies privileged accounts (e.g., accounts ending in tagged as Dual Admin Accounts) to determine if they should be vaulted
2. **Human & Non-Human Visibility & Mapping** – Hydden provides full context and risk scoring for every account, aiding in connecting CyberArk users, machine accounts, and service identities to their rightful owners. This also aids in simplifying vaulting decisions.
3. **Security Hygiene & Risk Assessment** – Hydden identifies orphaned, stale, and compromised accounts, as well as privileged identities with no MFA or excessive entitlements.

HYDDEN & CYBERARK PARTNERSHIP

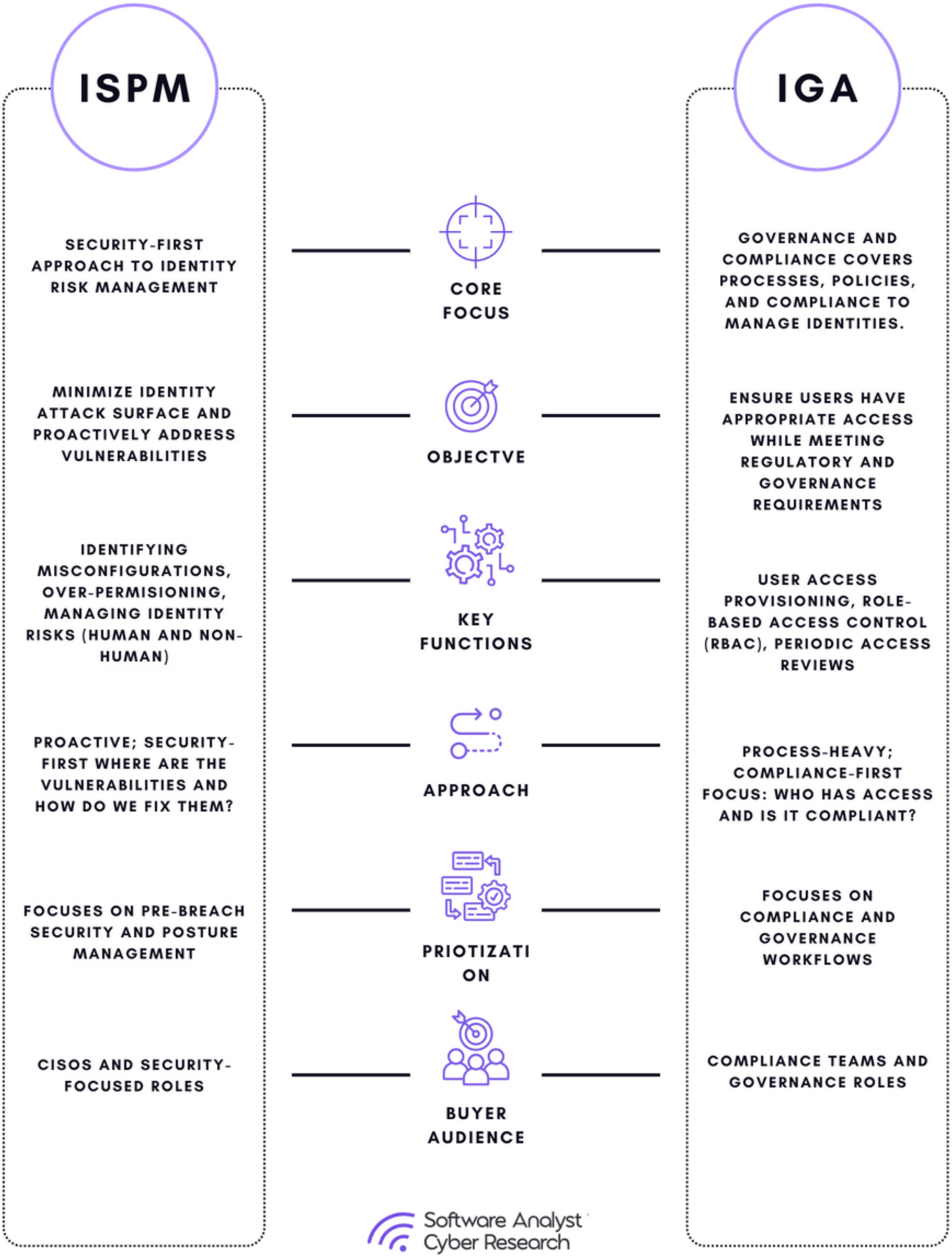
What stood out as a key advantage of this integration is Hydden’s ability to discover accounts across platforms, systems, and applications that typically fall outside CyberArk's standard discovery scope. Beyond PAM, Hydden provides the "visibility foundation" for IGA, PAM, and security platforms. They have built extensive integrations across multi-cloud & hybrid environments.

Automation and Remediation

Hydden integrates with automated security response workflows, allowing for trigger-based automation (e.g., automatically flagging and deactivating an account based on security violations). The platform automates identity posture management and alerts users to pending MFA setups, misconfigurations, and suspicious activities.

APPENDIX: ISPM VS IGA

Many industry practitioners are familiar with IGA. Some of the key components for what IGA does.



ISPM		IGA
SECURITY-FIRST APPROACH TO IDENTITY RISK MANAGEMENT	CORE FOCUS	GOVERNANCE AND COMPLIANCE COVERS PROCESSES, POLICIES, AND COMPLIANCE TO MANAGE IDENTITIES.
MINIMIZE IDENTITY ATTACK SURFACE AND PROACTIVELY ADDRESS VULNERABILITIES	OBJECTVE	ENSURE USERS HAVE APPROPRIATE ACCESS WHILE MEETING REGULATORY AND GOVERNANCE REQUIREMENTS
IDENTIFYING MISCONFIGURATIONS, OVER-PERMISIONING, MANAGING IDENTITY RISKS (HUMAN AND NON-HUMAN)	KEY FUNCTIONS	USER ACCESS PROVISIONING, ROLE-BASED ACCESS CONTROL (RBAC), PERIODIC ACCESS REVIEWS
PROACTIVE; SECURITY-FIRST WHERE ARE THE VULNERABILITIES AND HOW DO WE FIX THEM?	APPROACH	PROCESS-HEAVY; COMPLIANCE-FIRST FOCUS: WHO HAS ACCESS AND IS IT COMPLIANT?
FOCUSES ON PRE-BREACH SECURITY AND POSTURE MANAGEMENT	PRIOTIZATION	FOCUSES ON COMPLIANCE AND GOVERNANCE WORKFLOWS
CISOS AND SECURITY-FOCUSED ROLES	BUYER AUDIENCE	COMPLIANCE TEAMS AND GOVERNANCE ROLES

Software Analyst Cyber Research

CONCLUSION:

THE FUTURE OF IDENTITY ATTACK SURFACE MANAGEMENT

As the digital landscape continues to expand, identity has become the new perimeter in cybersecurity. The rise of non-human identities, the increasing complexity of multi-cloud environments, and the acceleration of identity-based attacks demand a more holistic and proactive approach to security.

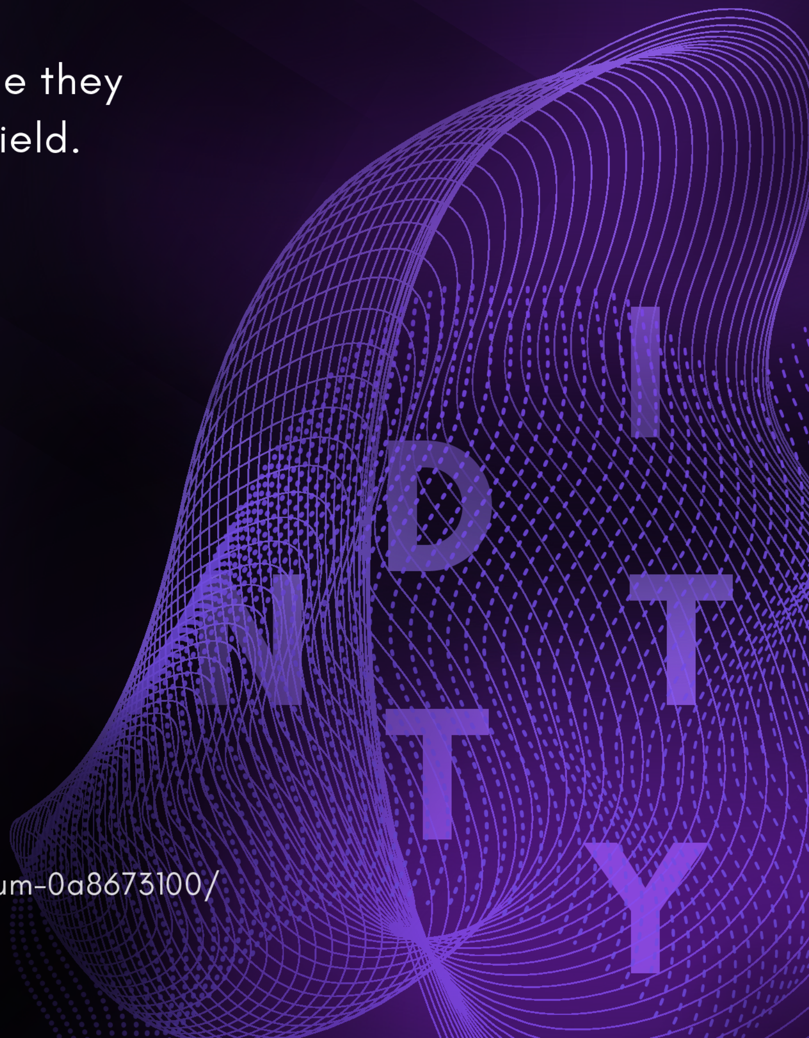
This report highlights that Visibility, ISPM, and ITDR form the foundation of a resilient identity security strategy. Visibility ensures organizations understand their attack surface, ISPM enforces proper security hygiene to minimize risk, and ITDR provides real-time detection and response to evolving threats. Together, these elements create a robust defense mechanism that adapts to modern identity-driven threats.

Going forward, organizations must embrace automation, AI-driven analytics, and continuous identity monitoring to stay ahead of attackers. Identity security is no longer just an IT function—it is a business imperative that impacts regulatory compliance, operational resilience, and trust. By prioritizing Identity Attack Surface Management, enterprises can significantly reduce the risk of identity compromise, privilege abuse, and supply chain attacks, ensuring that their most critical assets—identities—remain secure in an increasingly interconnected world.

Software Analyst®
Cyber Research

ABOUT

Software Analyst Cybersecurity Research (SACR) delivers in-depth analysis of the ever-evolving cybersecurity industry. Specializing in SOC, Identity, Network, Cloud, AppSec, and AI Security, our mission is to empower CISO's, security leaders, investors, and cybersecurity professionals with the knowledge they need to navigate this complex field.



https://x.com/InvestiAnalyst

https://softwareanalyst.substack.com/

https://www.linkedin.com/in/francis-odum-0a8673100/