



Heimdal®



FUTURES SAFE



CRITICAL

Brute-force login attempts on
srv-web-03 (10.2.45.18)



HIGH

Malware Trojan.GenericKD.631025
quarantined on LAPTOP-4521



HIGH

Data spike: 3.2 GB
outbound from NODE-4



MEDIUM

Excessive MFA failures
from 185.22.14.77.



CRITICAL

12 endpoints missing
patch KB5028166.

The State of MSP Agent Fatigue in 2025

When Security Tools Become the Problem They're Meant to Solve

MSPs are drowning in complexity.

Not from threats, but from the tools meant to protect against them.

You jump between consoles all day while clients complain about slow machines weighed down by multiple agents.

Each new "solution" promises simplicity but delivers another vendor relationship to manage, another alert stream consuming hours meant for growing your business.

We surveyed 80 MSPs across North America. More than half face alert fatigue weekly. Integration failures plague everyone.

This documents a broken system where security vendors chased feature lists over operational reality. Tool sprawl hurts everything.

MSPs deserve unified platforms that reduce complexity and deliver effective risk mitigation at a competitive cost, not point solutions that drain budgets and burn out teams.

Agent fatigue ends here.



Jesper Frederiksen

CEO at Heimdal

Agent fatigue isn't just a tech issue, it's a business risk.

MSPs are juggling tool after tool, but none of these solutions actually work together.

Risk data isn't shared, remediation isn't unified, and worse, clients feel the impact.

We saw this mess firsthand and spent over a year pressure-testing platforms before landing on Heimdal.

Not because it was trendy, but because it was the first solution that truly consolidated what mattered: protection, performance, and real-time response.

We're not here to sell whatever's profitable, we're here to find what actually works, test it hard, and stand behind it.

That's why FutureSafe exists. To cut through the noise and make cybersecurity something MSPs can actually deliver - **without burning out.**



Jason Whitehurst
CEO Futuresafe

Table of Contents

Main findings	05
Introduction: MSPs are struggling with agent fatigue	08
Background: A boom in cybersecurity tools	12
Methodology: A study into agent fatigue at MSPs	14
Analysis of the results	17
How are MSPs adapting to agent fatigue?	26
Conclusion: An end to agent fatigue?	31
Recommendations for tackling agent fatigue	34

Main Findings

"Too many tools... I wish we had one solution that does it all."

This desperate plea from an enterprise MSP managing 10+ security tools crystallizes what 80 managed service providers across North America told us in the first half of 2025.

They're drowning in alerts, juggling disconnected dashboards, and watching their best employees burn out.

What started as a suspicion in MSP forums and Slack channels is now confirmed by hard data: the tools meant to protect clients are breaking the people who manage them.

Understanding Agent Fatigue

We've all felt it.

That moment when another alert pings, and instead of investigating immediately, you pause. You're tired. You've checked dozens of false positives today. Your tools don't talk to each other. You're switching between dashboards just to understand what's happening.

This is agent fatigue.

And it's not just impacting individuals. It's compromising security outcomes across the entire MSP sector.

The Numbers Tell a Disturbing Story

Daily Exhaustion is the New Normal

56% of MSPs experience alert fatigue daily or weekly.

Most concerning is that 44% of large MSPs (501+ employees) face this burden every single day, and for those managing 1,000+ clients, daily fatigue is universal at 100%.

Integration is a Myth for Most

Only 11% enjoy seamless tool integration. The rest are drowning in swivel-chair operations.

89% must maintain multiple separate dashboards. Imagine explaining that inefficiency to a client.

False Positives: The Silent Killer

1 in 4 security alerts are false positives. That's thousands of wasted investigations.

Teams dealing with high false positive rates are significantly more likely to be fatigued.

It's a vicious cycle: more tools → more alerts → more false positives → more fatigue.

The Hidden Impact: When Fatigue Costs Lives

Here's what should keep every MSP owner awake at night: fatigued teams miss real threats.

MSPs experiencing high alert fatigue are significantly more likely to report missed or delayed threat responses. The tools meant to enhance security are creating blind spots through sheer exhaustion.

As one MSP confessed:

"My biggest challenge is seamless interoperability between tools while avoiding data silos, alert fatigue, and configuration conflicts that can reduce overall security effectiveness."

The Path Forward is Clear. If You're Brave Enough

The good news buried in our data?

20% of MSPs have already cracked the code.

These MSPs consolidated their security stack and report:

- Dramatically reduced complexity without sacrificing coverage
- Clearer visibility through integrated platforms
- Faster response times
- Simplified billing, onboarding, and compliance
- Most importantly: teams that aren't burned out

The stark reality: Agent fatigue is solvable.

The question is whether you'll be among the 20% taking action or the 56% still "considering it" while fighting fires all day.

In This Report

We surveyed 80 managed service providers in the first half of 2025 to understand the true impact of security tool proliferation.

The results paint a picture of an industry at a breaking point. But also reveal a clear path forward.

Agent Fatigue by the Numbers

- Over 75% of MSPs experience alert fatigue at least monthly
- About 25% of all security alerts are false positives
- Only 11% report seamless app integration across platforms
- The correlation is undeniable: more tools = more fatigue

Real-World Consequences

- Teams with higher false positive rates are significantly more likely to be fatigued
- Fatigued teams are significantly more likely to miss actual threats
- The irony: more security tools can mean less security

The Response So Far

- Only 20% of MSPs have consolidated their security solutions
- 56% are "considering it"—paralyzed by inertia
- Alternative strategies (tuning alerts, using AI) provide band-aids, not cures

INTRODUCTION:

MSPs are Struggling with Agent Fatigue

Too Many Security Tools Hinder MSPs - Rather Than Help Them

"Our apps don't fully integrate so we have to keep checking multiple platforms or the apps don't integrate at all and then we waste a lot of time trying to manage all of the platforms and who's managing them."

Small MSP, multi-vertical MSP

Every day, managed service providers are bombarded with alerts. Hundreds of them. From dozens of tools. Across thousands of endpoints.

These tools are essential.

They monitor for breaches, identify suspicious activity, and protect client data. But they're also creating an epidemic of exhaustion that's compromising the very security they're meant to provide.

MSPs must investigate every alert, assess severity, and decide on action.

When you multiply this by multiple tools that don't communicate, false positives that waste time, and the pressure of protecting numerous clients, you get a workforce that's tired, overworked, and frustrated.

We call this state 'agent fatigue'.

And it's reaching crisis levels.

What is Agent Fatigue?

Agent fatigue is the burnout MSPs experience when overwhelmed by too many security tools, endless alerts, and poor integration.

But it's more than mental exhaustion. It's a warning sign that your cybersecurity stack is actively working against you.

Think of it as death by a thousand paper cuts.

Each additional tool adds:

- More updates to manage
- More interfaces to learn
- More dashboards to monitor
- More vendors to coordinate
- More alerts to investigate
- More false positives to dismiss
- More time lost to context-switching

The result? Security teams spending more time managing tools than managing threats.

Understanding the Scale of Agent Fatigue

At Heimdal, we regularly hear MSPs describe these symptoms.

But anecdotes aren't data.

So we surveyed 80 North American MSPs to quantify what the community has been feeling.

The data confirms what MSP forums have been discussing: this is an industry-wide crisis.

Key Survey Findings

Alert fatigue isn't a "big MSP problem" but an industry epidemic affecting three-quarters of MSPs monthly. Even small operations are drowning in false positives, with larger MSPs bearing the heaviest burden.

Nearly 9 out of 10 MSPs are trapped in what one respondent called a "fragmented nightmare" of disconnected tools. The dream of unified security remains elusive, forcing teams to manually piece together threats across dashboards.

What starts as a 5-tool average quickly spirals out of control, with some MSPs juggling over 10 platforms. Each additional tool doesn't just add complexity but multiplies it exponentially, creating an operational maze.

The hidden cost of fragmented tools shows up in billing complexity, painful onboarding, and manual reporting that drains resources. MSPs are losing revenue not to security breaches, but to inefficiency managing their own stack.

MSP Insight

"**A common challenge** I face when integrating multiple security tools is ensuring seamless interoperability between them. They often use different data formats, APIs, or logging standards, which makes centralized visibility and correlation of security events more complex".

