# How to avoid cybersecurity tool sprawl and resource waste

CybelAngel

INTRODUCTION

# The hidden cost of tool sprawl

Security teams face a paradox. Despite investing more in cybersecurity than ever before, organizations are struggling to keep pace with threats. The problem isn't a lack of technology but too much of it.

According to Gartner's 2025 research, the average enterprise now operates 45 different cybersecurity tools. That's not a robust security posture; it's a management nightmare. With over 3,000 vendors competing in the cybersecurity market, organizations have accumulated tools at an unsustainable pace, creating what industry analysts call "tool sprawl."

The consequences are severe. Multiple overlapping vendors mean multiple integration points, conflicting alert priorities, and security teams spending more time managing tools than defending against threats. Research shows that security professionals waste 25% of their time dealing with false positives from poorly integrated security tools.

This isn't just an operational headache. Tool sprawl creates genuine security gaps. When alerts from different vendors don't correlate, genuine threats slip through the cracks. When teams are overwhelmed by noise from dozens of tools, they miss the signals that matter.

The response from security leaders is decisive. Gartner found that 75% of organizations are actively pursuing security vendor consolidation, a dramatic increase from just 29% in 2020. This shift represents one of the most significant trends in enterprise cybersecurity today.

This guide examines why tool sprawl has become the industry's most pressing operational challenge, how it undermines security effectiveness, and why external threat intelligence programs offer a compelling case study for successful consolidation.

# Understanding Tool Sprawl:
# How we got here

## The accumulation problem

Organizations rarely set out to build sprawling security tool environments, but tool sprawl develops gradually through predictable patterns: reacting to emerging threats by purchasing specialized protection for each new risk (ransomware tools, email gateways, cloud security solutions), adopting point solutions to address specific gaps rather than extending existing capabilities, inheriting duplicate security stacks through mergers and acquisitions, and maintaining outdated tools due to vendor lock-in and organizational inertia.

These tactical decisions compound over time, with what starts as 10 security vendors quickly escalating to 20, then 30, then 45, creating an unmanageable environment where each purchase made sense in isolation but collectively undermined operational (and cost!) efficiency.

But the financial impact of tool sprawl extends far beyond license fee:

It includes direct costs (redundant vendor licenses, support contracts, professional services, and multiplied training expenses), hidden operational costs (engineering time for custom integrations, administrative overhead, procurement expenses, and compliance auditing), and critical opportunity costs.

With over 80% of organizations expecting less than 10% budget growth in 2025, money spent on redundant tools is money unavailable for genuine security improvements, and analyst time spent managing tools is time not spent hunting threats or improving defenses.

## What about the security impact?

The security impact of tool sprawl is even more concerning than the financial burden. When 45 different tools each generate alerts with different severity scales, security teams drown in notifications, with analysts spending an estimated 25% of their time investigating false positives. Integration gaps emerge as different vendors use incompatible data formats and APIs, preventing critical threat intelligence from reaching the tools that need it, while fragmented data across dozens of platforms creates incomplete visibility. In 2024, 57% of organizations learned about their own breaches from external sources rather than internal tools, and skill gaps widened as security teams struggled to find analysts who understand all the tools in their environment, meaning organizations can't effectively use what they've purchased.

# Why should security vendor consolidation be a **priority?**

When incidents occur, everyone knows teams waste time correlating data across multiple tools and translating between formats, extending the window attackers have to operate undetected. These challenges are prodding security leaders to rethink their approach to how they actually build out security programs.

## The consolidation imperative

Vendor consolidation has become a strategic necessity driven by three key factors. Forrester's 2026 analysis found that software now accounts for 40% of cybersecurity spending, yet minimal budget growth means organizations can't continue adding vendors. CFOs increasingly demand ROI, and reducing vendor count while maintaining security posture delivers clear financial benefits.

> Security teams are burned out, and complexity is one key factor.

Gartner identifies cybersecurity burnout as a key concern, noting that stress stems from relentless demands in complex environments with limited resources. Consolidating vendors reduces daily complexity through unified platforms with consistent interfaces and integrated workflows.

Paradoxically, fewer tools often mean better security. When data flows through integrated platforms, correlations become possible that isolated point solutions can't achieve. Threats are detected faster, response is more coordinated, and visibility improves.

## What is research telling us about the benefits of trimming back tools?

Gartner's 2025 report identifies "cybersecurity technology optimization" as critical. With over 3,000 vendors in the market and organizations using an average of 45 tools, leaders must optimize their toolsets. Gartner recommends consolidating core security controls, enhancing data portability, using threat modeling to assess which capabilities need specialized tools, and balancing consolidation with proper security posture. The goal isn't minimizing vendor count at all costs, but finding optimal balance between breadth and manageability.

Optiv's analysis found that 75% of organizations will pursue consolidation specifically to improve security posture, not just cut costs. Successful efforts focus on identifying vendor overlap, mapping capabilities, and assessing vendors' abilities to serve as long-term strategic partners.

Research from Kovrr identifies vendor consolidation and using platforms as the top cyber risk management trend for 2025. Organizations are moving from best-of-breed point solutions toward integrated platforms delivering multiple capabilities through unified architectures. This shift is driving vendor behavior as security companies build comprehensive platforms organically or acquire point solution providers.

## What does a platform approach involve?

The alternative to tool sprawl is a fundamental shift toward platform-based security architectures. Modern platforms provide unified data architecture where all security functions share a common data model. When one component detects an indicator of compromise, that intelligence immediately becomes available to all other components, eliminating the integration tax that plagues multi-vendor environments.

Security analysts work within a single interface rather than pivoting between dozens of vendor portals, with workflows spanning multiple security functions without manual data transfer. This consistency then subtly accelerates analyst onboarding and day-to-day operations.

## Fragmented environments kill coordination

When incidents occur, platform architectures enable coordinated response across multiple security functions. Blocking a malicious domain can automatically update firewalls, endpoint protection, and email gateways. This coordination is nearly impossible in fragmented environments.

Platform approaches dramatically reduce operational overhead through a single vendor relationship, one procurement process, unified support escalation, consistent security auditing, and centralized policy management.

# External threat intelligence: A case study in consolidation

External threat intelligence programs perfectly illustrate both the tool sprawl problem and the benefits of consolidation. Organizations typically piece together capabilities from multiple specialized vendors, each addressing a narrow slice of the overall challenge, creating a fragmented environment that undermines security effectiveness.

## The fragmentation problem

Before consolidation, a typical external threat intelligence program resembles a patchwork quilt of disconnected services. One vendor scans the internet to identify exposed assets while another monitors cloud configurations and a third focuses on shadow IT detection. Each provides partial visibility with minimal integration between them. Separate vendors monitor for typosquatting, malicious domain registration, phishing sites, and brand impersonation, sending alerts through different channels with varying levels of detail and actionability.

Multiple services claim to monitor dark web forums, paste sites, and criminal marketplaces, but each has different coverage, varying data quality, and incompatible alert formats. Security teams must manually correlate findings across these sources. Organizations subscribe to commercial threat intelligence feeds, open-source intelligence sources, industry sharing groups, and government bulletins. Research shows that 90% of organizations use external threat intelligence sources, yet only 41% have formal plans for what intelligence to collect. The result is information overload without insight.

# How overlapping vendors creates issues

This multi-vendor approach creates specific challenges that undermine security operations:

## Alert overload usually means inconsistent priorities

When multiple vendors monitor overlapping threat categories, security teams face:

- **Duplicate alerts** about the same issues across different platforms
- **Inconsistent severity ratings** – one vendor's "critical" alert might be another's "medium"
- **No unified prioritization framework** across vendor sources

The result? Teams either investigate everything (impossible!) or develop ad-hoc prioritization schemes that miss genuine threats.

## The integration tax

What is more is that each vendor brings its own technical complexity:

- **Different authentication methods**, data formats, and rate limits
- Custom integrations that require building and ongoing maintenance
- **Broken workflows** when vendors update their APIs (which happens regularly)

This integration burden consumes engineering resources that should focus on security improvements.

