BEST PRACTICE GUIDE

IDENTITY ATTACK SURFACE MANAGEMENT:

VISIBILITY DRIVES SECURITY

HYDDEN

Table of Contents

Introduction 1

The Evolution of Identity Security 2

Attack Surface Management (ASM) and the Emergence of Identity Specific IASM 2

Traditional Identity Security Limitations 2

IASM's Unique Perspective 4

Alignment with Attacker Methodology 4

Integration with IAM Building Blocks 5

Authentication and Access Management Assurance 6

Privileged Access Management Enhancement 6

Identity Governance & Administration Fortification 7

Zero Trust Alignment 8

The Critical Role of Legacy System Integration 8

Future Trends and Considerations 9

Conclusion 10

Introduction

The enterprise identity landscape has become extraordinarily complex and fragmented. Organizations must manage human and non-human identities across on-premises systems, cloud environments, legacy applications, and modern microservices architectures. This complexity has created an expansive attack surface that traditional identity cybersecurity solutions struggle to address fully. As a result, Identity Attack Surface Management (IASM) has emerged as a critical capability for organizations seeking to protect their expanding identity perimeter.

Recent high-profile breaches have demonstrated that compromised identities remain the primary vector for cyber-attacks. For example, the root cause of the Change Healthcare cyber attack that impacted 190 million people was a server that did not have two-factor authentication enabled. According to industry research, 90% of organizations experienced an identity-related breach in the past year, with 93% of these breaches being preventable through more robust identity security measures. 50% of organizations said implementing privileged access controls could have prevented or minimized the effect of incidents, followed by timely reviews of access to sensitive data (42%) and implementing MFA for all users (37%).

90% Organizations experiencing an identity-related breach in the past year

93% Breaches preventable through more robust identity security measures

37% Organizations acknowledging MFA would have prevented or minimized damages

*Reference: https://www.idsalliance.org/white-paper/2024-trends-in-securing-digital-identities/

At its core, IASM is a comprehensive, end-to-end approach to discovering, monitoring, and securing every identity everywhere. An enterprise's identity attack surface is continually expanding. Every new employee, contractor, device, integration, and application involves the creation of new identities and credentials that are entry points to corporate systems. This best practice guide examines the evolution of IASM, its crucial role in modern cybersecurity programs, and why comprehensive visibility across all IT assets is fundamental to effective identity security.

The Evolution of Identity Security Attack Surface

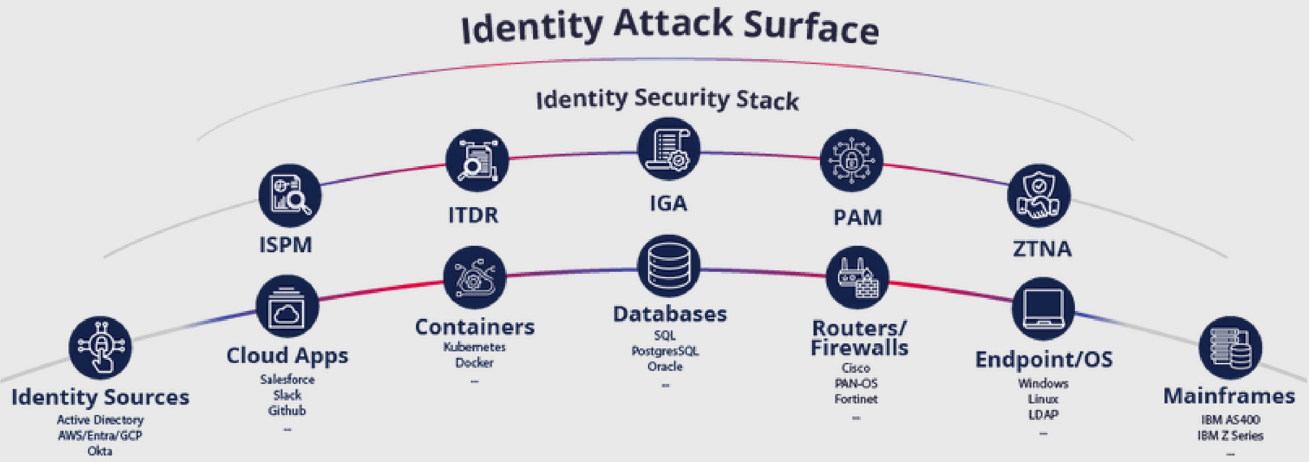
Attack Surface Management (ASM) and the Emergence of Identity Specific IASM