Large MSP, hospitality

Reading This Report

This report reveals the true state of MSP agent fatigue through three lenses:

- The Root Causes: We explore how the cybersecurity tool boom created today's overwhelming complexity
- The Current Reality: We analyze survey data showing how fatigue manifests and impacts MSP operations
- The Path Forward: We examine how pioneering MSPs are successfully tackling this challenge

Each section includes direct quotes from survey respondents.

Because sometimes the raw frustration of "Everything" (one MSP's answer to "biggest frustration") says more than any statistic.

BACKGROUND:

A Boom in Cybersecurity Tools

MSPs Are Using More Cybersecurity Agents Than Ever

"The good thing is having best of breed; the bad thing is that there is no integration between them."

Small MSP, healthcare

This rueful observation captures the MSP dilemma perfectly.

Over the past decade, the cybersecurity landscape has exploded with specialized tools.

Each promises to solve a specific threat. Each claims to be essential. Each adds another layer of complexity.

The Perfect Storm

Several forces converged to create today's tool sprawl:

Remote work exploded overnight, massively expanding attack surfaces. Cloud adoption accelerated, rendering perimeter security obsolete, while BYOD policies multiplied endpoints.

Each workplace transformation demanded specialized security tools to address newly discovered vulnerabilities.

Ransomware evolved into industrialized operations.

Nation-state tactics trickled down to common criminals, while AI-powered attacks and commoditized zero-day exploits democratized advanced threats.

Each new threat type spawned defensive tools, creating an arms race that favored vendors over MSPs managing an ever-expanding security arsenal.

GDPR, HIPAA, PCI-DSS, SOC 2, NIST and other frameworks became daily reality.

Each demanded specific controls and dedicated tools, while auditors expected separate solutions for every requirement. MSPs couldn't refuse tools that checked compliance boxes, even when they created operational chaos.

Venture capital flooded cybersecurity, funding thousands of startups promising silver bullets.

Each vendor focused on narrow niches, creating highly specialized tools. Integration was always "on the roadmap" but rarely materialized.

The Unintended Consequences

What started as "best of breed" selection became a monster.

A 2025 IBM study found that organizations now juggle an average of 83 different security tools from 29 different vendors. (Note: typically, several point solutions are bundled into one tool - for example, an antivirus tool might include point solutions for virus scanning, quarantining, or data cleanup).

For MSPs managing multiple clients, multiply that complexity.

Too Much of a Good Thing?

"Integrating multiple security tools is tough because they often don't work well together, create too much data to manage, and require specialized skills. It's also expensive and can lead to vendor lock-in".

Large MSP, financial services

MSPs face an impossible choice. Their contracts promise "best-in-class protection" - which clients interpret as "all available tools."

So MSPs deploy:

- Antivirus (usually multiple engines)
- Firewalls (network and host-based)
- EDR (Endpoint Detection and Response)
- XDR (Extended Detection and Response)
- Threat hunting tools
- Email security gateways
- DNS filtering
- SIEM platforms
- Vulnerability scanners
- Patch management systems
- Compliance platforms
- And more...

Each tool is powerful individually. Together, they create chaos:

Operational Chaos

- Silos: Each tool measures different things with different metrics
- Context switching: MSPs jump between 5-10 interfaces to investigate one incident
- Learning curves: New hires need months to become proficient
- Alert storms: 7 tools × 20 customers × dozens of daily alerts = overwhelming noise
- Missed threats: Critical alerts hide in the avalanche of notifications

The False Promise of "More is Better"

Here's the bitter irony our survey revealed: MSPs with the most tools were most likely to miss real threats.

Tool proliferation doesn't enhance security. It degrades it through MSP exhaustion.



MSP Insight

"Some of our security tools have steep learning curves and are difficult to navigate, requiring significant time and training for our analysts to master. The lack of intuitive interfaces makes it hard to quickly identify and respond to threats".

Enterprise MSP, hospitality

The cybersecurity industry has given MSPs powerful weapons.

But when you're carrying 10 different weapons, each with its own manual, maintenance schedule, and quirks, you're more likely to trip over your own arsenal than stop an attacker.

METHODOLOGY:

A Study into Agent Fatigue at MSPs

Our Survey Methodology and Respondents

The symptoms of agent fatigue have been discussed in MSP forums, Reddit threads, and Slack channels for years.

MSPs share war stories of 3 AM false positive alerts. Owners complain about turnover.

Everyone agrees something's wrong.

But how bad is it really? How widespread? What's driving it? Most importantly - what works to fix it?

We decided to move beyond anecdotes and gather hard data.

Methodology

We developed a hypothesis based on thousands of conversations with security professionals and our own market observations:

Managed service providers are overwhelmed by the growing number of security and compliance tools they use and are experiencing agent fatigue. This growth is hindering their ability to do their jobs effectively.

To test this, we created a 25-question survey mixing closed-ended questions for quantitative analysis and free-text responses for qualitative insights.

The survey launched in H1 2025. We used Large Language Model analysis to perform thematic coding on over 300 free-text responses, with human validation ensuring accuracy.

About the Respondents

We received 80 responses from a diverse cross-section of the MSP community:



Industry Focus MSPs served diverse sectors, with healthcare, financial services, and multi-sector providers most common. This diversity ensures our findings aren't skewed by single-industry peculiarities.

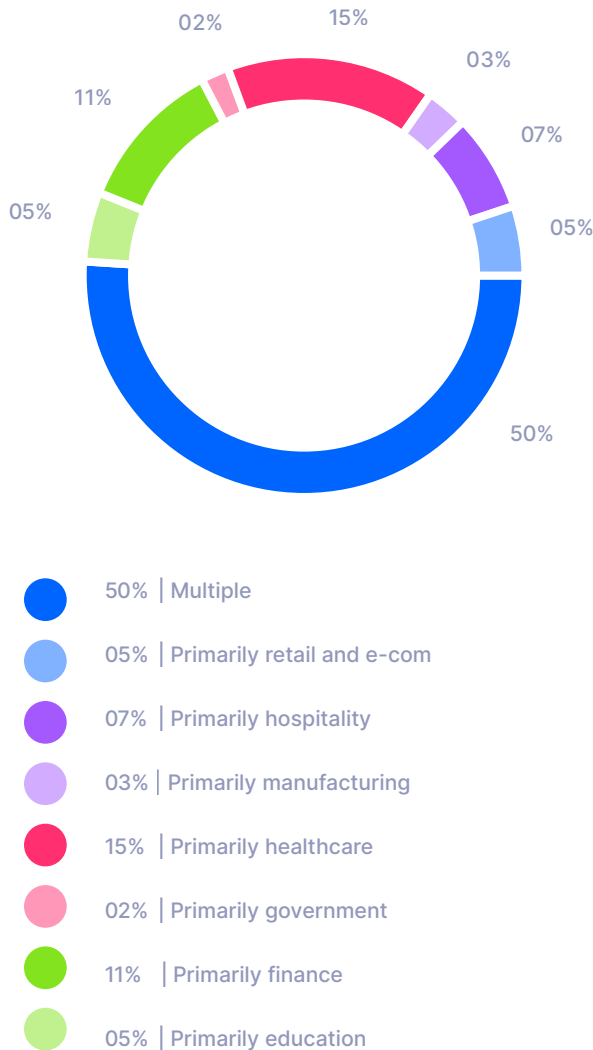


Figure 1: Primary Sectors Served

Security Tools Being Used

The variety of tools in use reflects the fragmented security landscape:

Most Common Tool Types

- **Endpoint Detection & Response (EDR) – 89%**
- **Antivirus/Antimalware – 83%**

- **Antivirus/Antimalware – 83%**
- **Firewalls – 81%**
- **Patch/Vulnerability Management – 79%**
- **DNS filtering – 69%**
- **XDR suites – 59%**
- **SIEM platforms – 46%**