## Missing context is a serious issue

The most damaging consequence of fragmented threat intelligence is the lack of context. Consider this scenario:

- **One vendor detects an exposed database**
- **Another identifies leaked credentials on the dark web**
- **A third spots your domain in a phishing campaign**

Are these related? Different manifestations of the same attack campaign? Or unrelated incidents?

In multi-vendor environments, security teams must manually piece together this context. Often, they never make the connections.

# The consolidated alternative

Forrester's research on external threat intelligence providers identified that most vendors specialize in one or two use cases. Only a handful of providers can efficiently cover the full spectrum including physical asset protection, brand and domain reputation protection, attack surface discovery and management, fraud detection, and third-party risk monitoring. These comprehensive providers enable organizations to replace 5-10 specialized point solutions with a single integrated platform.

Consolidated platforms discover and monitor all external-facing assets through integrated scanning technologies. Rather than manually correlating findings from multiple asset discovery tools, security teams gain complete visibility through a single inventory. When all external threat intelligence flows through a unified platform, context emerges naturally. The platform automatically correlates an exposed database with leaked credentials and active phishing campaigns, revealing attack patterns that fragmented tools miss.

## Why human analysts add a golden layer of expertise

It is no secret that platforms combine automated detection with human analyst expertise. CybelAngel detects 335,000 deep and dark web posts daily and employs dedicated cybersecurity experts to validate findings. This hybrid approach delivers the scale of automation with the judgment of experienced analysts, dramatically reducing false positives. Consolidated platforms send pre-investigated, verified security issues rather than raw intelligence requiring manual analysis. Security teams receive one unified format for incident reports with confirmed attribution, tailored to their specific requirements.

Organizations that consolidate external threat intelligence vendors report significant quantifiable benefits: 60-80% reduction in alert volume while improving quality, 30-50% faster incident response times, and 30-40% cost savings through eliminated redundant licenses and reduced integration overhead. CybelAngel's data shows a 51% increase in security alerts sent to clients in 2024 compared to the previous year—despite the threat landscape growing substantially—reflecting better detection capabilities with reduced noise. These efficiency gains free security teams to focus on genuine threats rather than false positives, while cost savings fund additional security improvements.

# Making Consolidation Work: 10 Essential Tips

1

## Audit your current environment

Document every security tool you currently deploy, including purchase date, annual cost, use cases, integration points, and organizational knowledge depth. Many organizations discover they're paying for unused tools or duplicate capabilities.

2

## Create a capability matrix

Map which vendors provide similar capabilities across your organization. You may find 3-4 tools performing essentially identical functions across different business units.

3

## Identify your core strategic platforms

Select 3-5 vendors as your foundation. Choose vendors that demonstrate financial stability, commitment to platform expansion, excellent support, strong integration capabilities, and alignment with your risk profile.

4

## Avoid over-consolidation

Industry experts caution against excessive dependence on single vendors. Ensure contracts include data portability provisions and maintain relationships with alternative vendors as backup options.

5

## Start with low-hanging fruit

Begin consolidation where multiple vendors provide genuinely redundant capabilities with minimal differentiation for immediate impact.

6

## Target integration bottlenecks

Prioritize consolidating vendors that require the most manual integration work, freeing engineering resources for higher-value activities.

7

## Focus on workflow efficiency

Consolidate areas where analysts must frequently pivot between multiple tools to complete common workflows—unified platforms dramatically improve efficiency.

8

## Run parallel systems during transition

Avoid consolidating everything simultaneously. Run new platforms alongside existing tools during transition periods to validate capabilities before decommissioning vendors.

9

## Invest in comprehensive training

Security teams develop muscle memory around existing tools. Provide thorough training on new platforms, not just brief overviews, and document new workflows, integration points, and escalation procedures.

10

## Prioritize change management

The most common cause of consolidation failure is inadequate change management, not technology shortcomings. Communicate changes clearly to all stakeholders throughout the process.

# How to handle the question of resistance internally

Security teams often resist consolidation, arguing that platform vendors can’t match the specialized expertise of point solution providers. This concern is increasingly outdated. Leading platform vendors either develop comprehensive capabilities in-house or acquire specialist companies, and Forrester’s research identified multiple vendors delivering both breadth and depth across external threat intelligence use cases. More importantly, “best-of-breed” capabilities trapped in isolated tools often deliver less value than “good enough” capabilities that integrate seamlessly with your security infrastructure.

Teams also worry about operational disruption during migration. Phased migrations and parallel operation minimize risk, while professional services from platform vendors guide transitions based on hundreds of similar projects.

Consider this: the disruption of not consolidating, ongoing integration maintenance, analyst burnout, and missed threats due to fragmentation, often exceeds any transition disruption.

Vendor lock-in deserves serious consideration. Address it through contractual provisions ensuring data portability, API-first architectures, multi-year contracts with clear performance expectations, and maintaining awareness of alternative vendors. The goal is strategic partnership with a small number of vendors, not complete dependence on a single provider.

# Moving forward

> Tool sprawl represents one of the most significant operational challenges facing security leaders today. The average organization's 45-tool security stack creates inefficiency, undermines effectiveness, and contributes to analyst burnout.

With 75% of organizations actively pursuing vendor consolidation, we're witnessing a fundamental shift in how security programs are built and operated.

External threat intelligence programs illustrate both the problem and the solution. Traditional fragmented approaches create overwhelming alert volume, integration complexity, and missing context. Consolidated platforms deliver unified visibility, contextual intelligence, and actionable insights while dramatically reducing operational overhead.

Success requires thoughtful execution: honest auditing of your current state, strategic planning that balances capability with manageability, impact-based prioritization, proper change management, and continuous optimization. With the external threat intelligence market projected to grow from $1.55 billion in 2024 to $6.55 billion by 2029, organizations have expanding options for consolidated platforms that address multiple use cases effectively. The question isn't whether to consolidate—it's how quickly you can execute a strategy that improves both security outcomes and operational efficiency.

WRAPPING UP

# Consolidation facts to share with your team

## 1. Tool Sprawl

75+ security products per organization

The average enterprise manages 75+ security products from multiple vendors, creating integration complexity and expanding the attack surface through fragmented visibility.

Source: Gartner Security Platform Consolidation Research

## 2. Alert Overload

54% of security alerts never investigated

SOC teams receive up to 10,000 daily alerts across disparate systems; over half remain uninvestigated due to volume and lack of context.

Source: CybelAngel 2024 State of EASM Report

## 3. CISO Burnout

94% report job-related stress impacting performance

Job-related stress affects performance for 94% of CISOs surveyed, with 63% reporting direct burnout observations in security teams.

Source: IANS State of the CISO Report 2025

## 4. Platform ROI

4x greater ROI with unified platforms (101% average)

Organizations implementing unified security platforms achieve four times greater return on investment compared to maintaining fragmented tool stacks.

Source: Forrester Total Economic Impact™ of CybelAngel

## 5. Market Adoption

75% of organizations pursuing vendor consolidation

Three-quarters of surveyed organizations actively pursued security vendor consolidation in 2022, establishing consolidation as industry standard practice.

Source: Gartner Survey on Security Vendor Consolidation

## 6. External Attack Surface

79% of exposures originate outside the perimeter

Nearly eight in ten critical data exposures stem from third-party services, Shadow IT, and unmanaged cloud resources beyond direct organizational control.

Source: CybelAngel 2024 State of EASM Report

# Further reading

Gartner, “Simplify Cybersecurity With a Platform Consolidation Framework”

Forrester, “The Total Economic Impact™ of CybelAngel”

Gartner, “Top Strategic Technology Trends for 2025”

ESG Research, “The Cybersecurity Talent Shortage and the Skills Gap”

NACD (National Association of Corporate Directors), “Cyber-Risk Oversight Handbook”

PwC, “Global Digital Trust Insights Survey”

McKinsey & Company, “Cybersecurity for Board Members: Key Strategies”