IASM emerged as a response to the growing recognition that identity-related vulnerabilities are found quite frequently within organizations, and in many cases are often easier for threat actors to exploit. Attack Surface Management (ASM) is an established sector that focuses primarily on system visibility and leans heavily into aspects of application security risks, such as vulnerability information. But it became clear that identity-based risks were increasingly exploited in breaches, particularly as organizations expanded their cloud presence, adopted hybrid environments, and embraced remote work. ASM alone was not comprehensive enough to address the unique identity risks associated with large and diverse environments.

As a result, IASM emerged as a dedicated practice to proactively manage identity risks within the broader ASM framework. It focuses on first providing comprehensive centralized visibility into all identities that are stored on or have access to each asset. Secondly, it highlights hygiene and risk issues related to the identities discovered. Lastly, it focuses on being able to take action to correct these risks. While ASM provides a broader approach to managing organizational security risks across various digital touchpoints, IASM zooms in on the specific threats associated with identities. In essence, IASM is a necessary sub-category of ASM, addressing the specialized threat landscape posed by identity-based vulnerabilities.

Traditional Identity Security Limitations

The other market force that caused IASM to emerge are the limitations around identity visibility in today's most widely used products. Managing the identity attack surface requires a holistic approach. A crucial part of this approach is a unified framework that ensures all security teams are working off the most up-to-date identity data. This strategy is instrumental in breaking down silos across teams and ensures all teams are easily sharing information, creating integrated policies, and acting upon the same data. This is how IASM serves as a strategic layer that cuts horizontally across the major identity security categories of IAM, IGA, and PAM. Solutions in these traditional categories are already extremely feature-rich but organizations have been hindered by their lack of continuous identity discovery and are unable to utilize their advanced capabilities. However, with an IASM platform, existing solutions are integrated and utilized to take remediating action or mature an existing implementation based on the analysis performed over data that is continuously collected. For example, IASM solutions will uncover any privileged accounts that are not securely vaulted and will enable you to directly vault them with your PAM credential manager.



Conventional Identity and Access Management solutions have focused primarily on authentication and authorization mechanisms (IAM), account lifecycle management and access certification (IGA), password management and vaulting (PAM), and ensuring that these solutions align with Zero Trust identity principles. While these capabilities remain essential, they operate on the assumption that organizations have complete visibility into their identity ecosystem. Additionally, these critical capabilities often operate in isolation, creating gaps in security coverage between these products. IASM cuts across these traditional boundaries by providing a comprehensive overlay that monitors and manages:

- Configuration states and hygiene across all identity types (B2E, B2C, machine)
- Attribute and event changes, including centralized auditing
- Compliance and framework alignment
- Identity risk, threat assessments and remediation actions

IASM’s Unique Perspective

With ASM’s lack of focus on identity combined with the limitations of traditional IAM approaches, IASM solutions began providing capabilities to proactively limit all potential points of exposure through which unauthorized actors can compromise, steal, or misuse user identities to gain access to systems, data, and services. This represents a paradigm shift from managing known identities to discovering and securing the entire identity attack surface, including unknown and potentially risky identity assets. Identity Attack Surface Management puts organizations in a position of strength by understanding how an attacker would perceive their identity attack surface and which areas that organization should prioritize based on the level of criticality so the organization can then transition to a proactive approach to managing identity risks.

Alignment with Attacker Methodology

IASM's strategic value derives from its alignment with an actual attacker’s methodologies. Threat actors don't care about organizational boundaries or security solution categories. They target any exposed identity regardless of its classification, exploit weak controls wherever they exist in the identity ecosystem, leverage cross-system vulnerabilities that may not be visible within individual security solutions, and seek the path of least resistance, often combining a variety of tools, techniques, and procedures to achieve their goals. Their approach is opportunistic and holistic.