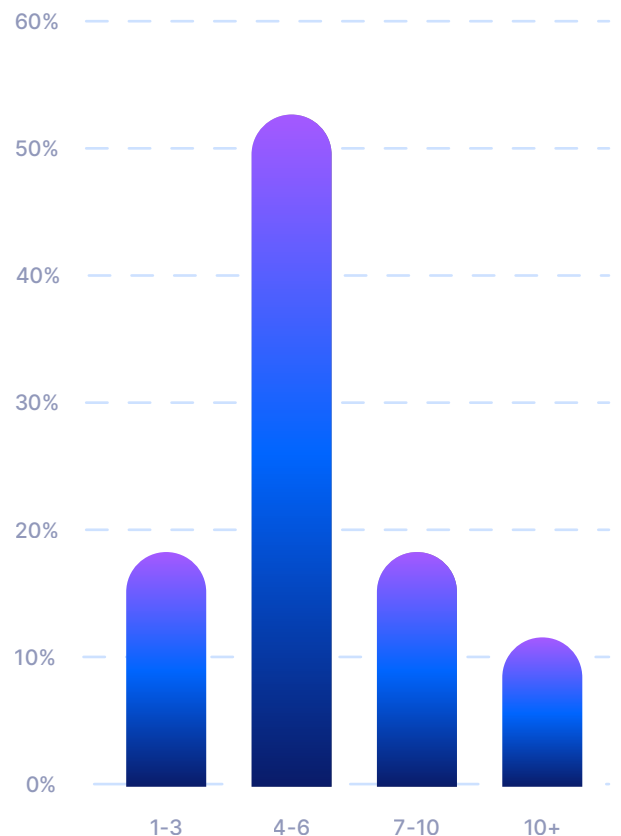


Figure 2: How Many Security Tools Do You Actively Use?

The majority cluster around 4-6 tools, which might seem manageable.

However, remember that each security tool is really a small toolbox. Its built-in modules (AV, EDR, vulnerability scanning, etc.) each spit out their own alerts and updates, adding extra work.

The 20% using 7-10 tools and 12% using 10+ are walking case studies in complexity overwhelming capability.

Analysis of the Results

A Picture of Agent Fatigue

"The complexity of configuring and managing all these different tools is overwhelming. It feels like we need a dedicated team just to keep them running".

Small MSP, multi-vertical MSP

This quote emerged from our free-text responses, but it could have come from any of the 80 participants.

The data reveals an industry where exhaustion has become normalized.

MSPs Are Feeling Overwhelmed

Our survey provides irrefutable evidence that agent fatigue is real, widespread, and directly linked to tool proliferation.

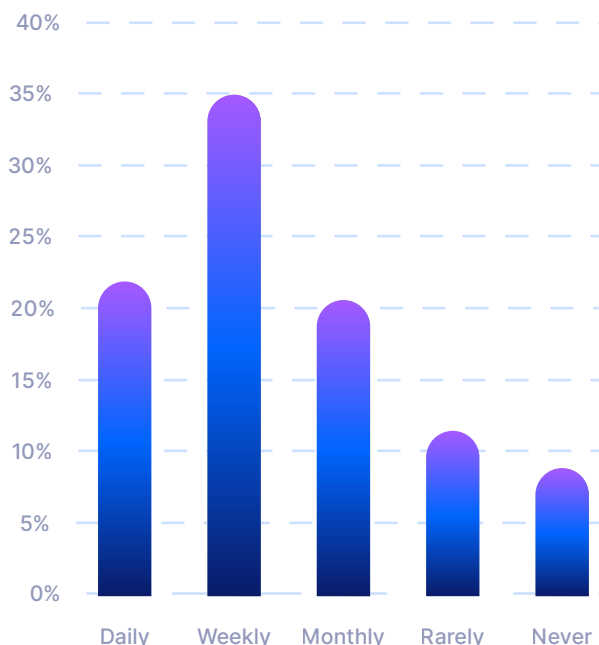


Figure 3: How Often Does Your Team Experience Alert Fatigue from Security Tools?

The Daily Grind of Exhaustion

Over half of MSPs experience alert fatigue either daily or weekly.

Think about that.

The majority of MSP security teams start their week knowing they'll be overwhelmed before Friday.

Large MSPs (501+ employees) face the worst of it: 44% experience daily fatigue. But size offers no protection.

Even micro MSPs with 1-10 employees report significant fatigue levels.

Client Count Multiplies the Pain.

The correlation is stark: more clients equals more fatigue.

Every MSP managing 1,000+ clients reported daily alert fatigue.

But even MSPs with 10 or fewer clients aren't immune - 47% still experience weekly fatigue.



Spotlight: Alert Fatigue is Nearly Universal

Over 75% of MSP experience alert fatigue at least monthly, and over 50% face it weekly or daily.

The more clients an MSP handles, the more likely their team is overwhelmed by alerts.

Alert fatigue stems directly from the multiplication effect: multiple tools × multiple clients × multiple sites × multiple alerts = exponential complexity.

Tool Quantity Drives Fatigue Quality

We compared tool counts against fatigue frequency and found a clear correlation:

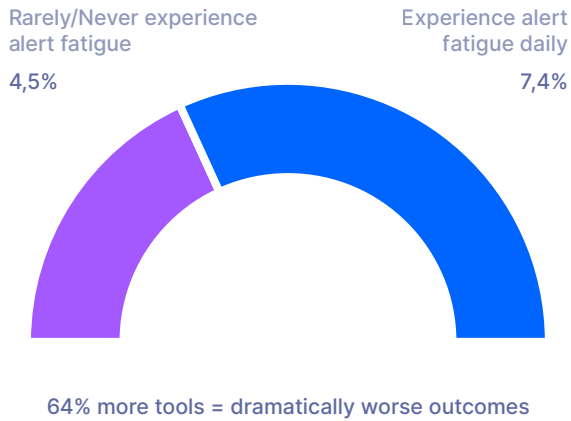


Figure 4: How Many Tools Do You Actively Use? (Average)

MSPs rarely experiencing fatigue use 4.5 tools on average.

Those facing daily fatigue? 7.4 tools.

That's a 64% increase in tools driving dramatically worse outcomes.



Spotlight: More Tools, More Fatigue

MSPs using 7+ tools experience nearly double the alert fatigue compared to those using 4 or fewer. Tool sprawl directly correlates with analyst burnout.



MSP Insight

"One MSP using over 10 tools who experiences daily alert fatigue captured the desperation: "Too many tools... I wish we had one solution that does it all".

Enterprise MSP, hospitality

Poor Tool Integration Increases Agent Fatigue

Integration, or lack thereof, emerged as the primary frustration source. Our LLM analysis of free-text responses revealed:

Top Frustration Themes

- Fragmentation/poor integration - 25 mentions
- Tool sprawl/too many dashboards - 18 mentions
- Manual effort/lack of automation - 14 mentions

Remarkably, 90% of free-text responses contained negative language: "too many tools," "waste of time," "overwhelming," "difficult," "frustrating." One MSP summed up their entire experience with a single word: "Everything."



MSP Insight

"The complexity of configuring and managing all these different tools is overwhelming. It feels like we need a dedicated team just to keep them running".

Small MSP, multi-vertical MSP

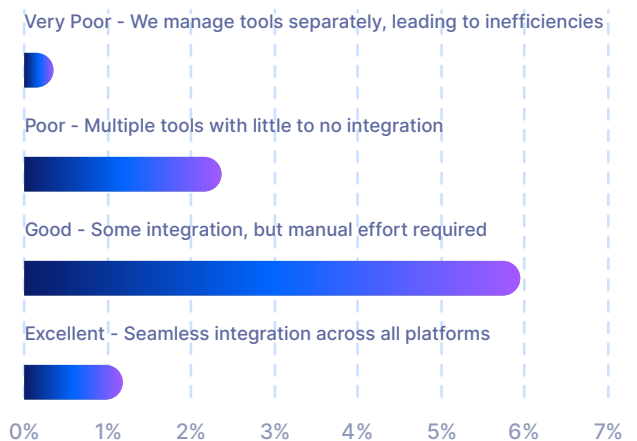


Figure 5: How Well Do Your Security Tools Integrate with One Another?

The numbers tell a stark story:

- Over 25% report poor or very poor integration
- Only 11% enjoy seamless integration
- The vast majority juggle multiple dashboards and databases



Spotlight: Integration is the Bottleneck

Poor integration is the most commonly cited frustration, with only 11% of respondents reporting seamless tool interoperability. Fragmented dashboards and data silos are fueling fatigue.

The free-text responses paint a picture of daily frustration:

- "Lack of true integration / single pane view" was mentioned 33 times
- "Incompatible APIs / data formats" appeared in 28 responses
- "Too many manual touches required"
- "Jumping through multiple tools is difficult"

The pattern is clear: better integration correlates with less fatigue.

