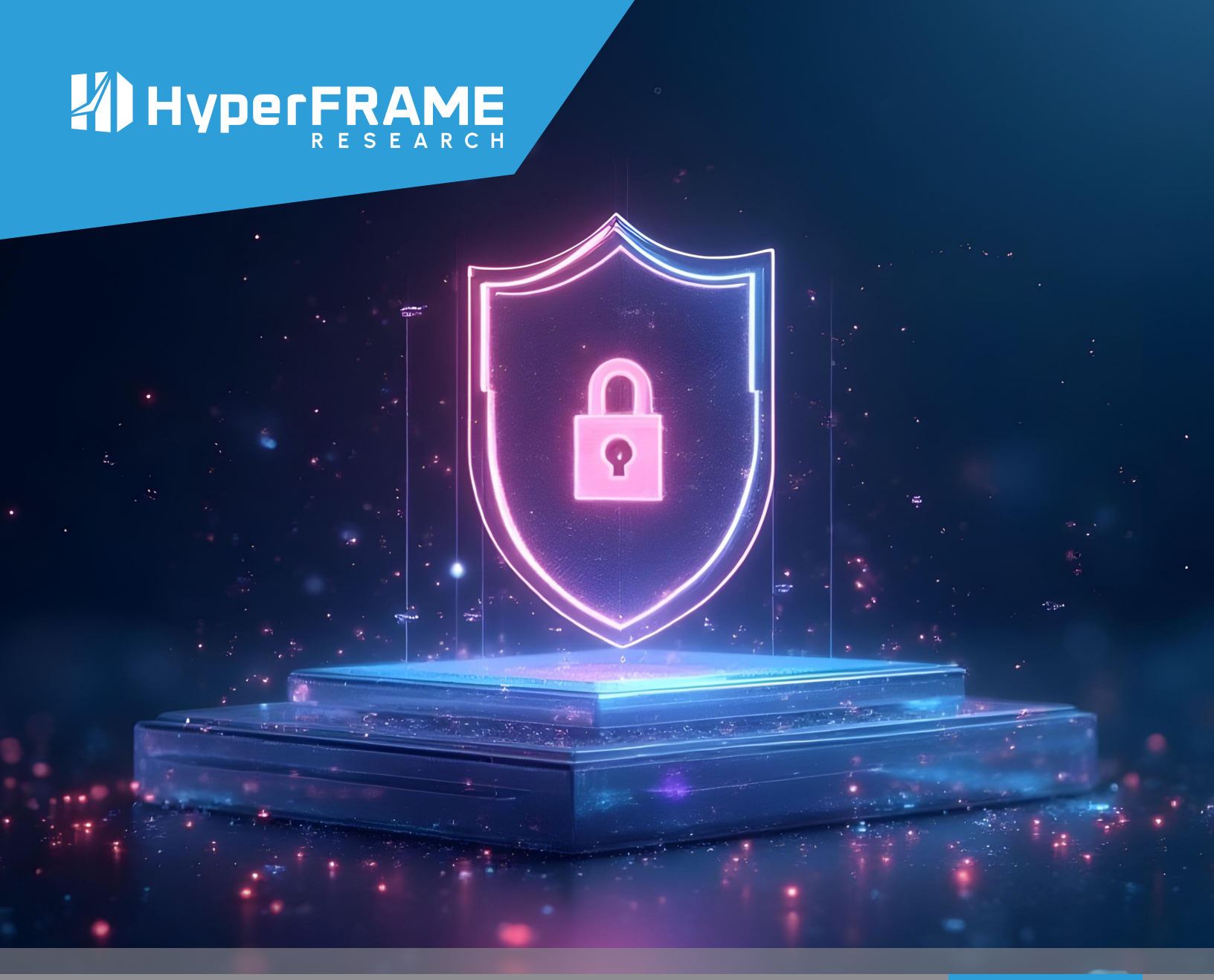
HyperFRAME RESEARCH



WHITE PAPER

From Cost Center to Business Catalyst: Making Identity Security Visible and Valuable

How Unified Identity Security Empowers Security Teams to Drive Business Outcomes

Authors:

Stephanie Walter
Practice Leader - AI Stack

Steven Dickens
CEO and Principal Analyst

OCTOBER 2025

Executive Summary

As AI evolves, the traditional cybersecurity perimeter has disappeared. Identity is now the main control point, and it's forcing security teams to become strategic business partners. To keep up with the pace of innovation, organizations must not only secure a growing number of human and machine identities, but also connect security results to business goals like operational resilience and risk reduction. The solution provides a unified approach that protects assets while allowing the business to move faster and with more confidence.

