SPECTEROPS

IDENTITY ATTACK PATH MANAGEMENT

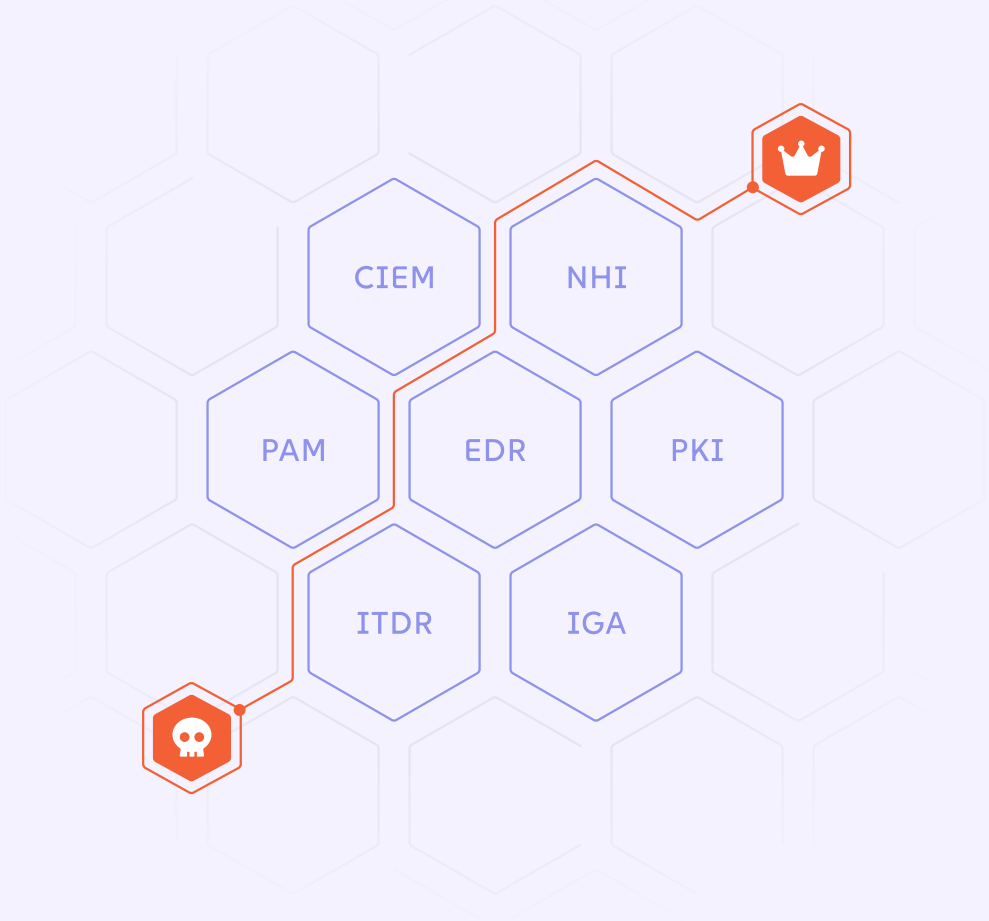
The CISO's Guide to Modern Identity Security

A strategic framework for security leaders navigating the shift from reactive incident response to proactive attack path management

Table of Contents

Being proactive means understanding adversary tradecraft. This enables you to reveal the attack paths to your business-critical assets before they're exploited. Existing security tools detect attacks and show access, but they don't prevent the paths that enable them.

Executive Summary



In nearly every major breach, attackers aren't breaking in through vulnerabilities. They're logging in with legitimate credentials and moving laterally through attack paths that already exist in your environment.

Traditional security tools excel at detecting malware and anomalous behavior, but they weren't designed to prevent the attack paths that enable lateral movement and privilege escalation. **Attack Path Management (APM) addresses this gap by continuously identifying, prioritizing, and eliminating the routes adversaries use to reach your crown jewel assets.**

Although our recent research* indicates that identity attack paths are amongst the top priorities for many organizations, we also observe that many still struggle to get a grip on identity security, despite nearly 60% of organizations increasing their spend on this very topic.

With this guide, we provide you with understanding of the issue, tools to measure your gaps and actionable steps to start growing your Attack Path Management as a practice.

* https://ghst.ly/sapm-25

Why Identity Attack Path Management Matters to Security Leaders

The Fundamental Challenge

Your existing security investments such as: Endpoint Detection and Response (EDR), Identity Threat Detection and Response (ITDR), Security Information and Event Management (SIEM) and Security Orchestration, Automation & Response (SOAR) are excellent at detecting compromise after it happens, but they don't address the underlying problem of attack paths.

Where some Vulnerability Management (VM) or Exposure Management tools may partially detect attack paths, they do not address them systematically or at the in-depth levels of identities and permissions. You're essentially installing cameras on some of your doors, while none of your doors have any locks installed.