MSPs with excellent integration rarely experience daily fatigue, while those with poor integration are far more likely to be overwhelmed.



MSP Insight

"**Our biggest challenge** is trying to achieve a single pane of glass approach so our technicians can see all the information for a customer's system in a single location without having to go between multiple consoles".

Large MSP, financial services

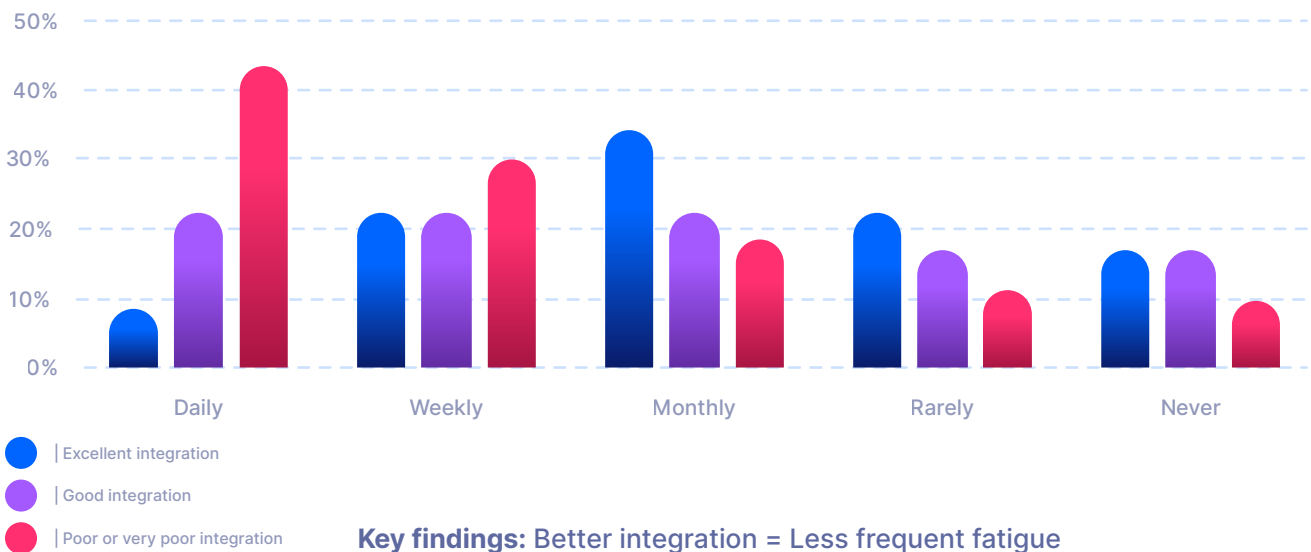


Figure 6: Frequency of Alert Fatigue Compared to Security Tool Integration

Agent Fatigue is Linked to False Positives

If alert volume is exhausting, false positives are demoralizing. Every false positive represents wasted time, eroded trust, and increased cynicism.

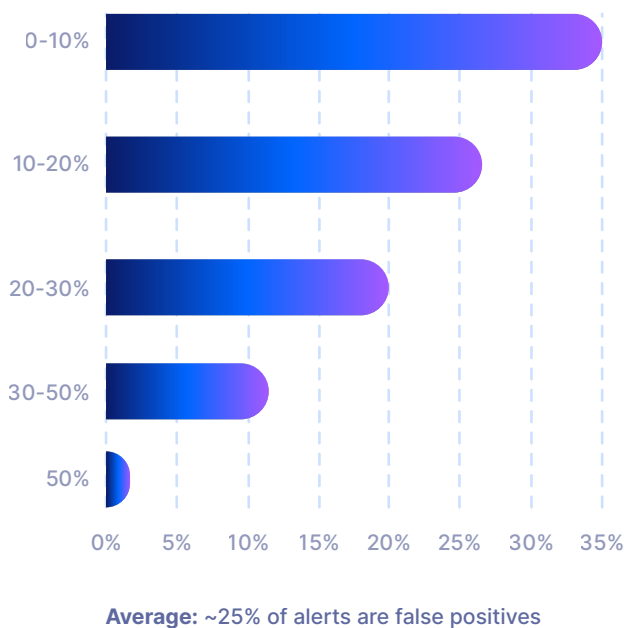


Figure 7: What Percentage of Alerts from Your Security Tools are False Positives?

The false positive problem is staggering:

- Nearly one-third of MSPs report 30%+ false positive rates
- For most, 1 in 4 alerts are noise
- Each false positive investigation steals time from real threats



Spotlight: False Positives Waste Time and Morale

Nearly one-third of MSPs say 30%+ of their alerts are false positives. These red herrings waste hours and compound fatigue, especially in teams already drowning in alerts.

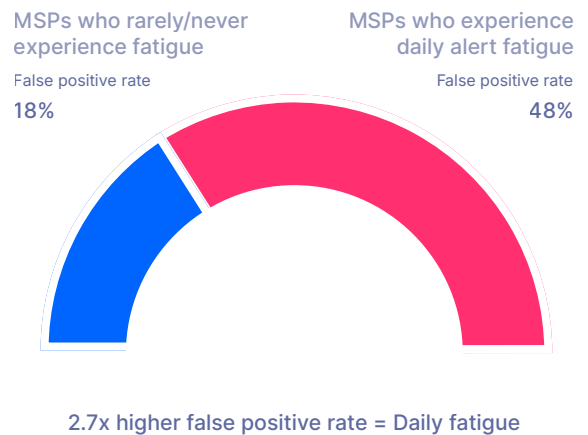
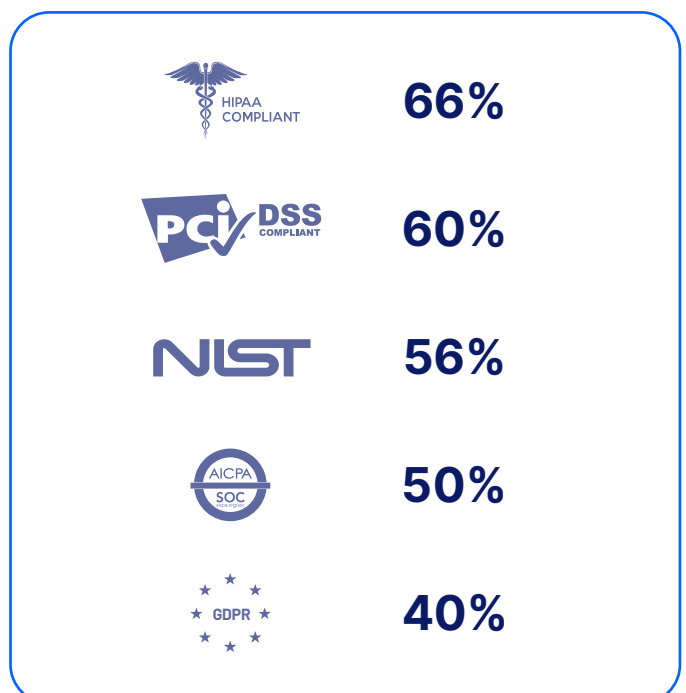


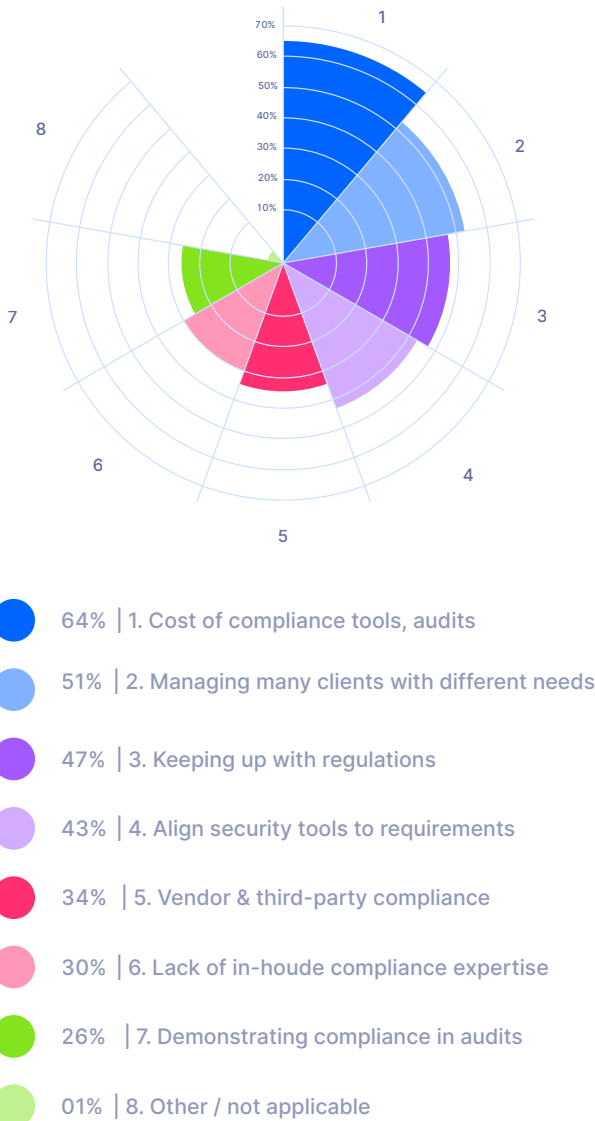
Figure 8: Alert Fatigue Versus False Positives