Many security teams struggle to show their value in business terms. Security initiatives are often seen as necessary expenses, relying on being reactive instead of demonstrating quantifiable benefits. This can limit investment and reduce the security team's strategic impact. Identities, or the representations of people and machines in a system, are increasingly targeted in attacks. Yet many traditional security tools lack the complete visibility needed for a quick and decisive response.

This gap is precisely where solutions like Teleport Identity Security prove their worth. The platform provides a unified view of identity activity across code, infrastructure, and cloud environments. Teleport delivers reductions in organizational risk and enables faster incident response. This critically supports the secure adoption of AI and broader digital innovation initiatives. Teleport's approach helps to elevate security from a reactive function to a strategic business enabler. This not only safeguards digital innovation, it also accelerates it.

The Hidden Cost of Invisibility in Security

Security teams typically have a perception problem. They are seen as necessary expenses rather than generators of value. Quantifying the financial return of security solutions that resonate with the C-suite in terms like increased revenue and reduced operational expenditure is inherently difficult. The problem is compounded by the fragmentation of identity systems and a general lack of visibility. Separate tools for developer access, cloud resources, and privileged accounts create blind spots. Not having clear insight impedes effective protection and also makes it incredibly difficult to communicate the value that security teams provide.

Hidden costs most likely extend beyond immediate financial penalties. Reputational damage, customer churn, and stifled innovation are real repercussions of not having a unified view of identity across the technology stack. Without this view, organizations are operating with critical blind spots. With these blind spots come prolonged detection times, increased breach severity, and a diminished capacity to respond effectively to threats. Persistent invisibility prevents security teams from proactively addressing vulnerabilities and forces them into a reactive cycle. Addressing this invisibility is a prerequisite for shifting the role of security from a reactive cost center to a strategic business partner.

Here's an example of how damaging these blind spots can be. Attackers can gain entry not through an exotic zero-day exploit, but by using valid employee credentials that have long-lived access rights. Because the access looks legitimate, the intrusion can go undetected for weeks. During that time, the attackers can move laterally, exfiltrate sensitive data, and disrupt operations. This can result in regulatory scrutiny and reputational fallout. This example illustrates the core problem: when credentials and identities retain excessive, persistent access, they become prime targets. Without the ability to see and control how identities are used in real time, organizations remain vulnerable to attackers who can operate in plain sight.

Beyond preventing breaches, achieving full identity visibility lets security teams report on metrics that directly impact the business, such as mean time to detect (MTTD) and mean time to respond (MTTR) to identity incidents. Regularly tracking and communicating these KPIs helps demonstrate not only compliance but also heightened operational resilience and readiness. These are key concerns for executive stakeholders. Security teams further legitimize their value to the enterprise by connecting operational security outcomes to business continuity.

Identity Security as a Business Enabler

Security incidents involve more than just technical issues; they pose real business risks. They can disrupt operations and affect organizational reputation. Incidents can cause downtime, data loss, and regulatory violations. These have a direct impact on customer trust, revenue, and operational efficiency, which makes identity security a core enabler of business continuity and innovation. Teleport Identity Security is built to tackle this head-on. It's architected to deliver real-time, end-to-end visibility

into all identity-related activity across cloud environments, codebases, and infrastructure. This allows for early detection of critical risks such as lateral movement, privilege misuse, and shadow access. Teleport provides immediate context around these unusual activities, which means security teams can step in quickly to stop problems before they get out of hand.

The business benefits of having such a strong identity security are clear. Being able to translate how resilient an organization's security is into concrete business metrics becomes much easier. For example, less downtime directly means a more resilient business, which is a huge win for any leadership team. Faster responses to incidents naturally improve customer service and the overall customer experience because disruptions are minimized, and trust remains intact. Providing strong security for AI and data center infrastructure ensures that these projects aren't held back by security vulnerabilities. Protection for these strategic initiatives means they can move forward confidently with lower operational costs and compliance risks. This simplifies audits and reduces potential fines.