Identity Attack Surface Management gets you to think like the attackers by continuously scanning for and identifying exposed credentials, risky access patterns, and potential identity-based attack vectors that malicious actors could exploit. Rather than simply enforcing static policies, IASM actively discovers and maps the complete identity landscape, including dormant accounts, excessive privileges, disabled accounts, and exposed credentials across cloud services, third-party applications, and development environments. This allows an organization to surface these paths of least resistance and prioritize correcting identity-based risks.

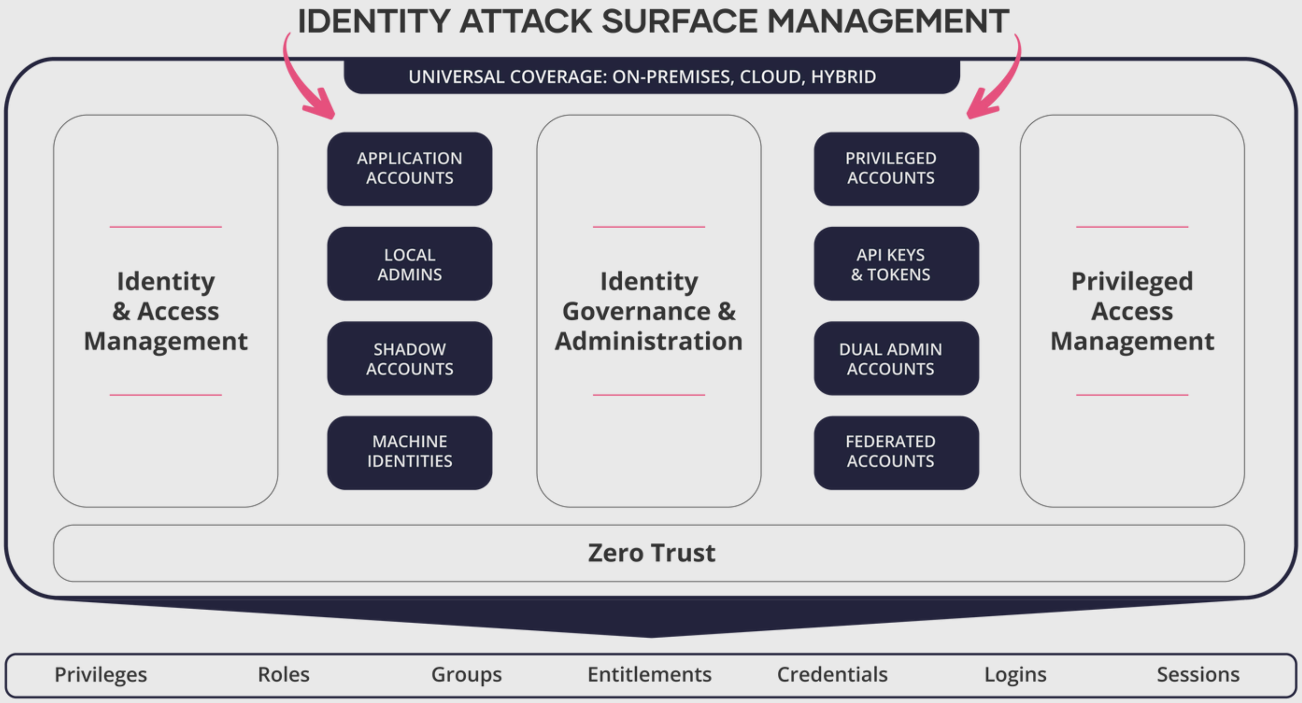
This proactive security approach to identity protection does not replace traditional IAM tools but rather enhances their effectiveness by providing critical intelligence about real-world exposure and attack paths that can inform more targeted hardening of identity controls. This shift will transform a security practice from implementing a control to check a box to maturing the identity building blocks already in place.

Integration with IAM Building Blocks

Discovery is the backbone of an IASM solution. This process involves identifying and cataloging all user accounts to provide a clear, real-time view of who is accessing what resources and ongoing monitoring of user activities to detect anomalies that could indicate a security threat. Discovery typically involves three different processes:

1. Querying target systems and applications using their APIs or direct log data
2. System and identity log parsing standardization and analysis
3. Event and attribute-driven data capture

These processes collectively provide comprehensive visibility into all identities across all IT assets. This data is then used to continuously monitor and track changes over time at the individual identity and account level to detect identity-based threats. The following sections outline how Identity Attack Surface Management platforms provide this data layer of discovered identities and threat detection analysis to other existing IAM investments.