The correlation is undeniable: high false positive rates triple the likelihood of experiencing fatigue. It's a vicious cycle—more tools generate more alerts, which include more false positives, which exhausts analysts, who then miss real threats.

Compliance Challenges Influence Agent Fatigue

Compliance adds another layer of complexity. Our respondents juggle multiple frameworks:





(Percentage exceed 100% because respondents could choose multiple options)

Figure 9: Biggest Compliance Challenges MSPs Face

After cost, nearly every other compliance challenge relates to agent fatigue:

- Managing different client requirements
- Keeping up with changing regulations
- Aligning security tools to frameworks
- Demonstrating compliance across multiple tools

When asked about ideal compliance solutions, MSPs overwhelmingly wanted:

- "Automation / continuous monitoring" - 28 mentions
- "Unified / all-in-one tools" - 22 mentions
- "Better reporting & dashboards" - 18 mentions

MSPs aren't asking for another compliance checklist.

They want an integrated compliance companion that lives within their existing tools.

Too Many Tools Increases Admin Burden

The operational impact extends beyond security into core business processes.

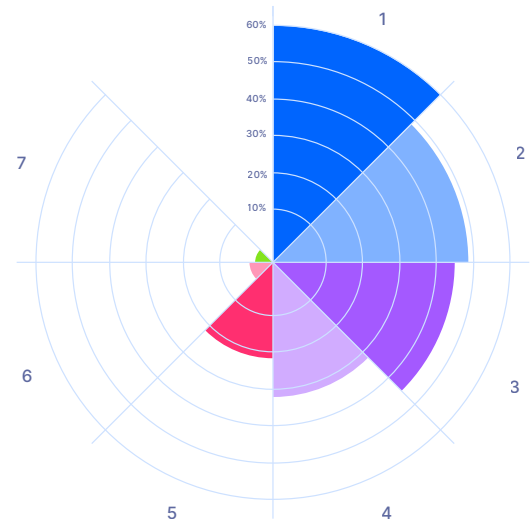


Figure 10: Biggest Billing and Invoicing Pain Points

Billing complexity stems from:

- Different pricing models per tool (per-seat, per-device, per-GB)
- Tracking usage across multiple platforms
- Reconciling vendor invoices with client billing
- Time wasted on manual calculations

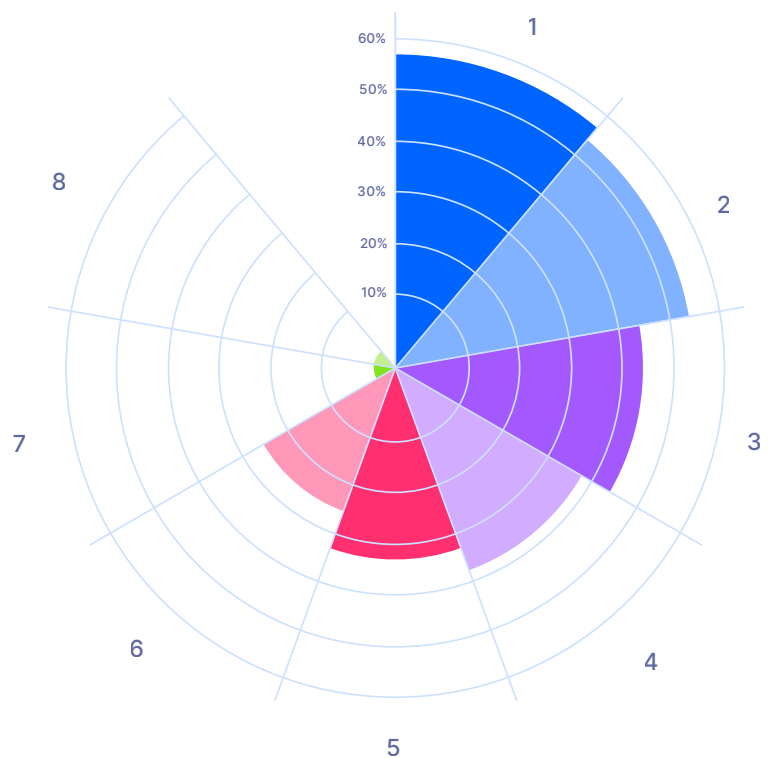


Figure 11: Biggest Onboarding Challenges for New Clients

Onboarding reveals the true cost of complexity:

- Rolling out multiple agents to new environments
- Training clients on various portals
- Coordinating between different vendor requirements
- Manual deployment processes that should be automated

Over half of respondents specifically mentioned "lack of automation in the process" as their primary onboarding frustration.

Agent Fatigue Has Consequences

The ultimate question: does fatigue impact security outcomes?

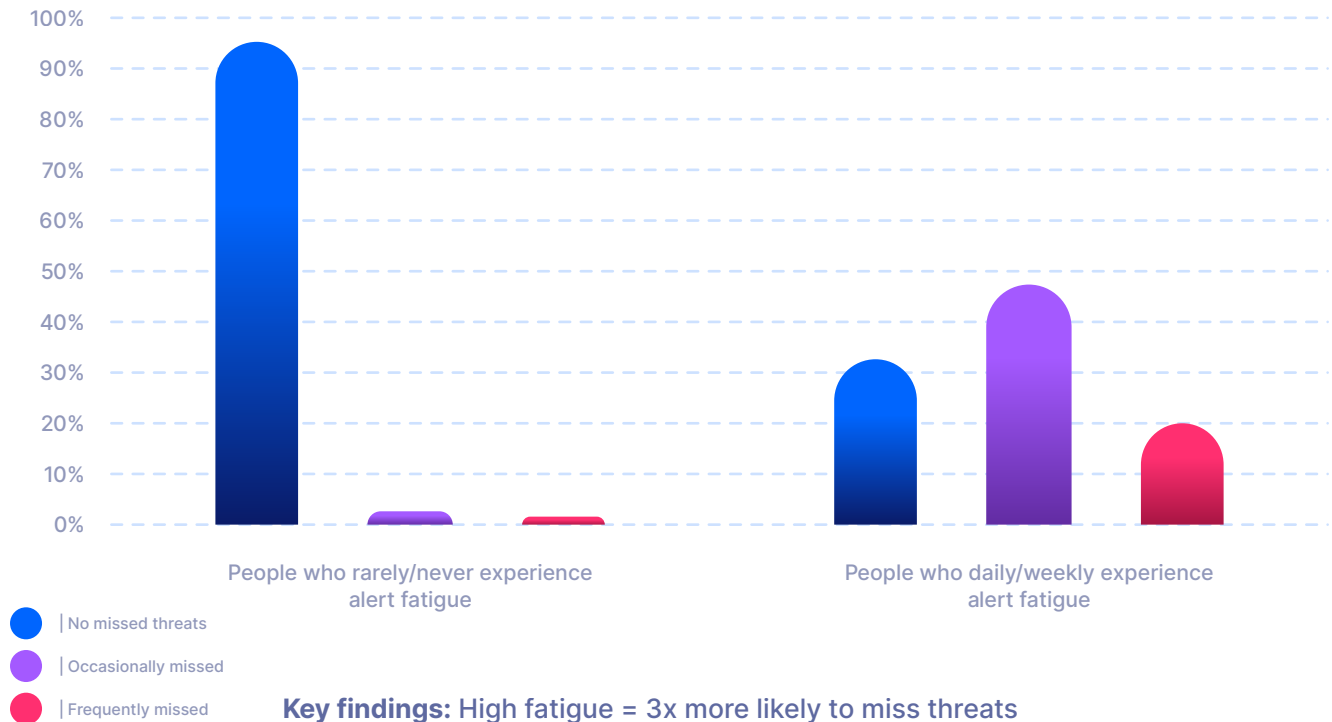


Figure 12: Has Alert Fatigue or Too Many Security Tools Ever Led to a Missed or Delayed Response to an Actual Threat?

