Netdata®

CYBERSECURITY

How to Secure 109 Machine Identities While Beating the 72-Minute Attack Window

An executive blueprint for CISOs on taming agentic AI, eliminating tool fragmentation, and reclaiming time.

The 12-hour blind spot

Let's skip the standard vendor introductions and speak plainly: The perimeter you spent the last decade securing is gone. Today, attackers aren't breaking into your network; they are simply logging in.

While the Board demands rapid AI adoption to accelerate the business, this speed has created a dangerous operational paradox for security teams.

According to the latest Global Incident Response Report from Palo Alto Networks*, the fastest real-world intrusions now reach data exfiltration in just 72 minutes. However, when an identity-related incident occurs, security teams spend an average of 12 hours trying to correlate signals across siloed identity tools to understand what happened. Attackers are moving at an unprecedented speed, while defenders are trapped in the manual friction of tool sprawl.

This whitepaper dissects the root cause of the "fragmentation tax," explains why the human-to-machine identity ratio has broken legacy access models, and outlines how Netdata partners with enterprise leaders to implement Zero Standing Privilege (ZSP) and unified platformization to close the uncontrolled privilege gap.

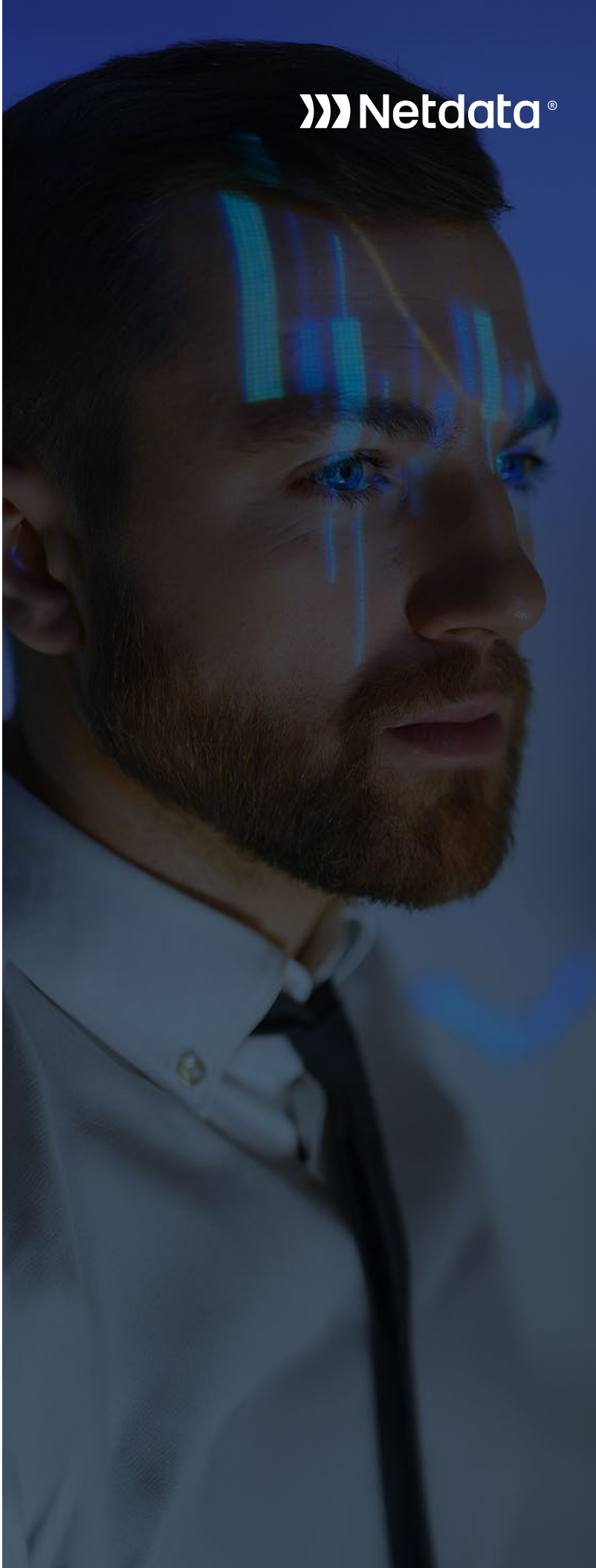
*Source: Palo Alto Networks Unit 42, Global Incident Response Report 2026 (Analysis of 750+ major cyber incident investigations).

The invisible workforce (109:1 reality)

Your organizational chart is lying to you. Humans are no longer the dominant species on your network.

According to the 2026 Identity Security Landscape Report, organizations now contend with an average of 109 machine identities for every human employee. This ecosystem of service accounts, workload identities, APIs, and secrets has recently been joined by the fastest-growing identity subset: AI agents.

The study reveals that 99% of enterprise organizations report already deploying AI agents in production environments.



Netdata®

However, the report highlights a critical board-level risk:

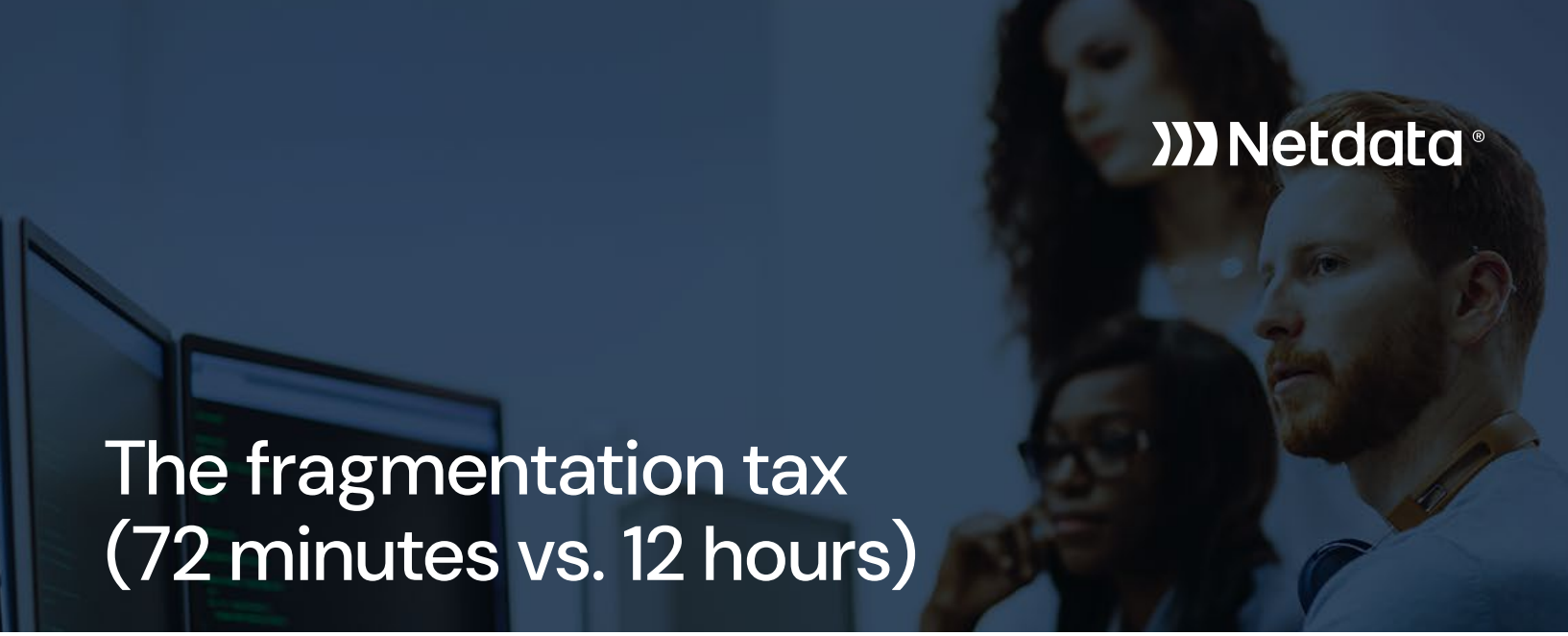
40% of AI agents already possess direct access to sensitive organizational data, including financial records, PII, PHI, and intellectual property.

61% of frontline practitioners report that least privilege is not effectively enforced, directly contradicting the 54% of C-suite executives who believe their organization has it completely under control.

96% of human identities operate with access permissions far beyond what is required for their actual roles, with 42% having direct access to core organizational data.

When you combine over-privileged human accounts with swarms of autonomous AI agents operating without runtime controls, identity transforms from an administrative function into your largest attack surface.

Source: Vanson Bourne, 2026 Identity Security Landscape Report. A global study of 2,930 cybersecurity decision-makers across Americas, JAPAC, and EMEA.



The fragmentation tax (72 minutes vs. 12 hours)

When a compromised identity begins moving laterally, visibility is your only lifeline.

Unfortunately, decades of purchasing disconnected point solutions for Identity and Access Management, Privileged Access Management, and Identity Governance have created a fractured landscape.

The scale of this exposure is documented in recent threat data:

90% of organizations report experiencing at least one successful identity-related breach in the last 12 months.

83% experienced two or more breaches during the same period.

89% of forensic investigations revealed that identity gaps were a core driver of breach execution.

97% of organizations admit that identity tool fragmentation actively delays their incident response, creating a 12-hour response lag.

Security analysts are forced to jump between five to ten different consoles, manually stitching together logs from cloud permissions, PAM vaults, and active directories.

Meanwhile, adversaries leverage AI tooling to exfiltrate data in as little as 72 minutes.

Source: Vanson Bourne, 2026 Identity Security Landscape Report & Palo Alto Networks Unit 42, Global Incident Response Report 2026.

Netdata®

The operational timebomb (47-day rule)

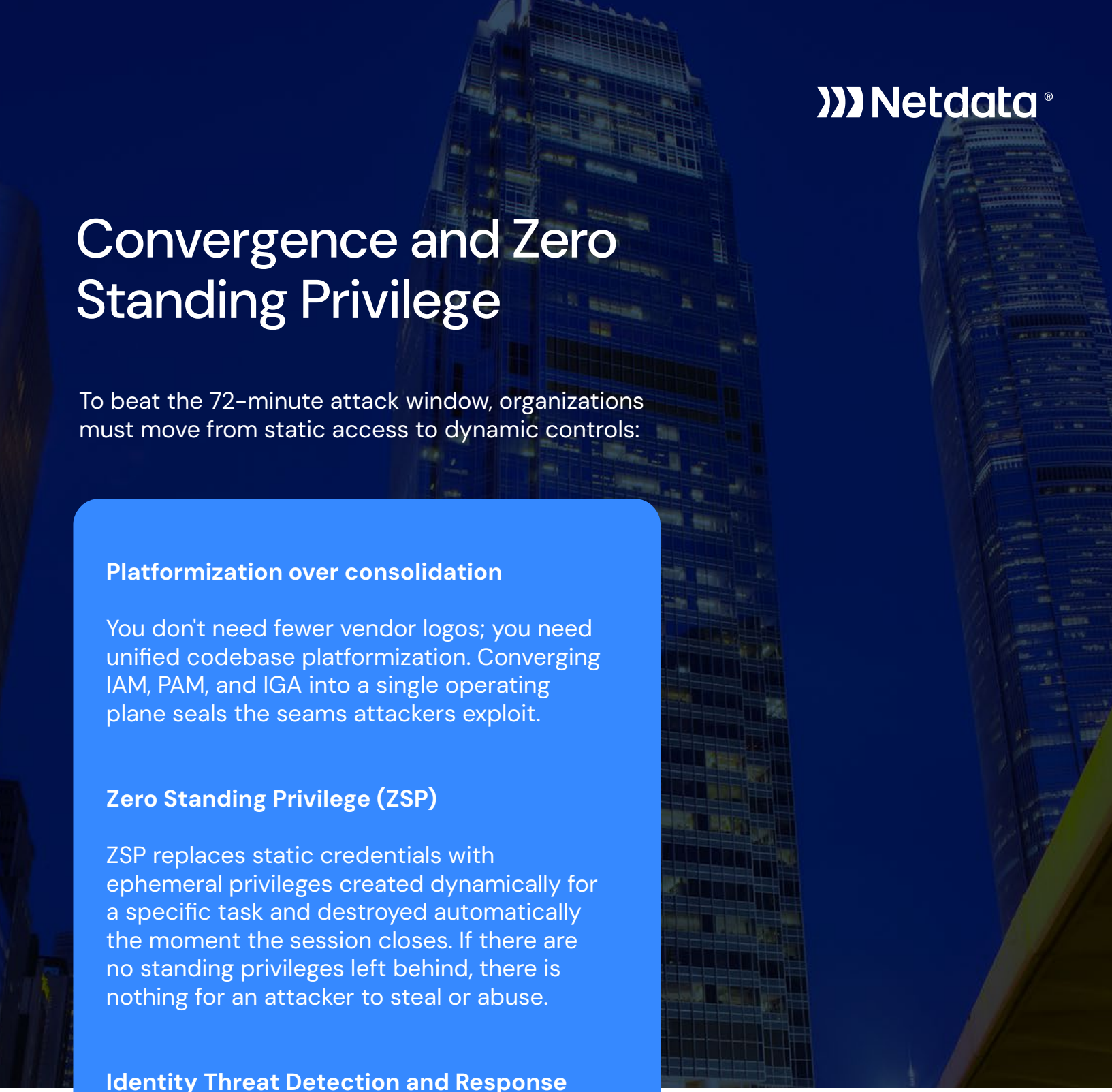
The speed paradox doesn't just apply to active breaches; it threatens everyday business continuity.

Public TLS certificate lifetimes are stepping down from 398 days to just 47 days. This transition triggers an 8 to 12-fold increase in manual workloads. For an organization managing 1,000 certificates, administrative overhead skyrockets from 4,000 hours to 48,000 hours, with an estimated average financial risk of $272,088 from certificate-related outages.

Despite this imminent deadline, 71% of organizations have not fully automated certificate renewal and monitoring across all environments.

If your team is buried in 48,000 hours of manual certificate rotations, they have zero capacity to hunt for compromised AI agents or govern zero-trust architectures.

Source: Vanson Bourne, 2026 Identity Security Landscape Report. A global study of 2,930 cybersecurity decision-makers across Americas, JAPAC, and EMEA.



Netdata®

Convergence and Zero Standing Privilege

To beat the 72-minute attack window, organizations must move from static access to dynamic controls:

Platformization over consolidation

You don't need fewer vendor logos; you need unified codebase platformization. Converging IAM, PAM, and IGA into a single operating plane seals the seams attackers exploit.

Zero Standing Privilege (ZSP)

ZSP replaces static credentials with ephemeral privileges created dynamically for a specific task and destroyed automatically the moment the session closes. If there are no standing privileges left behind, there is nothing for an attacker to steal or abuse.

Identity Threat Detection and Response (ITDR)

ITDR acts as the real-time kill switch, detecting lateral movement, credential harvesting, and unauthorized MFA bypasses to terminate sessions instantly across endpoints, clouds, and SaaS apps.

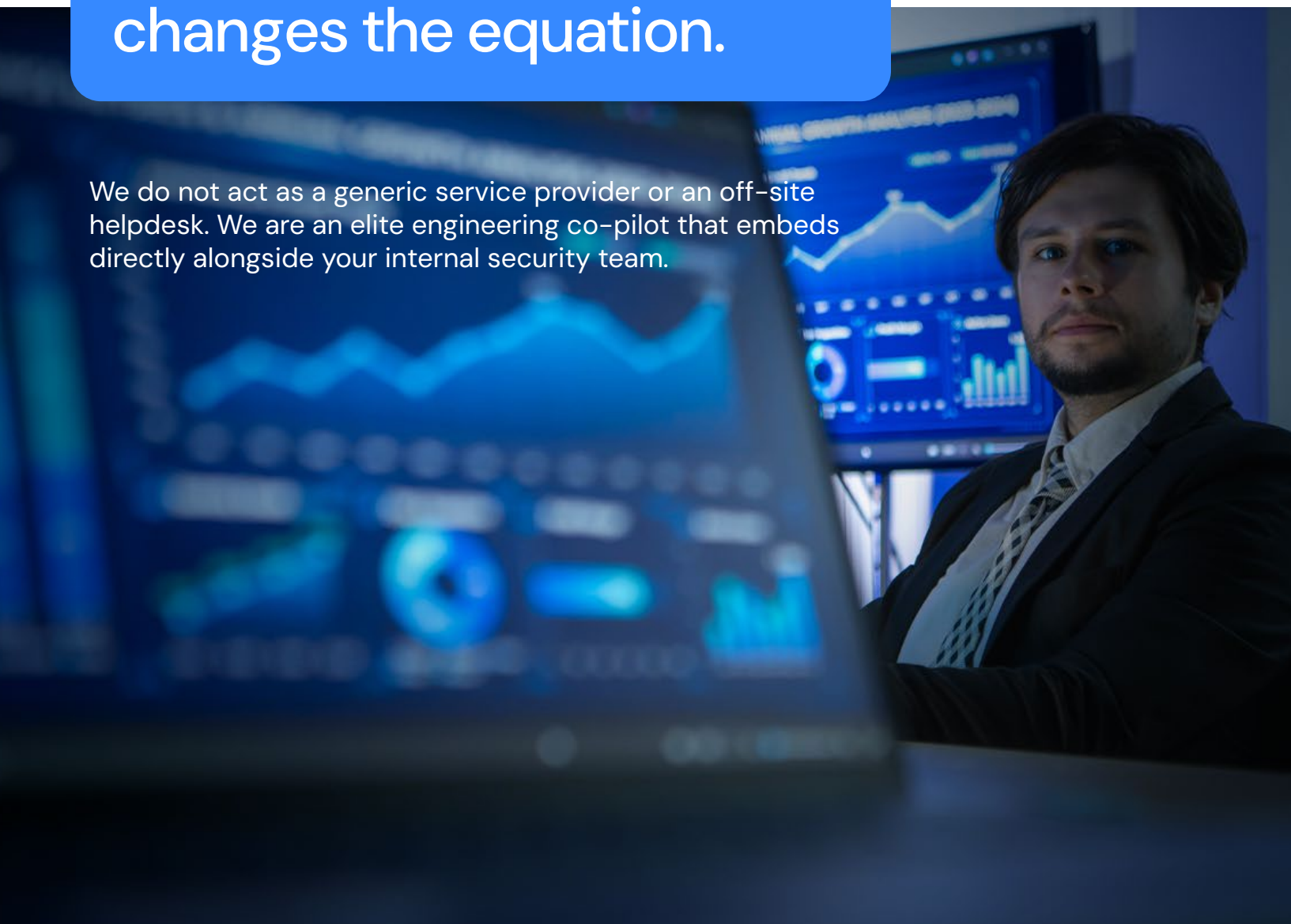
The Netdata advantage: From 12 hours to 10 minutes

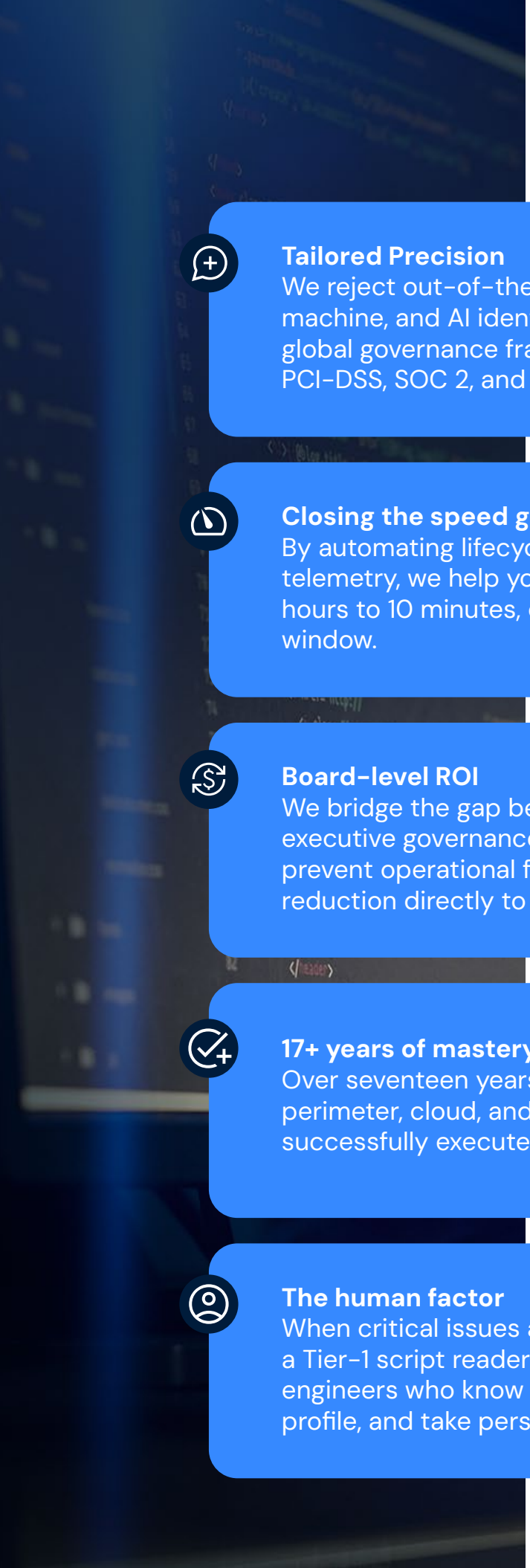
Here is the fundamental truth that software manufacturers rarely admit: Buying a world-class platform like Idira provides the horsepower, but software does not drive itself.

Without expert tuning, continuous governance, and deep operational alignment to your specific topology, even the most advanced identity platforms end up underutilized, misconfigured, or turned into expensive shelfware.

This is where Netdata changes the equation.

We do not act as a generic service provider or an off-site helpdesk. We are an elite engineering co-pilot that embeds directly alongside your internal security team.





Netdata®

Tailored Precision
We reject out-of-the-box configurations. We map your human, machine, and AI identities, aligning automated policies directly to global governance frameworks like NIST SP 800-207, ISO 27001, PCI-DSS, SOC 2, and HIPAA.

Closing the speed gap
By automating lifecycle management and unifying your identity telemetry, we help your SOC reduce investigation times from 12 hours to 10 minutes, definitively beating the attacker's 72-minute window.

Board-level ROI
We bridge the gap between technical implementation and executive governance, helping you eliminate redundant licensing, prevent operational friction, and deliver demonstrable risk reduction directly to your Board of Directors.

17+ years of mastery
Over seventeen years of hands-on experience navigating perimeter, cloud, and AI security evolutions, backed by 1,000+ successfully executed enterprise projects.

The human factor
When critical issues arise, you don't talk to a generic AI chatbot or a Tier-1 script reader. You gain direct access to senior security engineers who know your network topology, understand your risk profile, and take personal ownership of your operational stability.

Accelerate your security strategy safely

The choice is no longer between stopping AI adoption or exposing your data.

By combining a unified identity security architecture with Netdata's battle-tested engineering team, your organization can enable business velocity with absolute confidence.

Ready to eliminate your identity blind spots and beat the 72-minute window? Schedule an architectural discovery session with our lead security specialists today.

Netdata®

www.netdatanetworks.com