Authentication and Access Management Assurance

IASM solutions continuously monitor identity configurations, access privileges, and changes in real time—across infrastructure, endpoints, devices, systems, and applications. This proactive approach prevents unauthorized changes that increase your attack surface and automatically remediates security posture issues to minimize risk and maintain a secure identity hygiene.

IASM ensures robust authentication and access management by:

- Eliminating poor security posture: Uncover, remediate, and prevent identity hygiene issues that increase risk like stale passwords, accounts without MFA, dormant accounts, compromised credentials, and many other indicators of risk
- Quantifying potential blast radius: Prioritize the most vulnerable accounts based on risk score and understand the entire blast radius of a compromised identity
- Monitoring authentication patterns: Track anomalous activity like failed logins and bypassing MFA as indicators of compromise
- Monitoring unexpected identity events: discover suspicious account creation or deletion events or honeypot implementations

Privileged Access Management Enhancement

Today's PAM solutions were not designed to collect identities continuously, leaving large periods of time where additions, removals, and changes to accounts are entirely missed. Many PAM solutions focus on scanning individual systems for discovering accounts, which is often prone to errors due to network communication requirements or other environmental complexities such as permissions or scripts. These discovery issues have created massive identity security blind spots, especially as the number of human and machine accounts required to implement and integrate security tools and business applications has rapidly increased. These blind spots result in poor identity hygiene and misconfigurations that lead to cyber exposure. Modern PAM tools require real-time data to better inform contextual-based access policies that require granular access control. With IASM providing an identity data layer, PAM tools can attain total coverage of privileged human and machine identities across every on-premise or SaaS infrastructure, application and system to ensure dynamic and agile control.

IASM augments PAM by:

- Widening the scope to be inclusive of all potential sources of identities: Uncover “shadow” user and machine accounts that are not in your secrets vault to ensure applicable governance policies are applied
- Improving privileged group management: Ensure high risk privileged accounts and groups changes are routinely monitored and align with just-in-time and just-enough-privilege principles
- Identifying unauthorized privilege escalation paths: Enforce least privilege for every single account across your identity ecosystem
- Monitoring privileged account usage patterns: Detect anomalous privileged account activity and take remediating action to prevent unauthorized access to security controls, devices, workstations, and applications
- Detecting misconfigured privilege assignments: Automatically correlate multiple human and machine accounts to a single identity to ensure a human account owner has the same privileges applied for all account on all target systems

Identity Governance & Administration Fortification

Identity blind spots can occur with legacy IGA solutions that do not scale, utilize outdated integrations, and require heavy customizations for extensibility. With IASM, a foundational identity data layer guarantees both modern and legacy IGA solutions can manage every identity in real-time.

IASM strengthens IGA through:

- Continuous access policy validation: Guarantee complete identity lifecycle governance by automatically correlating multiple human and machine accounts to a single identity and applying applicable governance policies to every account that is owned by the same human
- Cross-system entitlement correlation: Validate access rights on disparate systems, streamlining and expedite user reviews
- Automated identity risk assessment: Threat and risk analysis of every discovered identity based on adherence to best practices
- Compliance monitoring and reporting: Automatically map security issues and best practice violations to the top standards and frameworks like ISO, NIST, CRI, and GDPR

Zero Trust Alignment

Align your identity solutions with Zero Trust principles by cleaning up and enforcing standardized controls across a hybrid, on-premise, and multi-cloud landscape. Control identity sprawl, compare access across distributed systems, and reduce management complexity for a zero-trust security program.