From Reactive to Preventive

The APM approach shifts your approach from reactive to preventive. Rather than waiting to detect lateral movement, Attack Path Management (APM) identifies the paths that enable it and eliminates them before they can be exploited.

This gives you measurable risk reduction and confidence that your assets are protected against the techniques adversaries use.

Measurable Improvement Over Time

For security leaders, this means moving beyond breach response to breach prevention, with quantifiable metrics that demonstrate security improvements to boards and executives.

APM transforms identity security from a compliance checkbox into a strategic advantage and allows you to continuously monitor your identity security.

As adversaries abuse attack paths in between your existing security tools, it becomes critical to demystify adversary tradecraft. By understanding how adversaries move through your organization, you can flip the narrative.

The Operational Challenges Solved by APM

Identity APM creates alignment by providing a shared graph of privilege relationships that all teams can understand and act upon. It transforms identity security from a series of disconnected technical fixes into coordinated risk reduction with clear accountability and measurable outcomes.

Visibility Gap

Most organizations lack comprehensive understanding of how adversaries can traverse their environments, on premise, cloud, or hybrid. Traditional identity focused tools show individual permissions but miss the complex, transitive relationships that create exploitable paths to your critical assets.

Critical Asset Protection

Traditional tiered or enterprise access models provide the blueprints for best practices, but how can you verify whether your design is implemented correctly? Furthermore, modern organizations need security boundaries that align with business structure: Cloud vs. on-premises, business units, or compliance scopes. CISOs struggle with unintended attack paths that cross these logical boundaries, allowing adversaries to escalate from low-privilege environments like user systems to critical regulated assets, such as PCI or HIPAA assets. **APM with Privilege Zones capabilities enables organizations to define custom security boundaries based on business context and continuously eliminate attack paths that violate these boundaries, transforming abstract security policies into enforceable controls.**

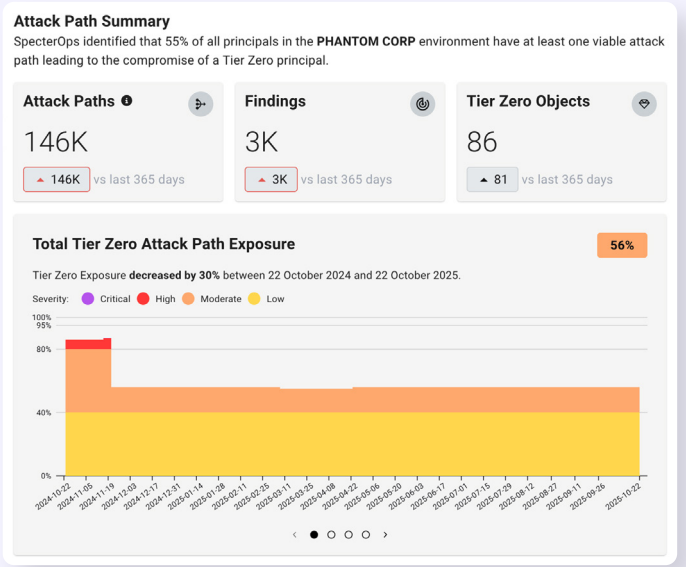
Prioritization Paralysis

Security teams are overwhelmed by thousands of identity findings from various tools, with no clear way to prioritize which issues pose the greatest risk. Without understanding impact and exploitability, teams often focus on easy fixes rather than high-impact changes. To overcome this, APM focuses on remediating strategic choke points rather than less meaningful spot-fixes.

Cross-Team Coordination

Security, Identity, and Infrastructure teams work in silos with different tools, metrics, and priorities. This fragmentation means attack path remediation efforts are often duplicated, incomplete, or blocked by organizational friction. The success of an APM practice relies on having the right stakeholders onboard across the organization.

Quantifiable Outcomes and Strategic Metrics



Risk Reduction Metrics

Track these metrics to understand identity security posture and remediation impact from a risk management perspective:

- Total active attack paths to critical identities and resources
- Current number of active choke points (findings)
- Total remediated attack paths to critical identities and resources
- Total remediated attack path choke points (findings)
- Privileged Identity Exposure

Operational Efficiency

Monitor distribution of remediation efforts across teams, such as successful remediation rate without rollbacks, mean time to remediate (MTTR), and attack path regressions (automated processes that re-insert previously fixed attack paths).

These metrics reveal whether your APM program is creating operational efficiency or organizational friction. We address the issue of identity tech dept, which is often an overlooked and underestimated issue, despite Identities being the foundation of trust within organizations.

Scope and Baseline

Ensure that the scope of your APM program is tracked to balance attack path trends with monitored identities and resources by monitoring:

- Total identities covered
- Total privileged identities monitored
- Total number of relationships between identities

Validation of Controls

From an Identity Governance and Administration (IGA) and (Internal) Audit point of view, maintaining an APM program will provide a way to continuously validate the implementation of authorization and security controls for identities. Where many tools provide limited insights from a configurational point of view, APM provides a vendor-agnostic and holistic identity risk overview.

Executive Reporting

APM provides concrete metrics for board presentations: "We eliminated 240 attack paths to domain admin privileges this quarter, reducing our organization's exposure by 34%". This transforms abstract identity risk into business-relevant security improvements across the organization, especially when applied to, for example, business units or groups of regulated assets (privilege zones).

Strategic Value

Unlike traditional security metrics that measure activity, APM metrics measure actual risk reduction. They demonstrate whether your security investments are making your organization more secure instead of just generating more alerts. These metrics can also be used in various other use cases, such as mergers & acquisitions, which typically impact the level of identity risk within an organization significantly. Attack Path Management allows you to pro-actively identify the risk of connecting or merging Identity Services.

The Business Case for Enterprise APM

Assessment Economics

Traditional Red team assessments are designed to test your detection and response processes, and they may execute only a handful of attack paths during each engagement. As Red teaming is not designed to uncover each attack path in an environment, the very nature of this type of assessment makes it an extremely costly way to identify attack paths at scale.

Proactive Identification

By proactively identifying and eliminating attack paths through Attack Path Management, you can force Red teams to focus on what they are meant to be doing: Identifying the unknown-unknowns within an environment and executing novel attack techniques while evading detection.

Scale Advantage

Assessments are typically point-in-time and limited in scope for practical considerations. This gives a limited view of the environment and its risks. With Enterprise APM solutions like BloodHound Enterprise, you continuously map millions of attack paths across your entire hybrid environment, giving you an always up-to-date view of your identity security posture.

Coverage Gap

The number of identities is always growing alongside the business. Currently for every employee there are five identities within the organization. Non-Human Identities (NHI) will accelerate this with the adoption of AI agents. This sprawl creates a gap in coverage if you are not continuously monitoring identity risks.

With an Identity APM practice you ensure continuous monitoring of the exposure of your critical identities and resources, and rapid addressing of any identified issues.

Data Enrichment

Less quantitative, but still an important factor—APM data can be utilized to further enrich other processes. APM enhances incident response decisions based on the available attack paths for each impacted identity. For example, across a collection of phishing emails or EDR alerts, APM can surface which identities have attack paths to critical assets so your team can better prioritize response actions.

Maturity Evolution: From Reactive to Strategic

Current State Reality

Most organizations operate at lower APM Maturity levels, meaning they often discover attack paths only after incidents, remediate ad-hoc without tracking, and work in departmental silos with subjective risk prioritization.

The Maturity Pathway

APM maturity progresses from ad hoc cleanup efforts (level 1) through documented processes (level 2) to enterprise-wide programs with cross-functional alignment (level 3-4) and ultimately to preventive design that avoids attack paths at provisioning time (level 5).

Identity Risk Awareness

Administering and securing identities are different aspects of identity risk management. However, by aligning on the matter across teams, there is not only a collective understanding of the issue but also an increase in the collective knowledge. This reduces chances of introducing identity risks in the first place and makes employees feel better equipped to address potential identity risks.

Strategic Transformation

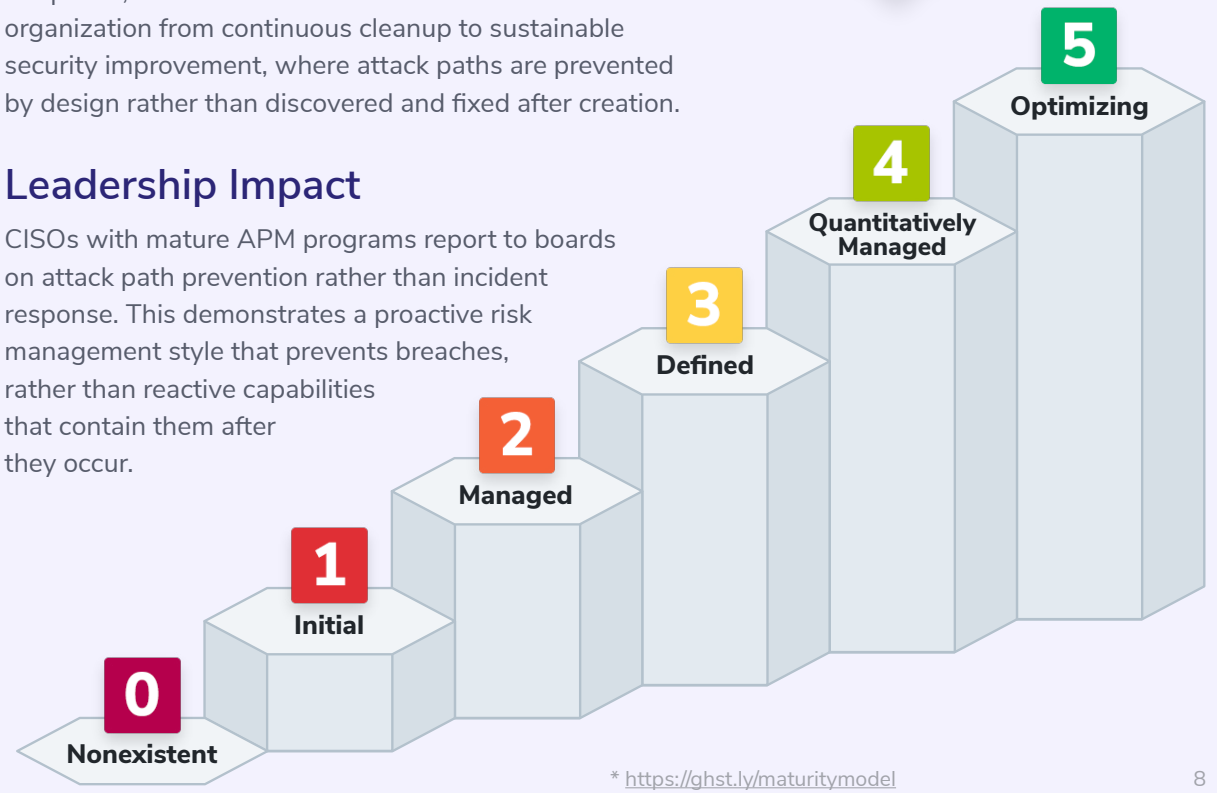
Advanced APM programs embed attack path considerations into identity governance, provisioning templates, and architectural decisions. This shifts the organization from continuous cleanup to sustainable security improvement, where attack paths are prevented by design rather than discovered and fixed after creation.

Leadership Impact

CISOs with mature APM programs report to boards on attack path prevention rather than incident response. This demonstrates a proactive risk management style that prevents breaches, rather than reactive capabilities that contain them after they occur.

Curious about your organization's APM maturity level?

Read the report* ›



* https://ghst.ly/maturitymodel

Implementation Considerations for Security Leaders

Start with Business Context

Identify your business-critical assets. These are the systems, data, and services that would create significant business risk if compromised. APM should focus on protecting what matters most, not just achieving perfect security hygiene. With APM maturity increasing, the scope can be increased to encompass other business- or compliance-driven subsets of assets.

Speed of Deployment

Getting started with an APM tool, such as BloodHound Enterprise, can be done within mere minutes. Deploy a collector into your environment, let it ingest your identity data and the APM tool will analyze all attack paths. Within mere minutes, a mature APM tool will present you with a prioritized list of findings to address, along with actionable recommendations.

Build Cross-Functional Alignment

Successful APM requires coordination between Security, Identity, and Infrastructure teams. Establish shared metrics, common vocabulary, and joint response playbooks before deploying technology solutions.

Plan for Scale

Prioritize platforms that deliver continuous monitoring across your entire identity infrastructure, both on-premises Active Directory and Entra ID. And step away from point-in-time assessments that lose value rapidly in dynamic environments where identities, permissions, and configurations change daily.

Resource Allocation

For organizations with limited security resources or competing priorities, Managed APM services offer a practical alternative. Rather than tasking your team with tool operation, analysis, and threat modeling, a managed service delivers prioritized, context-specific remediation actions tailored to your environment. Your team receives actionable findings they can implement immediately, without the overhead of running the platform or interpreting raw data and attack paths.

Measure What Matters

Focus on risk reduction metrics, such as attack paths eliminated and critical asset exposure reduced, rather than operational metrics such as scans completed and reports generated.

> **The goal of an APM practice is measurable security improvement, not security theater.**

The Path Forward

Identity Attack Path Management represents a fundamental evolution in how organizations approach identity security. Like Vulnerability Management before it, APM is transitioning from a specialized capability to an essential identity security practice.

For security leaders, the question isn't whether to adopt Identity APM, it's how quickly you can move from reactive incident response to proactive attack path prevention. The organizations that make this transition first will have significant competitive advantages in risk management, operational efficiency, and stakeholder confidence.

The technology exists. The methodologies are proven. The business case is clear. The differentiator will be execution: Building the cross-functional alignment, establishing the measurement frameworks, and creating the organizational capabilities that transform APM from a security tool into a strategic advantage.

Discover how to eliminate attack paths before an attacker exploits them in our full State of Attack Path Management 2025 report that includes:

- Technical playbooks
- Real-world case studies
- An implementation roadmap that leading organizations use to reduce their attack surface by 60-80% within the first quarter of adoption

Read the report* ›

* https://ghst.ly/sapm-25