Even with a wide collection of tools, most security and infrastructure teams still can't see everything they need to. Critical gaps remain, like hidden service accounts, unknown access paths, machine identities no one realized existed, because the signals from all those tools don't align. The result is slower investigations, longer times to detect and respond, and a perception that security is stuck putting out fires instead of helping the business move forward. A unified identity security platform changes that. Suddenly the unknowns become visible, incidents can be traced in real time, and investigations that once dragged on for days are wrapped up in hours. When security leaders can point to avoided downtime, reduced risk, and smoother audits, the conversation shifts. What was once viewed as an overwhelmed cost center becomes a trusted partner that makes the business more resilient and frees it to innovate.

This all adds up to a fundamental shift. Security teams stop being just the folks who fix problems when they happen. Instead, they become proactive partners who help to ensure the business keeps running smoothly. They support resiliency and help to de-risk innovation. By cutting down on the potential weak spots tied to identities and access, organizations can avoid costly breaches and keep things running, protecting revenue continuity while keeping customers happy.

Elevating the Security Team's Role and Value

Teleport lets security teams fundamentally alter the conversation around their function and shift from merely instilling fear, uncertainty, and doubt (FUD) to demonstrating tangible value. Teleport helps address threats quickly before they significantly disrupt business, but perhaps most importantly, Teleport provides tools to quantify and effectively communicate risk reduction.

Another way to elevate the security function is to deliver actionable, data-driven insights to business leaders. Security teams can clearly show their contribution to business outcomes by providing regular reports on avoided costs, minimized downtime, and incident-free periods. Even better if calculations can be done to show how the outcomes affect the bottom line. These proofs of performance help shift perceptions from security as a necessary expense to security as a driver of efficiency, reputation, and growth.

Security teams can shift their perception from reactive defenders into strategic business partners. It takes communicating security outcomes in terms of reduced exposure, avoided costs, and supported business initiatives. By tying security efforts and results to business goals, such as market expansion, new product development, or customer satisfaction, security teams can secure budgets and gain stakeholder buy-in. This fosters a culture where security is seen as integral to innovation and growth.

Implications for AI and Innovation

The rapid acceleration of AI initiatives and broader digital innovation inherently introduces new layers of identity complexity. We are witnessing an explosion of new systems, with an increasing number of machine identities alongside human identities, all requiring secure access. Consider what happens when a user supplies their corporate credentials to an LLM so it can pull information or execute tasks on their behalf. On the surface, activity in the system looks like it's coming from a legitimate employee account. In reality, those credentials may now be driving automated actions initiated by the model itself, or worse, by an attacker who has compromised the model. Sensitive data could be queried, privileges escalated, or configuration changes made under the guise of normal user activity. Without unified identity visibility, it becomes nearly impossible to tell whether a human is performing the work or whether an AI agent or bot is acting with borrowed credentials. That ambiguity opens the door for attackers to blend in with normal operations, undermining both trust in AI systems and the integrity of the data they touch.

Teleport's identity chain observability directly strengthens the foundational security upon which these AI driven operations depend. This capability can significantly reduce the risks associated with credential misuse or insider threats. It provides visibility into who or what is accessing critical data and AI models. These threats have the potential to disrupt AI model integrity, compromise sensitive data, or incapacitate cloud applications. Security underpinned by identity visibility can transform security from being seen as a potential blocker to a powerful enabler of innovation. Organizations can explore new AI capabilities and complete digital innovation knowing their core assets are protected.

Recommendations for Security Leaders

Our primary recommendation for security leaders is to deeply understand their organization's key business drivers and then meticulously align all security solutions with these overarching metrics. This involves moving beyond technical jargon and beginning to understand and quantify the actual cost of a security-caused outage. What does that mean for revenue, for customer trust, for employee productivity?