The answer is unequivocal: yes.

MSPs experiencing less fatigue rarely miss threats. Those with daily or weekly fatigue are significantly more likely to report missed or delayed responses.



Spotlight: Fatigue Has Real-World Consequences

MSPs with high alert fatigue are significantly more likely to miss real threats. Ironically, using more tools does not prevent breaches - it increases the risk of missing them.

Most disturbing: having more security tools correlates with MORE missed threats, not fewer.

MSPs with the highest tool counts were most likely to report missed incidents.



MSP Insight

"My biggest challenge is seamless interoperability between tools while avoiding data silos, alert fatigue, and configuration conflicts that can reduce overall security effectiveness".

Medium sized MSP, multi-vertical MSP

Analysis of the Results

Chapter Summary

Our analysis reveals an industry in crisis.

Alert fatigue affects the vast majority of MSPs, with over 75% experiencing it monthly or more. This isn't a problem affecting only large operations.

The data shows that tool proliferation directly drives fatigue, with each additional tool multiplying complexity exponentially.

Poor integration amplifies the problem, forcing analysts to work harder for increasingly worse outcomes. The operational impact extends far beyond security response.

False positives erode team morale, wasting precious time on non-threats while real dangers lurk undetected.

Meanwhile, compliance requirements add layers of complexity without delivering meaningful protection value.

Business operations suffer through unnecessarily complex billing processes and manual client onboarding that drain resources from strategic work.

Most critically, our research confirms what many MSPs suspected. Fatigued teams miss real threats.

The data paints a clear picture of an industry where good intentions around comprehensive protection have created bad outcomes, leaving overwhelmed MSPs missing the very threats they set out to stop.

In the next chapter, we explore how MSPs are responding to this crisis.

How Are MSPs Adapting to Agent Fatigue?

Varied Strategies to a Common Issue

MSP Insight

"We have tried reduction in alert creation for low level impact data points, implementation of automation and aggressive filtering".

Medium sized MSP, multi-sector focus

Awareness of agent fatigue is nearly universal.

Our free-text analysis found 90% of respondents using negative language about their current setup.

Over half report weekly or daily exhaustion.

So what are MSPs doing about it?

The results reveal a striking pattern:

- **The Pioneers (20%):** Already consolidated and reporting positive outcomes
- **The Contemplators (56%):** Recognize the need but haven't acted
- **The Resisters (20%):** Prefer best-of-breed despite the pain
- **The Curious (4%):** Open to learning more



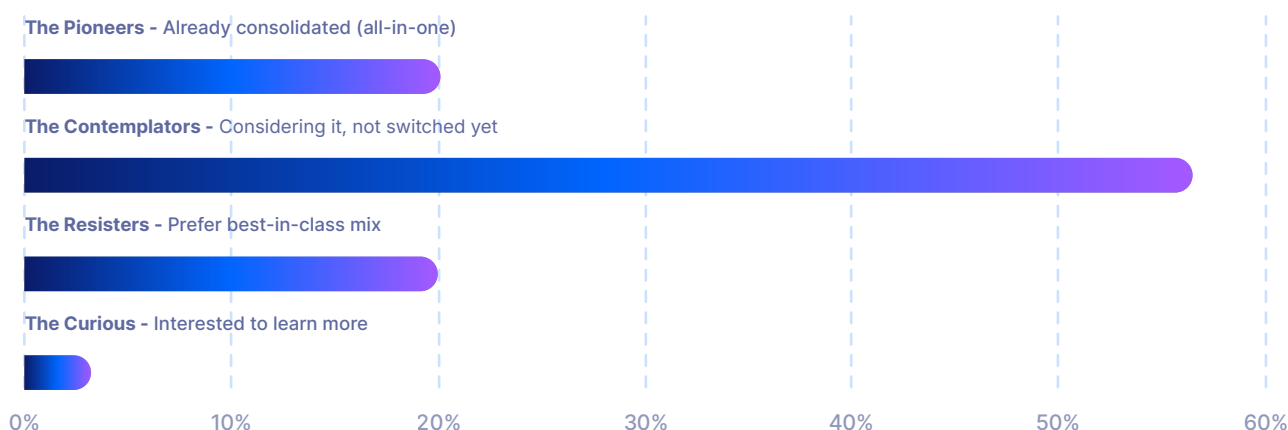
Spotlight: Many Know the Problem, Few Act

90% of MSPs express frustration with their current tool setup, yet over half haven't acted to consolidate or integrate. The awareness is there, but change is slow.

This gap between recognition and action deserves deeper exploration. Why do MSPs continue suffering when a solution exists?

Consolidating Tools

Tool consolidation represents the most direct path to reducing fatigue. Single-vendor platforms promise unified dashboards, consistent interfaces, and integrated workflows.



Key findings: 76% recognize need for consolidation, but only 20% have acted

Figure 13: Security Tool Consolidation

Barriers to Consolidation Include:

- **Sunk costs:** "We already paid for 3-year licenses"
- **Migration fear:** "Moving all our clients would be a nightmare"
- **Vendor lock-in concerns:** "What if we pick the wrong platform?"
- **Feature gaps:** "No single vendor does everything perfectly"
- **Inertia:** "We're too busy fighting fires to replace the fire truck"

Strategies to Reduce Fatigue

We asked MSPs: "What strategies have you tried to reduce alert fatigue?"

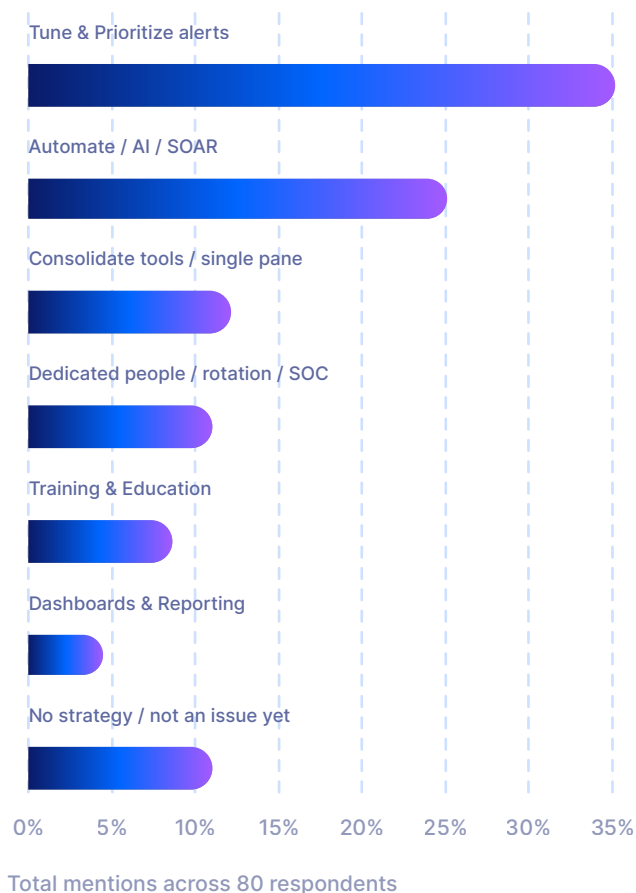


Figure 14: Strategies to Reduce Alert Fatigue

The Tactical Responses

We asked MSPs: "What strategies have you tried to reduce alert fatigue?"

Tuning and Prioritizing (35 mentions)

The most common approach - essentially accepting the tool sprawl but trying to reduce the noise.

MSPs report:

- Setting higher thresholds
- Filtering low-priority alerts
- Creating risk-based hierarchies
- Focusing on "critical only" notifications

Automation/AI/SOAR (25 mentions)

A promising but underutilized strategy. Only 31% have tried automation, despite its potential. Those who have reported significant benefits.