IASM helps organizations align with Zero Trust principles by:

- Ensuring MFA is universally enforced: Provide a comprehensive centralized view of MFA status and MFA type information where possible.
- Ensure identity stores adopt use of federated credentials: Ensure adoption of SSO grows over time and local accounts decline across applications
- Ensure risk assessments extend to identities: Align identity specific configuration and policy settings across identity stores
- Identifying zero standing privilege permanent privilege assignments: Continuous discovery provides full visibility and scales to discover every account's access rights and monitor changes so that you can reliably monitor groups membership to maintain zero standing privileges
- Monitoring just-in-time access usage: Comprehensive auditing and behavioral analytics to precisely control and monitor ephemeral access
- Validating privilege elevation workflows: Automatically detect, validate, and reconcile access rights, proactively removing unnecessary permissions and minimizing potential attack surfaces

The Critical Role of Legacy System Integration

Across IAM, PAM, IGA, and zero-trust implementations, legacy systems present unique challenges, like outdated authentication mechanisms and limited logging capabilities that can limit discovery capabilities. Effective IASM solutions overcome these challenges by developing advanced compatibility frameworks across these complex, interdependent technological ecosystems. IASM solutions must support legacy protocols and authentication methods, provide non-intrusive monitoring capabilities, and offer flexible API and connector frameworks, allowing organizations to take a gradual modernization path. Additionally, some legacy systems simply do not offer methods to acquire identity information through APIs. Connector frameworks must be versatile enough to ingest identity data through syslog exports and consume identity data from other proprietary log files.

Future Trends and Considerations

Organizations should prepare for emerging trends and new tactics that threat actors will leverage to compromise identities. This will influence how IASM may evolve and develop future capabilities. The following key development areas stand out as areas to watch:

AI and Machine Learning Integration: The evolution of AI in identity security will enable more sophisticated pattern recognition for detecting anomalous behavior and predicting potential identity-based attacks before they occur and stopping them. At-first we expect these systems to produce a certain degree of false positives that will improve over time. This will particularly enhance the ability to identify subtle privilege escalation attempts and leverage signal correlation to detect complex attack chains that traditional rule-based systems might miss.

Personal and work device identities merge: The division between work and personal life continues to merge, expanding the potential blast radius for identity-based attacks. Employees may share or sync corporate credentials and other sensitive data to their personal accounts. But, those personal systems do not have any monitoring or security controls provided by the organization. If these systems or identities become compromised by threat actors, security teams will have no opportunity to detect and remediate the breach. It's anticipated that threat actors will extend their reach and leverage information stored in personal accounts to attack organizations, which will have an impact on the scope of IASM.

Increasing pressure to extort or blackmail victims: Some threat actors have recently begun paying for access to organizational networks, and employees are handing over access. This has been accelerated by the shift towards remote-first work environments. Other actors are targeting individuals or entire families to blackmail them to provide network access. IASM is likely going to incorporate insider risk detection components in the near future.

Zero Trust Network Access (ZTNA) Convergence: Identity solutions will increasingly integrate with ZTNA architectures, creating a more standard and predictable approach to access control and identity verification. This convergence will lead to more context-aware authentication decisions based on device posture, network location, and user behavior patterns. Many of these solutions are intended to replace VPNs. We expect these systems to be targeted soon, like the VPN solutions of today. These systems will increasingly need to become part of the scope for IASM visibility and management – especially as they integrate with PAM solutions to provide any level of automatic retrieval of passwords for connections to remote systems.

Decentralized Identity Management: The rise of blockchain-based and decentralized identity solutions will impact how organizations approach identity verification and management. This shift could fundamentally change how credentials are stored and verified, potentially reducing the risk of large-scale credential breaches.

Quantum Computing Considerations: As quantum computing capabilities advance, identity security solutions will need to adapt to quantum-resistant cryptography to protect against future threats to current encryption methods. This will affect how credentials are secured and how authentication protocols are designed.

Biometric Authentication Evolution: Advanced biometric authentication methods, including behavioral biometrics and continuous authentication, will become more prevalent in identity security solutions, particularly for high-risk access scenarios. Monitoring this adoption and ensuring compliance may become a norm, similar to MFA adoption.

Conclusion

Identity Attack Surface Management represents an inevitable evolution in an enterprises' security strategy. Organizations must move beyond traditional IAM approaches to implement comprehensive IASM solutions that provide visibility and control across their entire identity ecosystem. Success requires careful consideration of legacy systems, modern architectures, and emerging technologies, along with a structured implementation approach that balances security requirements with operational efficiency.