



How Consolidating 83 Security Tools Drives a 101% ROI

An executive blueprint for CISOs and CIOs on eliminating the 5% complexity tax, rationalizing stack architecture, and delivering board-level value.

A man in a dark suit and striped tie is shown in profile, looking down at a laptop. He is standing in front of a city skyline at night, with lights from buildings visible in the background. The scene is dimly lit, with a blue tint. The background image is partially obscured by large, semi-transparent blue geometric shapes (polygons) that frame the text.

The executive hook & operational paradox

To speak candidly, your security budget isn't underperforming because you lack capabilities, it is bleeding money through a hidden complexity tax.

While your Board demands cost optimization and operational agility, the traditional playbook of purchasing a new point solution for every emerging threat has reached a critical breaking point. Enterprise environments are now trapped in a dangerous operational paradox: accumulating more security tools has not made organizations safer. It has made them slower, more complex, and significantly more expensive to run.

Each additional point solution dilutes the effectiveness of your existing stack, creating a fragmented patchwork that inflates management overhead while leaving critical risk gaps wide open.

Data-backed industry reality

This complexity tax is no longer a hidden operational nuisance; it is a measurable financial drain on the enterprise:

83 solutions from 29 vendors

is the average number of security tools enterprises juggle nowadays, according to research by the IBM Institute for Business Value.

52% of security executives

cite tool complexity as the single greatest impediment to their security operations.

>5% of annual revenue

is what C-suite executives estimate as the total business impact of security complexity. For a \$20 billion enterprise, this represents a \$1 billion annual drag.

Source: IBM Institute for Business Value & Palo Alto Networks, Capturing the Cybersecurity Dividend: How Security Platforms Generate Business Value.

The root cause

The delusion that "more tools equal more security" has severely compromised internal operations:

74% of executives

admit that the current workload on their security operators is excessive, while 80% acknowledge constant pressure to reduce security costs.

6 separate DLP tools

are deployed on average for an enterprise, creating a fragmented management nightmare.

96% of tech leaders

admit that maintaining existing DLP policies is a constant uphill battle, while 38% of all generated alerts are false positives.

Source: Omdia / Enterprise Strategy Group, The Data Security Imperative: How AI-powered Data Security Enables the Modern Workforce.

AI acceleration & data leak surface

Compounding this fragmentation tax is the rapid shift toward cloud environments and Generative AI.

Data no longer lives neatly behind enterprise firewalls; 85% of modern enterprise work takes place directly inside the web browser. Research shows that 52% of enterprises suffered a sensitive data loss event in the past 12 months, with 75% of those organizations experiencing three or more separate loss events. Crucially, 43% of these exfiltration cases stemmed directly from generative AI tool usage.

Attempting to govern modern AI workflows and browser-based data movement across 29 separate vendor consoles is mathematically unviable.

Without architectural consolidation, new technology initiatives will either fail to scale due to security friction or expose corporate IP to untracked exfiltration.

Unlocking the 101% ROI

To eliminate complexity and reclaim business velocity, forward-thinking leaders are pivoting from fragmented point tools to unified platformization:

Operational metric	Fragmented architecture	Platformized architecture	Business impact
Mean Time to Identify (MTTI)	High dwell time	72 days faster	Drastic reduction in blast radius
Mean Time to Contain (MTTC)	Extended exposure	84 days faster	Rapid incident resolution
Average ROI	28% ROI	101% ROI	Nearly 4x greater financial return
Return on Security Spend (ROSI)	32% ROSI	116% ROSI	Demonstrable board-level value
Executive perception	8% view security as value generator	96% view security as value generator	Transforms security into business enabler

Source: IBM Institute for Business Value & Palo Alto Networks, Capturing the Cybersecurity Dividend: How Security Platforms Generate Business Value.

The Netdata advantage: Proven engineering execution

Acquiring world-class security platforms establishes theoretical capability. However, it takes dedicated human engineering to transform that capability into an active operational defense.

Organizations can attempt to manage complex platform migrations in-house or rely on generic, ticket-focused help desks. When evaluated based on execution speed, stack rationalization, and board-level risk reduction, the Netdata co-pilot model remains the undisputed standard for enterprise delivery.

**12-hour to
10-minute
acceleration**

It is achieved by automating lifecycle management and unifying security telemetry, closing the critical speed gap against modern adversaries.

**17+ years
of mastery**

And 1,000+ Enterprise Projects back our engineering teams, protecting over 150 leading organizations across complex cloud, network, and identity environments.

**95%
satisfaction
& 101% ROI**

This reflects our commitment to eliminating redundant licensing, preventing operational friction, and delivering demonstrable value directly to the Board.

**Uncompromised
rigor**

Ensures that every architectural policy and hardening rule strictly maps to global frameworks, including NIST SP 800-207, ISO 27001, PCI-DSS, SOC 2, and HIPAA.

**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.

Accelerate your consolidation strategy

The choice is no longer between inflating software budgets or accepting unmanaged security exposure.

By combining a platformized architecture with Netdata's battle-tested engineering team, your organization can eliminate the complexity tax, optimize capital expenditure, and drive business velocity with total confidence.

Ready to evaluate your tool redundancy and build a high-ROI consolidation roadmap? Schedule an architectural discovery session with Netdata's lead security specialists today.