Consolidation (mentioned by the 20% who've done it)

These MSPs report the most comprehensive improvements. Not just reduced alerts but transformed operations.

MSP Insight on Strategies

"We've tried tuning alert thresholds, prioritizing high-fidelity alerts, integrating tools for centralized visibility, and using automation to handle low-risk events, freeing up time for more critical analysis".

Small sized MSP, multi-sector focus



MSP Insight on Strategies

"We use AI automation and assessment. Improved SOAR playbooks and per client exemptions and analysis".

Small MSP, multi-sector focus

Gap Between Words and Actions

The most revealing finding? The contradiction between stated priorities and actual behavior.

What MSPs Say They Want:

- 58% cite "ease of integration" as a top vendor selection factor
- Multiple free-text responses yearn for "single pane of glass"
- Integration frustration tops the complaint list

What MSPs Actually Do:

- Maintain fragmented toolsets from multiple vendors
- 20% explicitly prefer best-of-breed approaches
- Continue adding new point solutions

This cognitive dissonance reveals the power of inertia.

MSPs know integration is critical, yet continue operating fragmented environments.



Spotlight: The Talk-Do Gap

While 58% say integration is a top priority, many still use fragmented tools that don't communicate. MSPs know what they need, but internal inertia and vendor lock-in keep them stuck.

The Successful 20%

What differentiates the MSPs who've successfully consolidated?

Common Characteristics:

- **Leadership buy-in:** Consolidation was a strategic initiative, not a tactical fix
- **Phased approach:** They migrated gradually, learning as they went
- **Vendor partnership:** Chose vendors who supported the transition
- **Clear metrics:** Measured improvements in efficiency and outcomes
- **Team involvement:** Included the users in platform selection

These MSPs report:

- Significantly reduced false positives
- Clearer visibility across all clients
- Faster threat response times
- Improved analyst satisfaction
- Simplified compliance reporting

How Are MSPs Adapting to Agent Fatigue?

Chapter Summary

MSP responses to agent fatigue fall into three distinct categories.

The Band-Aid Brigade (20%)

These MSPs acknowledge the problem and respond with tactical fixes like alert tuning and basic automation.

While they recognize something needs to change, they remain fundamentally stuck in tool sprawl.

Despite their efforts, teams continue experiencing ongoing fatigue because the underlying complexity remains unchanged.

The Contemplators (56%)

The majority of MSPs fall into this category. They recognize consolidation as the answer and understand exactly what needs to happen.

However, they find themselves paralyzed by implementation challenges and migration concerns.

These MSPs are perpetually waiting for the "right time" that never seems to arrive, while their teams continue burning out in the background

The Pioneers (20%)

This group bit the bullet and consolidated their security stack.

They successfully overcame migration challenges and are now reaping significant benefits in terms of reduced fatigue, improved response times, and happier teams.

Most importantly, they serve as proof that transformation is not only possible but delivers measurable results.

The gap between awareness and action represents the real challenge facing the industry.

MSPs know what needs to be done. The question is whether they'll find the courage to act before agent fatigue causes irreparable damage to their teams and clients.

CONCLUSION:

An End to Agent Fatigue?

Some MSPs Can See a Future with Less Fatigue

After analyzing 80 survey responses and over 300 free-text comments, we can draw clear conclusions about the state of agent fatigue in the MSP sector.

Agent Fatigue is Alarming Common

The numbers don't lie:

- 75%+ of MSPs experience agent fatigue at least monthly
- Over half face it weekly or daily
- Large MSPs and those with extensive client bases suffer most
- But no MSP is immune - even small shops report significant fatigue

The qualitative responses reinforce the statistics.

MSPs describe feeling "overwhelmed," "frustrated," and "exhausted."

One summed up their entire security operation with a single word: "Everything" is their biggest frustration.

MSP Insight

"Our apps don't fully integrate so we have to keep checking multiple platforms or the apps don't integrate at all and then we waste a lot of time trying to manage all of the platforms and who's managing them".

Small MSP, multi-sector focus

This quote crystallizes the daily reality: MSPs aren't just managing security. They're managing the chaos of their security tools.

MSPs Want Change

Our survey reveals universal awareness of the problem:

- 90% use negative language about their current setup
- 58% prioritize integration when selecting new vendors
- Free-text responses overflow with wishes for "single pane of glass"
- MSPs have tried various strategies to address fatigue

The desire for change is palpable. MSPs understand that:

- Alert overload reduces effectiveness
- Poor integration wastes time
- Tool sprawl complicates billing and onboarding
- Fatigue increases the risk of missing real threats

They're implementing short-term tactics (alert filtering) and considering long-term strategies (consolidation).

The will exists, but execution lags.

Many MSPs Suffer from Inertia

Here's the painful irony: while MSPs desperately want change, most haven't taken decisive action.

Why the Paralysis?

- Sunk investments: "We've already spent so much on these tools"
- Migration complexity: "Moving all our clients would take months"
- Learning curves: "My team finally knows these systems"
- Vendor relationships: "We have contracts to honor"
- Daily firefighting: "We're too busy to stop and reorganize"

Only 20% have committed to consolidation.

Another 56% are "considering it" - a holding pattern that could last indefinitely while teams burn out.

The Success Stories Show the Way

The 20% who've consolidated report transformative results:

- Dramatically fewer false positives
- Clearer visibility across all clients
- Faster response times
- Simplified operations
- Happier teams

These pioneers prove agent fatigue isn't inevitable - it's a choice.

They faced the same challenges as everyone else but decided the status quo was unacceptable.

Recommendations for Tackling Agent Fatigue

1. Consolidate and Integrate

The data is unequivocal: fewer, integrated tools equal less fatigue and better outcomes.

MSPs using 4 or fewer integrated tools report:

- 50% less alert fatigue
- Fewer false positives
- Clearer threat visibility
- Simplified billing and onboarding
- More time for strategic work

Action steps:

- Audit your current tool inventory
- Identify redundancies and gaps
- Evaluate platforms that combine multiple functions
- Plan a phased migration approach
- Set clear success metrics

2. Automate Where Possible

Only 31% of MSPs have implemented AI/SOAR solutions—a massive missed opportunity.

Modern automation can:

- Triage alerts before they reach your team
- Auto-respond to known threat patterns
- Correlate events across multiple data sources
- Generate compliance evidence automatically
- Free analysts for high-value investigations

MSPs using automation report:

- 60-80% reduction in manual alert handling
- Faster mean time to response (MTTR)
- Consistent handling of routine incidents
- Improved job satisfaction

3. Invest in Compliance Platforms

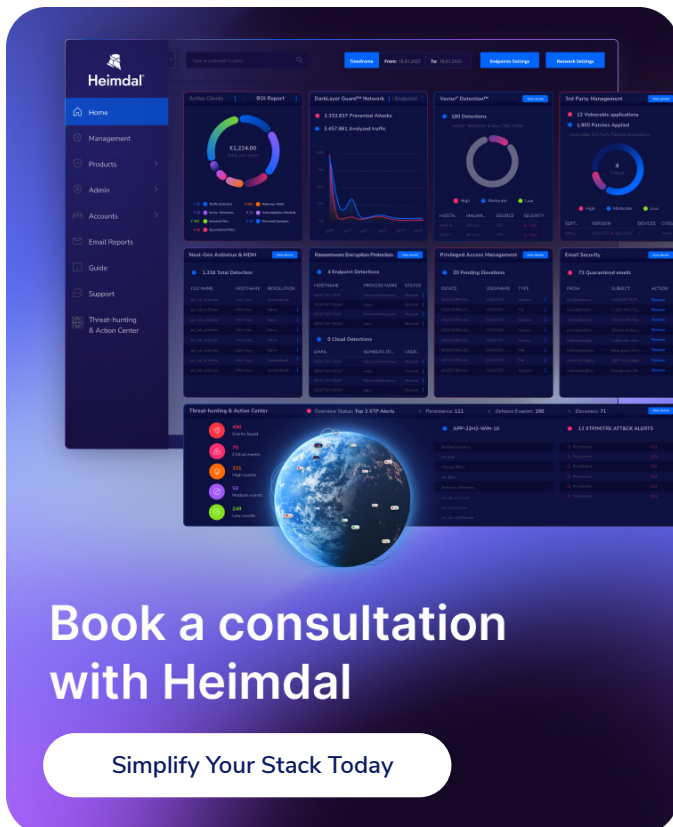
Compliance multiplies tool complexity unnecessarily.