Deeply understanding business drivers means framing identity security decisions in the language of risk, revenue, and compliance, not just technology. For instance, instead of saying, "We need a better solution to manage access for internal applications," a leader might point out that "we face a quantifiable risk of major disruption if a single contractor account is compromised." That shift makes the case for just-in-time access controls and detailed session auditing as a way to protect the product roadmap and keep projects on track. Similarly, rather than simply stating, "We need to buy an identity platform to meet a new regulation," a more effective argument highlights the business trade-off: either absorb recurring losses from fines and manual overhead, or make a one-time investment in a modern access platform that resolves compliance gaps, reduces audit effort, and saves money over time. By tying solutions directly to avoiding risks, preserving revenue, and lowering costs, security leaders can demonstrate that identity security is not just a safeguard, but a driver of business outcomes.

Furthermore, it's imperative to recognize identity as the new perimeter. The traditional network boundary has dissolved; access controls now reside at the identity layer. Additional recommendations include:

- Invest in tools that provide visibility into every identity and its associated activity, and partner closely with business stakeholders.
- All security outcomes should be framed in business terms and emphasize metrics like risk reduced, and innovation initiatives supported.
- Highlight security's critical role in AI adoption, compliance with evolving regulations, and operational resilience across the enterprise.
- Having proactive engagement with concrete metrics will redefine security's standing in the organization.

Looking Ahead

The value of robust identity security can and must be articulated in KPIs understandable to the C-suite. It's no longer sufficient to merely state that security protects. Organizations must demonstrate how identity activity, when made visible and actionable, directly contributes to the organization's bottom line. Teleport helps to achieve precisely this. It can support elevating the role of security teams and transform them from cost centers into strategic partners that protect the organization and provide measurable business value. As digital footprints continue to expand, and threats evolve, seeing, understanding, and controlling every identity's access becomes not just imperative but a competitive advantage. Identity security solutions like Teleport are an investment in the resilience and innovative capacity of the entire organization. Speed, trust, flexibility: that's what identity security, done well, brings to the table.

We're seeing leaders now ask, "What's the upside?" They want real numbers: how many hours saved, which revenue streams protected, how much time shaved off audit responses. The data is starting to roll in. One enterprise reported saving roughly 40 engineering hours during a security incident thanks to Teleport's comprehensive logging capabilities. Another customer reduced their weekly database forensic investigation time from two and a half hours to just minutes by relying on Teleport's centralized audit logs. These kinds of outcomes turn abstract promises into tangible results that executives can measure. When teams can point to saved hours, smoother audits, and faster investigations, even skeptics begin to recognize security not as overhead, but as a business accelerator. Tools like Teleport help make this shift practical. By collapsing the complexity of who can access what across sprawling cloud environments, companies save time and avoid headaches. Mistakes get picked up quickly, and meeting compliance requirements turns into a routine, not a fire drill.

One thing seems clear: as digital footprints grow, trust will only matter more. The organizations treating identity security as a real business asset, not just another expense, are setting themselves up to lead, not follow. The future will reward those who invest in visibility and readiness, because in this landscape, it's better to build on solid ground than hope for the best.

ABOUT HYPERFRAME RESEARCH:

HyperFRAME Research delivers in-depth research and insights across the global technology landscape, spanning everything from hyperscale public cloud to the mainframe and everything in between. We offer strategic advisory services, custom research reports, tailored consulting engagements, digital events, go to market planning, message testing, and lead generation programs.

Our industry analysts specialize in rigorous qualitative and quantitative assessments of technology solutions, business challenges, market forces, and end user demands across industry sectors. HyperFRAME Research collaborates closely with your Analyst Relations, Product, and Marketing teams to build and amplify your thought leadership, positioning your expertise to enhance brand and product recognition. Through content that engages readers, viewers, and listeners alike, we ensure your voice resonates across channels.

CONTACT HYPERFRAME RESEARCH:

Steven Dickens
CEO & Principal Analyst | HyperFRAME Research
Email Address:
steven.dickens@hyperframeresearch.com
Telephone Number:
+1 845 505 1678
X: @StevenDickens3
LinkedIn: Steven Dickens
BlueSky: Steven Dickens

CONTRIBUTORS

Steven Dickens
CEO & Principal Analyst

Stephanie Walter
Practice Leader - AI Stack

INQUIRIES

Contact us if you would like to discuss this report and HyperFRAME Research will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "HyperFRAME Research." Non-press and non-analysts must receive prior written permission by HyperFRAME Research for any citations.

LICENSING

DISCLOSURES

HyperFRAME Research provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.


HyperFRAME
RESEARCH