A compliance platform is a software layer that plugs into your existing security tools, automatically maps each control to every required framework, continuously gathers evidence, and spits out audit-ready reports.

This eliminates spreadsheet-driven, manual compliance busywork.

Modern compliance platforms can:

- Map controls once, report to multiple frameworks
- Continuously collect evidence
- Generate audit-ready reports on demand
- Integrate with existing security tools
- Eliminate repetitive manual work



Book a consultation with Heimdal

Simplify Your Stack Today

Why You Should Consolidate: Comparison of MSP Security Strategies

Metric	Without Consolidation	With Consolidation
Tool Count	7+ tools from multiple vendors	Fewer tools, often from single provider
Alert Fatigue	Daily or weekly fatigue common	Alerts reduced and prioritized
Integration Issues	Multiple dashboards, poor interoperability	Single pane of glass, seamless workflows
Analyst Time	Spent switching tools and managing noise	Focused on real threats and analysis
Compliance Effort	Manual, repetitive, hard to scale	Automated, report-ready, always-on monitoring
Onboarding/Billing	Confusing, inconsistent, high-touch	Streamlined, consistent, and efficient
Threat Detection	Higher risk of missing real threats	Better visibility and faster response
Team Morale	Frustrated, overwhelmed, high turnover	Engaged, empowered, sustainable

Don't Put Up with Agent Fatigue

Is your team frustrated, overwhelmed, and struggling to differentiate real threats from noise?

You're not alone, but you don't have to accept it.

The path forward is clear:

- Acknowledge the true cost of agent fatigue (missed threats, team burnout, client risk)
- Commit to consolidation as a strategic priority, not a someday goal
- Partner with vendors who understand MSP challenges and support your transformation
- Measure the results in both operational metrics and team satisfaction

The Choice is Yours

Our research reveals an industry at a crossroads. The current path with ever more tools, ever more complexity, ever more fatigue, is unsustainable.

MSPs who continue down this road risk:

- Losing their best employees to burnout
- Missing critical threats in the noise
- Falling behind more efficient competitors
- Failing to meet client expectations

The alternative path...

- Consolidation
- Integration
- Automation

... requires courage and effort. But the 20% who've taken it report transformative results.

A Final Thought

One MSP who successfully consolidated told us: "Not really too frustrated, but I know we can do better and be more efficient."

Notice the calm confidence. No desperation. No overwhelming frustration. Just quiet satisfaction with room for continuous improvement.

This could be you.

The question is: will you join the 20% who've solved agent fatigue, or remain with the 56% still "considering it" while your team suffers?

The data shows the way.

The pioneers prove it's possible.

The only thing missing is your decision to act.

Want to Learn More?

Agent fatigue doesn't have to be your reality.

Modern platforms designed specifically for MSPs can eliminate the chaos while enhancing your security posture.

If you're ready to move beyond "considering" consolidation and want to understand how unified security platforms work in practice, we're here to help.

Share this report with your team. Discuss it in your MSP communities. And when you're ready to take action, reach out to vendors who truly understand the MSP challenge - not those offering just another tool to add to your stack.

Your team deserves better than daily exhaustion. Your clients deserve better than fatigued analysts. You deserve better than managing chaos instead of growing your business.

The future belongs to MSPs who solve agent fatigue. Will you be among them?

BREAK FREE FROM AGENT FATIGUE

Book Your Consultation

If this report resonates with the challenges your team faces...



daily fatigue



mounting complexity



missed threats

... you're not alone. But you do have options.

At Heimdal, in partnership with FutureSafe, the exclusive provider of Heimdal in the US, we work with MSPs daily to reduce agent fatigue, cut through tool sprawl, and bring clarity back to security operations.

No hard pitch. Just a real conversation about what's possible when you consolidate and simplify.

If you're ready to stop "considering it" and start taking action, book a consultation with our team.

We'll listen, map your current stack, and show you where you can eliminate pain without sacrificing protection.

Fewer agents. Fewer headaches. Stronger security.

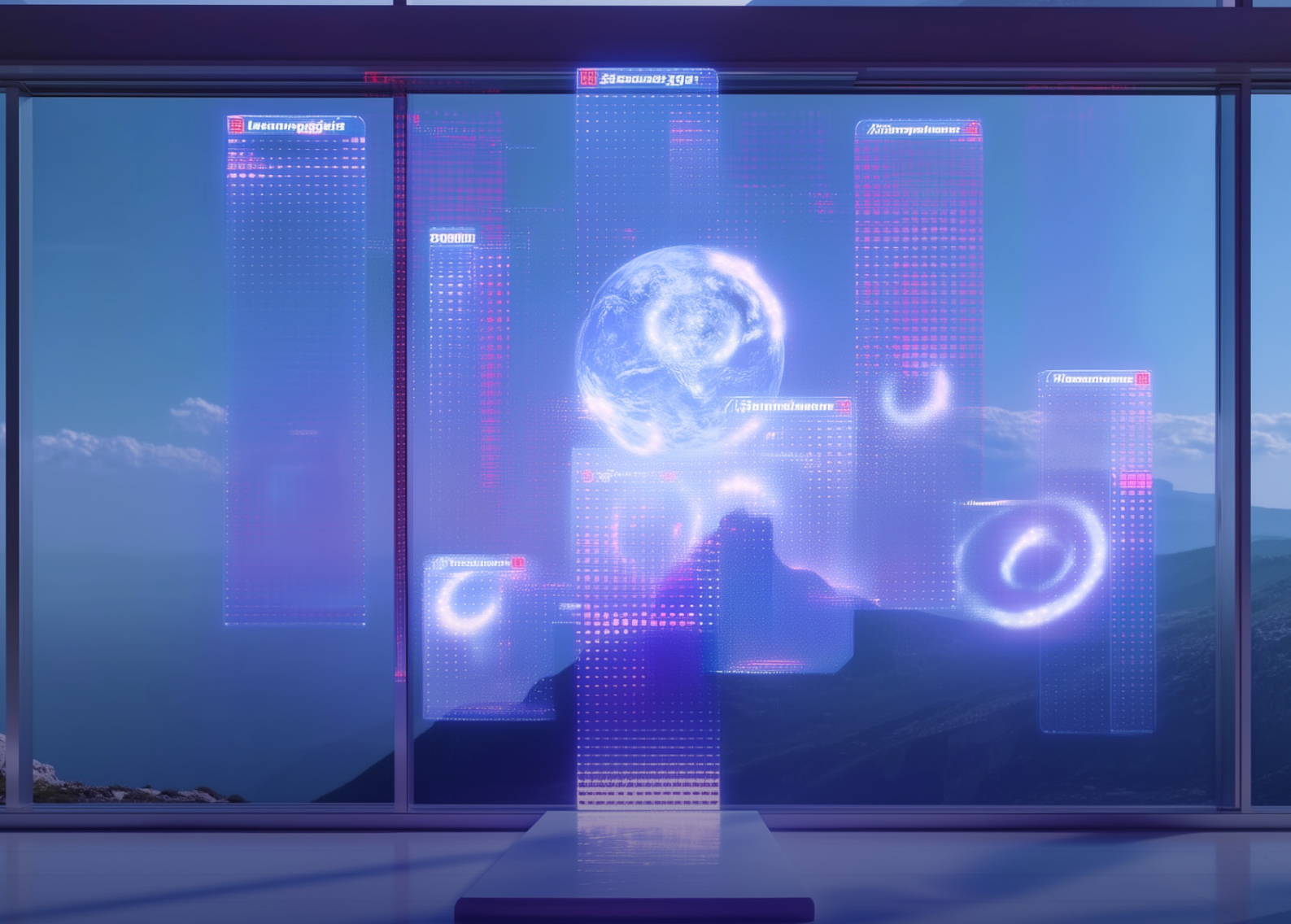


Heimdal®



FUTURESAFE

One Platform. Total Security.



heimdalsecurity.com

2025 Heimdal ®. All rights reserved. Registered trademarks and service marks are the property of their respective owners

Follow us on:

