Spur™

The 2026 IP Intelligence Study

The IP Intelligence Gap: Why Security Teams Struggle to Move from Detection to Decision

5 Best Practices for Turning IP Threat Signals into Real-Time Response

Table of Contents

Contents

Executive Summary 03

Methodology 04

Key Terms 05

FINDING 1: VPNs & Proxies Are Used in 94% of Security Incidents, but Visibility Is Lacking 06

FINDING 2: Credential Abuse via Proxies Causes Major Business Impact 08

FINDING 3: IP Intelligence Remains Reactive, Despite Demand for Proactive Use 09

FINDING 4: Employee Proxy Use Creates a Major Visibility – and Security – Gap 11

FINDING 5: IP Intelligence Workflows Are Fragmented Across Tools and Data Sources 13

FINDING 6: Lack of Context Is the Top Analysis Challenge 15

FINDING 7: IP Intelligence Effectiveness Is Rarely Measured 17

FINDING 8: Budget Constraints Delay Adoption, but Change Is Expected Soon 19

Best-Practice Recommendations for Security Teams to Advance Their IP Intelligence Programs 21

About Spur 23

Charts and Data References

Chart 1: Prevalence of anonymizing services in security incidents 06

Chart 2: Understanding of incidents from residential proxy abuse 07

Chart 3: Confidence in control over IP-based access paths 07

Chart 4: High-impact threats 08

Chart 5: Primary IP intelligence use cases 09

Chart 6: Operational use cases for IP intelligence 10

Chart 7: Current vs. desired IP intelligence capabilities 10

Chart 8: Current security posture over employee devices 11

Chart 9: Concerns over LAN access by residential proxies 12

Chart 10: Treatment of residential or consumer IP traffic in your organization 12

Chart 11: IP intelligence tooling 13

Chart 12: Integration points for IP intelligence 14

Chart 13: Biggest challenges with current IP approach 15

Chart 14: Value received from existing IP intelligence sources by area 16

Chart 15: KPIs used to measure IP intelligence effectiveness 17

Chart 16: Impact of ineffective IP intelligence 18

Chart 17: Operational impact of improved IP intelligence 18

Chart 18: Adoption plans for IP intelligence tools 19

Chart 19: Barriers to adoption 20

Executive Summary

Cyber criminals and fraudsters increasingly use anonymizing infrastructure such as VPNs and residential proxies to hide their malicious activity behind otherwise normal looking IP addresses, in turn bypassing traditional security defenses. Residential proxies in particular have become a pathway of choice for some of the most damaging incidents as reflected in Google's takedown of IPIdea, one of the world's largest residential proxies, and law enforcement takedown of the SocksEscort proxy network blamed for tens of millions in fraud. In fact, the U.S. Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) issued an alert in March 2026 identifying residential proxies as a key tool for cyber criminals.

The solution to better protect organizations from the risks of anonymized IPs is advanced IP context, but the results of the Spur 2026 IP Intelligence Study show that organizations have a long way to go to move beyond simple reactive IP enrichment to better understand the *who* and *why* behind IP addresses.

This study examines how organizations use IP intelligence to detect threats, investigate incidents, and enforce security controls.

Respondents report that anonymizing infrastructure such as VPNs and residential proxy networks appear frequently in security incidents, creating challenges for detection and attribution with existing tooling. At the same time, organizations report significant gaps in context, measurement, and internal visibility, limiting the effectiveness of current IP intelligence programs.

The results show that IP intelligence is widely adopted but still immature and fragmented in practice. Most organizations rely on it primarily for reactive investigation and blocking, while only a minority of companies use it for predictive security decisions or automated enforcement.

Key Findings

Across the survey results, three major findings emerge:

Anonymizing infrastructure is now a routine component of attacks.

- **94%** of respondents say that security incidents involve anonymizing VPNs or residential proxies from sometimes to always.
- **Half** of companies report high-impact credential abuse incidents tied to anonymizing infrastructure.

Usage of IP intelligence is still immature.

- Most teams rely on it for **reactive investigation and blocking** rather than proactive decision-making.
- **Few** respondents indicate they have complete control over residential proxy use in their environments.
- **34%** do not measure the effectiveness of their IP intelligence efforts at all.

Context and automation will define the next generation of IP intelligence.

- **47%** say the biggest challenge with IP intelligence is lack of contextual information about the IP, with many citing the need for AI coverage.
- **84%** believe better IP intelligence would significantly reduce investigation time.
- **Half** of companies are planning to evaluate a new solution in the next 12 months.

These results suggest that the next evolution of IP intelligence will focus on action and decisioning, rather than simple enrichment.

Methodology

The survey was conducted between mid-February and early March 2026 and collected more than 200 responses from practitioners responsible for investigating, detecting, or mitigating IP-based threats across multiple industries, with the highest representation in the Information Technology (IT), Telecommunications, and Financial Services industries.

Participants represented a range of security roles including:

- Security operations
- Incident response
- Threat intelligence
- Threat hunting
- Fraud prevention
- Compliance

The survey included more than 20 questions covering topics such as:

- Threat exposure
- Operational workflows
- Technology usage
- Data sources
- Organizational impact
- Future investment plans

Respondents were asked to report both current practices and future priorities related to IP intelligence.

Key Terms

Before we dive into the study results, let's examine key anonymizing technologies and the role of IP enrichment in better understanding the context behind an IP address.

VPNs

VPNs (short for virtual private networks) use IPs from servers owned or rented by a VPN provider, typically located in data centers. Subscribers to VPN services can connect into any of these IP addresses and use them to hide their "true" IP address, and all traffic is attributed to that service.

Proxies

Proxies are intermediary services that forward requests to a destination on behalf of a user. Also used to mask a user's identity, they come in different flavors: traditional data center, residential, and mobile.

- **Data center proxies** originate from, and route traffic through, hosting providers and cloud networks such as AWS or Google.
- **Residential proxies** route traffic through an IP address sourced from a consumer ISP, typically from a home network.
- **Mobile proxies** route traffic through an actual smartphone, tablet, or SIM farm using a mobile data connection.

Although not every VPN or proxy connection is malicious in nature, security, threat hunting, and fraud teams continually strive to understand the intent behind every connection to prevent fraud and cybercrime.

IP Enrichment

IP enrichment is the practice of applying context to raw IP addresses to better understand network ownership, infrastructure, anonymization, geolocation, and risk signals. The product of enrichment is **IP intelligence.**

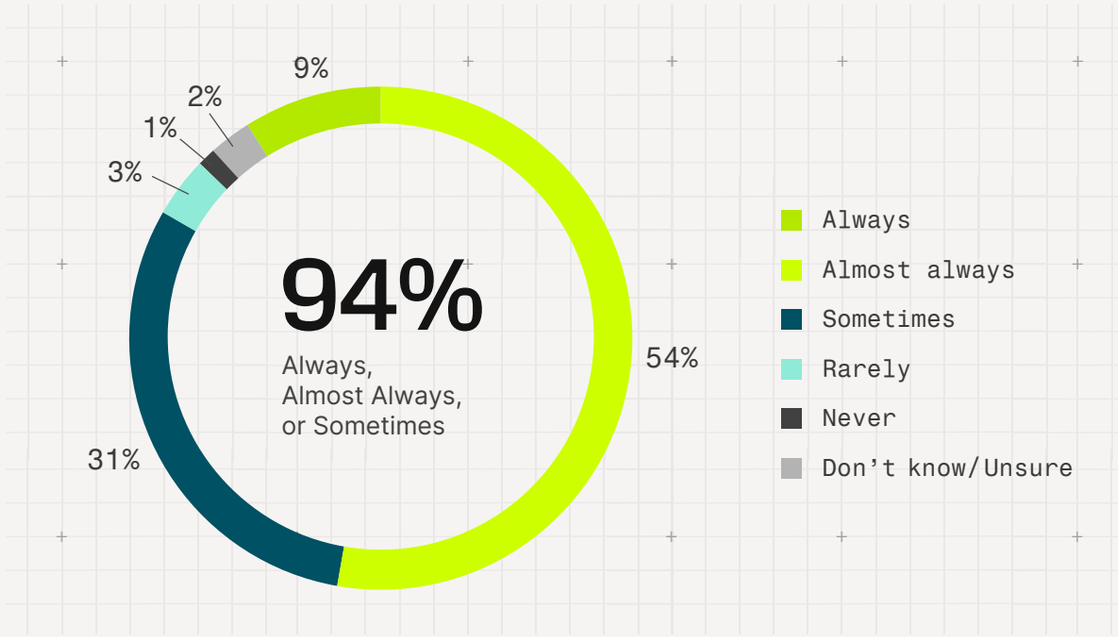
Finding 1

94% of organizations report that anonymizing infrastructure, such as VPNs and residential proxies, is used in security incidents.

Anonymizing infrastructure is a common feature of nearly all IP-related incidents. When asked how frequently anonymizing VPNs or residential proxies appear in relevant incidents, **63% or respondents said always or almost always** *(Chart 1)*.

Chart 1: Prevalence of anonymizing services in security incidents

How often is an anonymizing VPN or residential proxy service used in incidents affecting your organization?



Consumer VPNs Proton, Nord, Express, Surfshark, and Mullvad were the top 5 cited. Top-referenced residential proxy networks included OxyLabs, Bright Data, NetNut, and IPIDEA – each appearing frequently alongside consumer VPNs.

Yet, when you consider the risk of a VPN or residential proxy incident always or almost happening, **only 30% of respondents indicate that IP-related risks were well understood** before incidents occurred *(Chart 2)*, and only **32% are very confident** that all IP-based access paths into their organization are inventoried and monitored *(Chart 3)*.

Incidents are happening at a high rate. Many organizations saw the risks beforehand. Few are confident that access paths are monitored with enough fidelity. This is a recipe for a major incident if organizations don't take this more seriously.

Chart 2: Understanding of incidents from residential proxy abuse

Has your organization experienced an incident from residential proxy abuse? If so, which statement best applies?

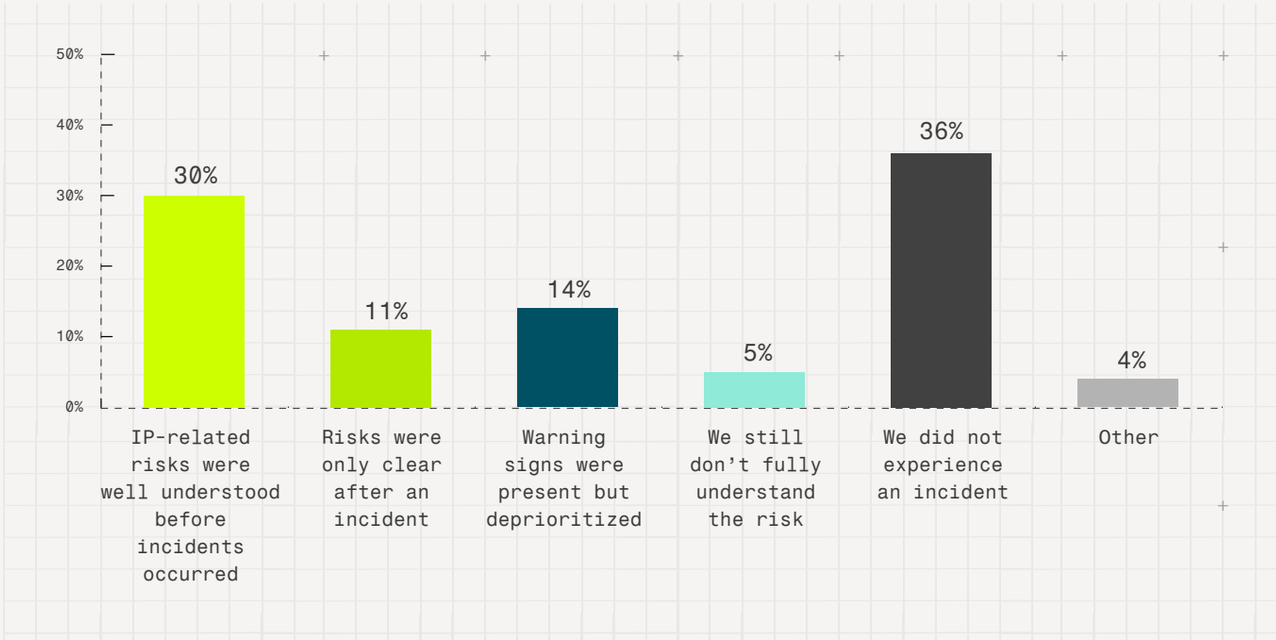
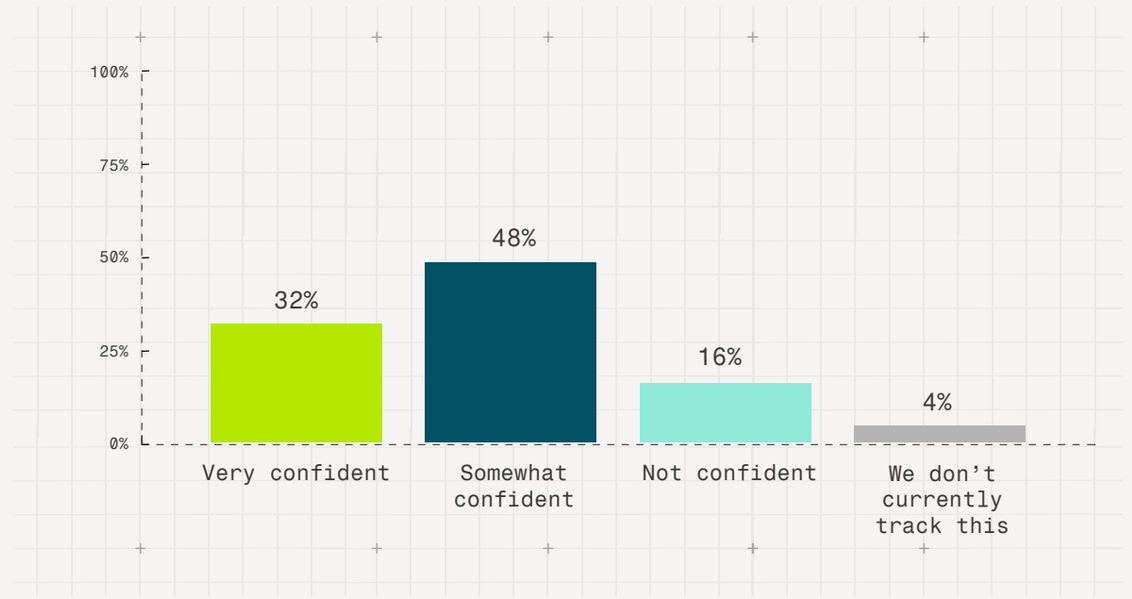


Chart 3: Confidence in control over IP-based access paths

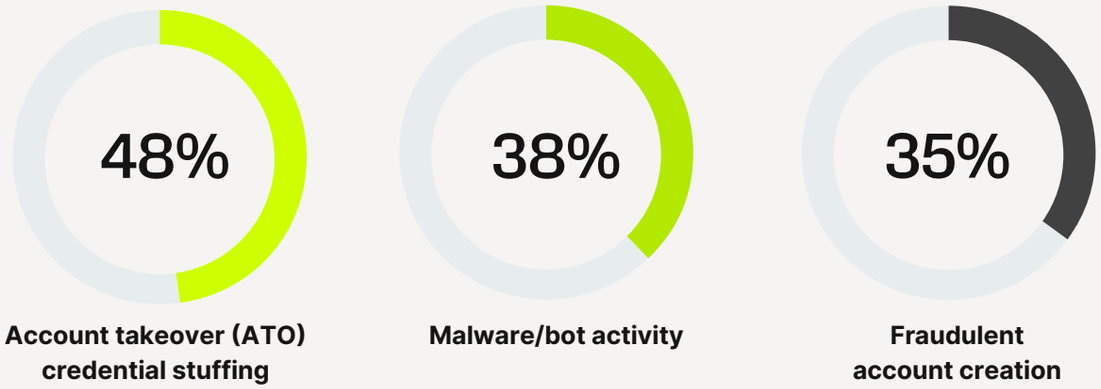
How confident are you that all IP-based access paths into your organization are inventoried and monitored?



Finding 2

Half of companies have reported significant operational or financial impact from credential abuse via VPNs and residential proxies.

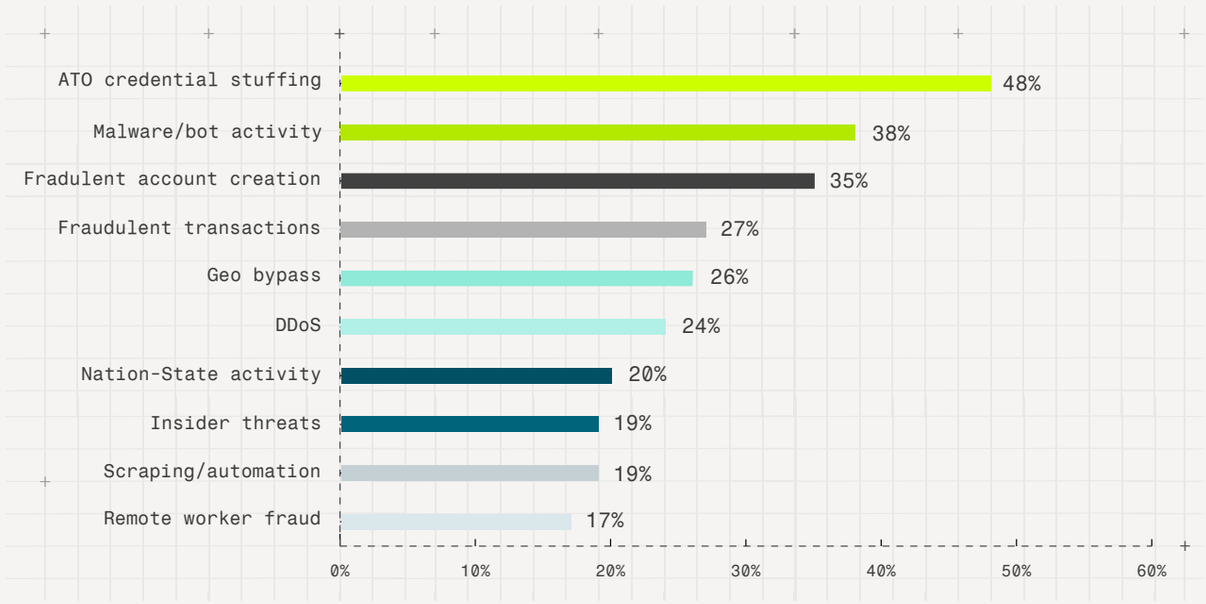
Respondents report encountering a wide range of IP-related threats over the past 12 months. The most commonly reported threat types include:



Among these threats, credential abuse had the highest rate of high-impact incidents, with **nearly half (48%) of respondents reporting significant operational or financial impact** *(Chart 4)*. This suggests that IP intelligence is closely tied to account security and bot mitigation, not just traditional network abuse.

Chart 4: High-impact threats

Which of the following IP-based threats have had a high impact on your organization in the last year?



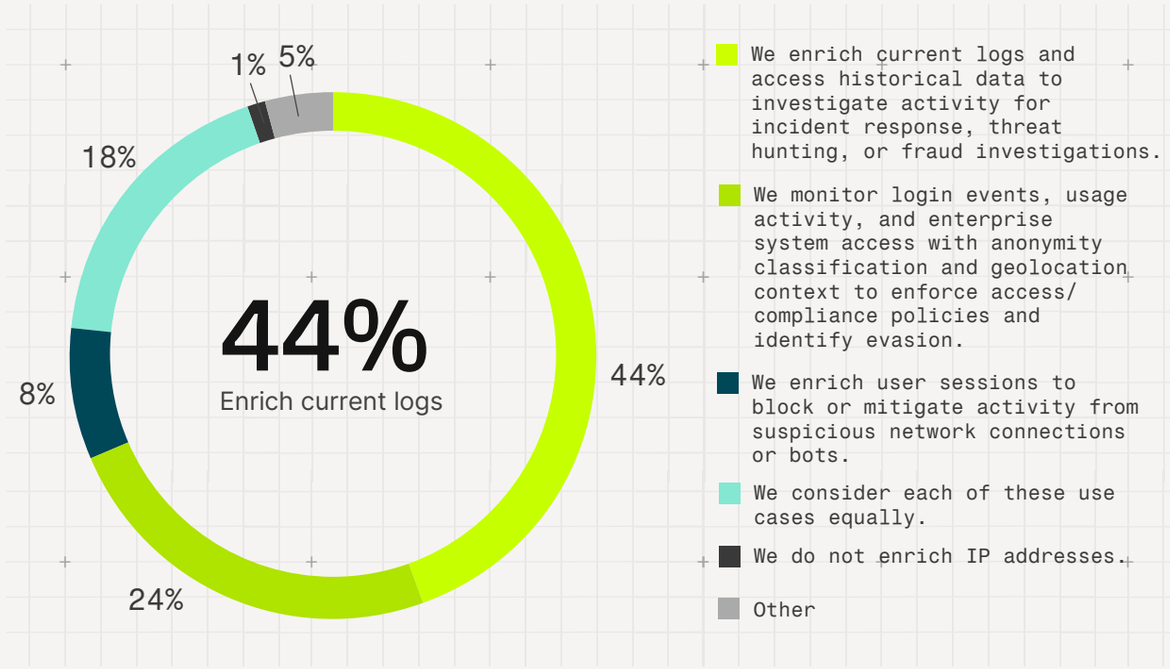
Finding 3

Despite knowing the risks of anonymous activity, most organizations only use IP intelligence for investigation and blocking rather than proactive decisions – but they want more.

Most organizations still rely on IP intelligence primarily for reactive investigative workflows. The most common primary use case is **enriching logs and analyzing historical data during investigations at 44%** *(Chart 5)*.

Chart 5: Primary IP intelligence use cases

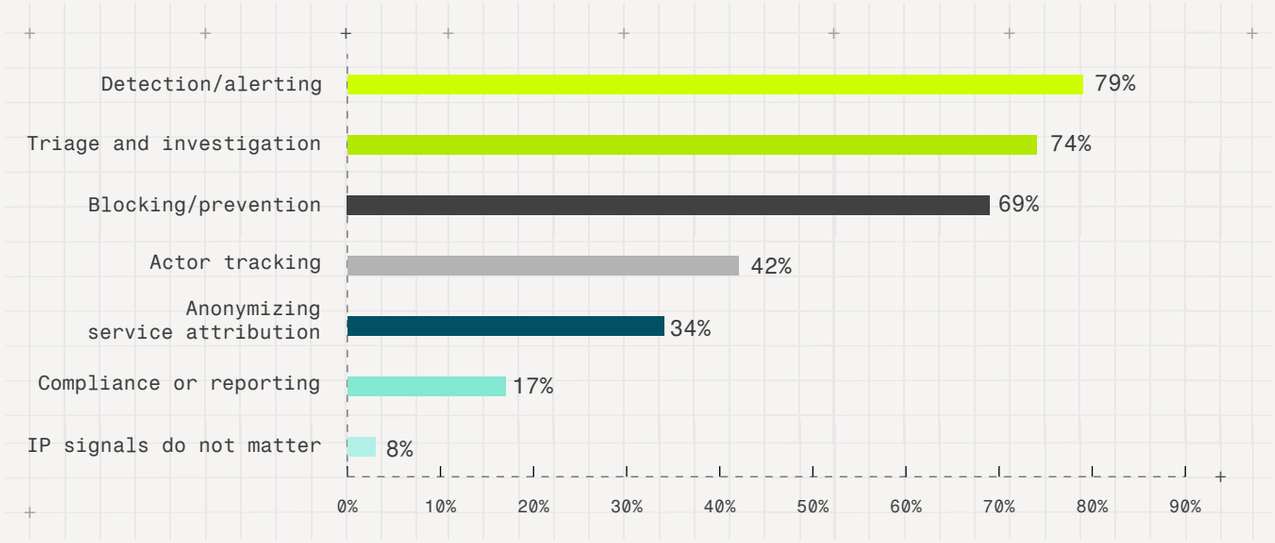
Which statement below would you consider to be your primary use case for enriching IPs?



Operational use cases reinforce this pattern, with **79% of respondents utilizing IP intelligence for detection and alerting, 74% for incident investigation, and 69% for blocking or prevention** *(Chart 6)*.

Chart 6: Operational use cases for IP intelligence

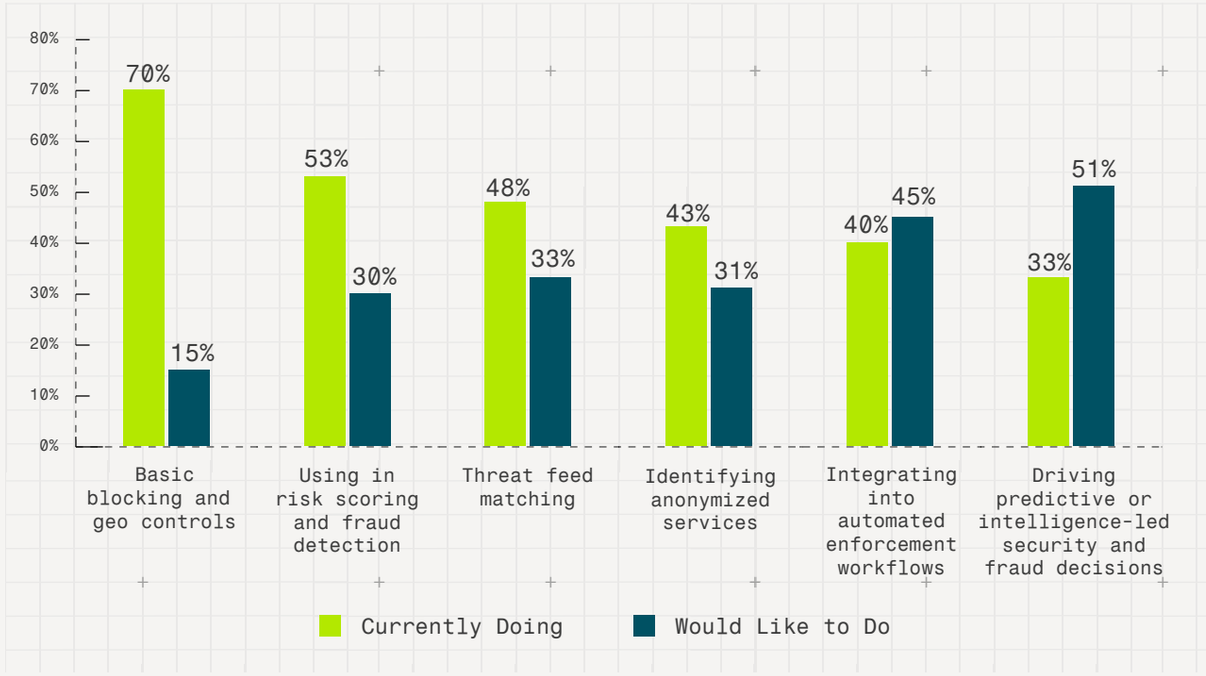
In what contexts do IP signals matter most?



Respondents express strong interest in expanding their IP intelligence capabilities. Half of respondents want IP intelligence to support predictive decision-making or automated enforcement workflows *(Chart 7)*.

Chart 7: Current vs. desired IP intelligence capabilities

How are you operationalizing IP intelligence data today? What do you wish you could do with IP intelligence that you can't do today?



Finding 4

Many organizations lack visibility and control over proxy usage on employee devices representing a massive security vulnerability.

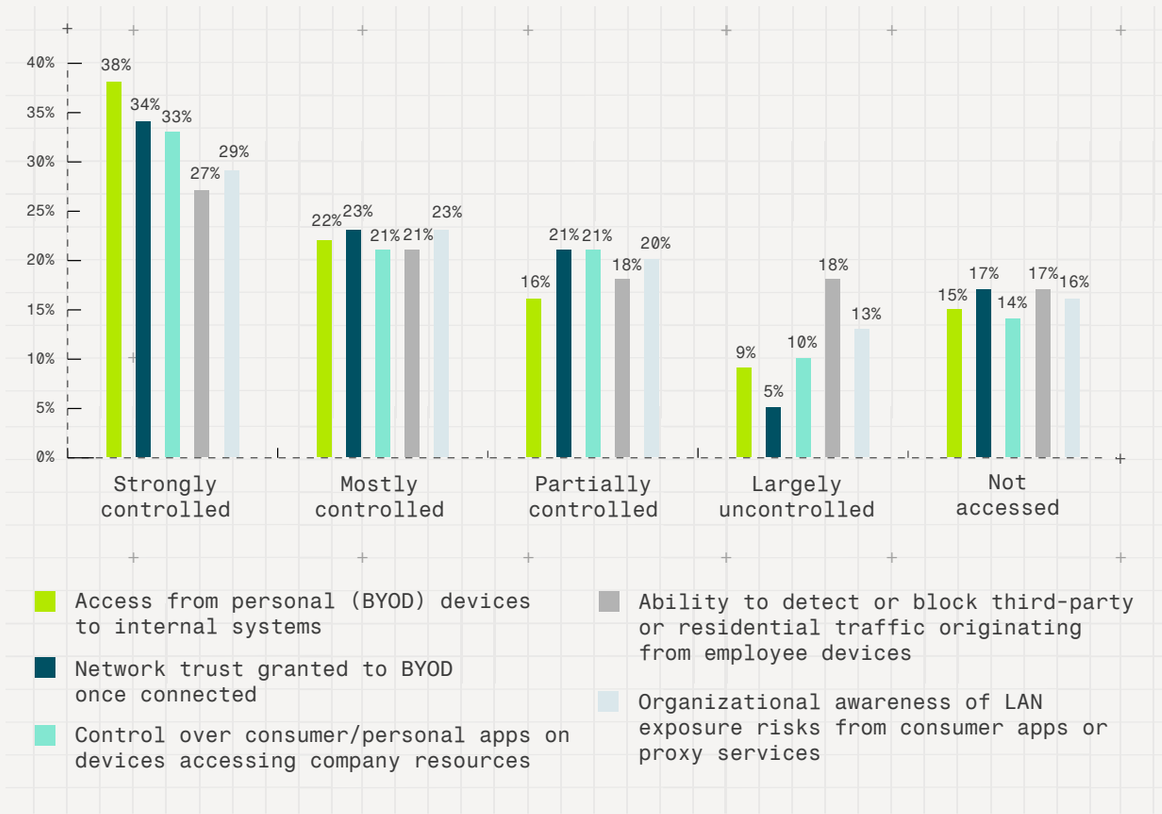
Survey results reveal a gap between the prevalence of anonymizing infrastructure in incidents and organizations' ability to detect or control it internally.

A surprisingly low **38% of respondents indicated that access from personal (BYOD) devices to internal systems is strongly controlled,** while **23% said network trust granted to BYOD once connected was only mostly controlled**.

Between **14-17% of companies aren't even assessing** these areas *(Chart 8)*.

Chart 8: Current security posture over employee devices

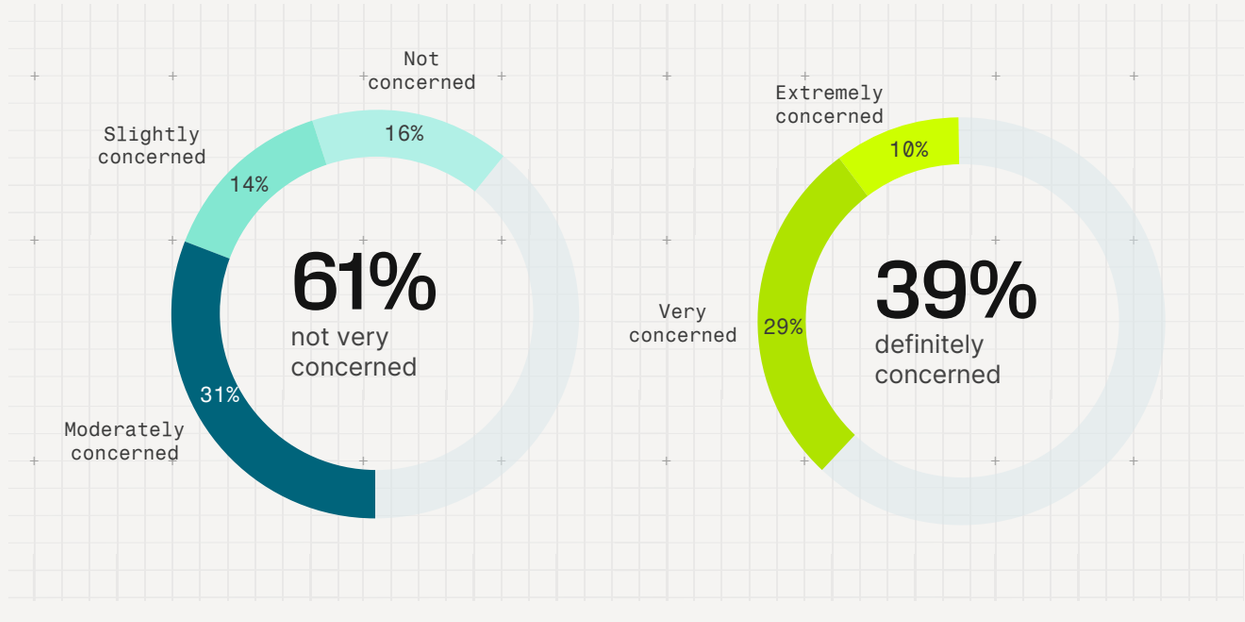
Which of the following best describes your organization's current posture across these areas?



In fact, a shocking **61% of respondents report being moderately, slightly, or not at all concerned about the potential exposure of their internal network via residential proxies** on employee devices or consumer apps *(Chart 9)*. Considering recent vulnerabilities associated with LAN access by residential proxies, organizations have a long way to go to improve their awareness of this risk.

Chart 9: Concerns over LAN access by residential proxies

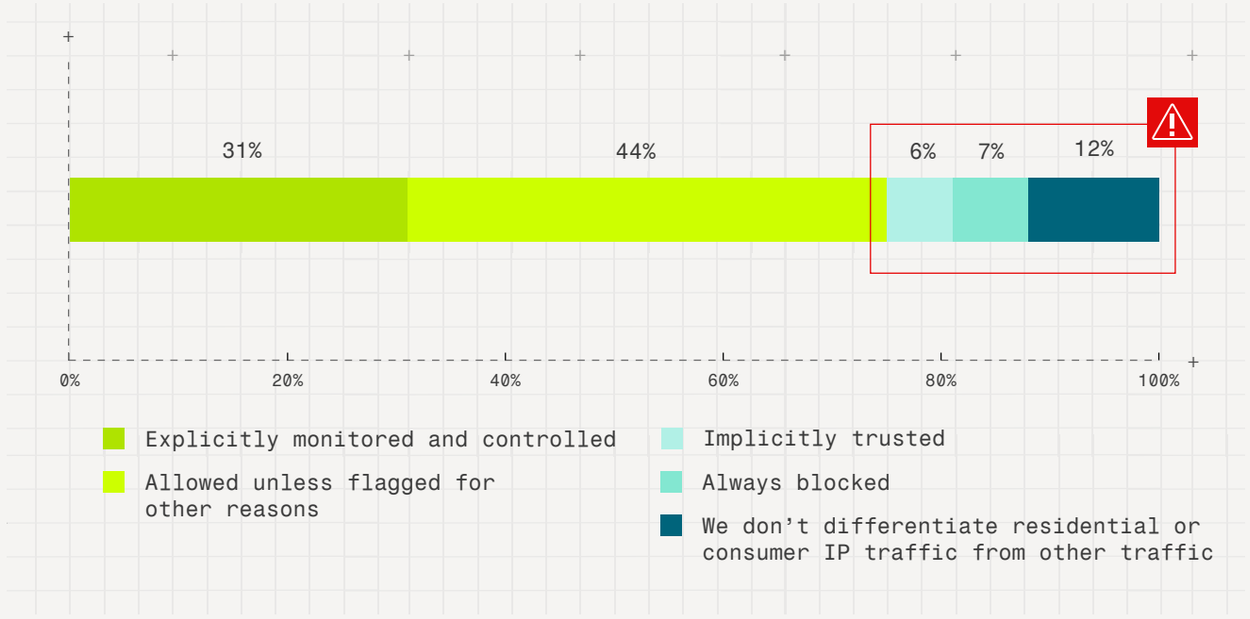
How concerned are you about the potential exposure of your internal network via residential proxies on employee devices or consumer applications?



About a fourth of respondents treat residential or consumer IP traffic with either too little control (6% implicitly trusted, 12% don't differentiate at all) or too much control (7% always blocked) *(Chart 10)*. **Too little control opens organizations up to IP-based threats, and too much control has a negative effect on user experience from overblocking and too much friction.**

Chart 10: Treatment of residential or consumer IP traffic in your organization

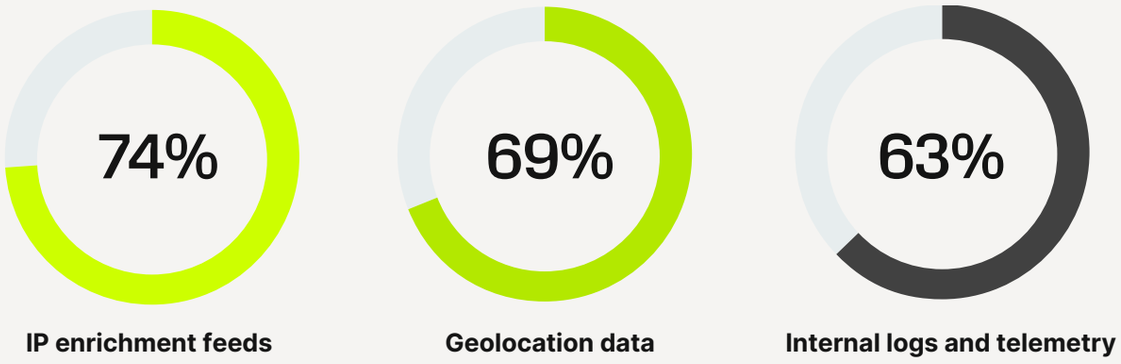
Which of the following best describes how residential or consumer IP traffic is treated in your environment?



Finding 5

IP intelligence workflows remain fragmented across tools and data sources.

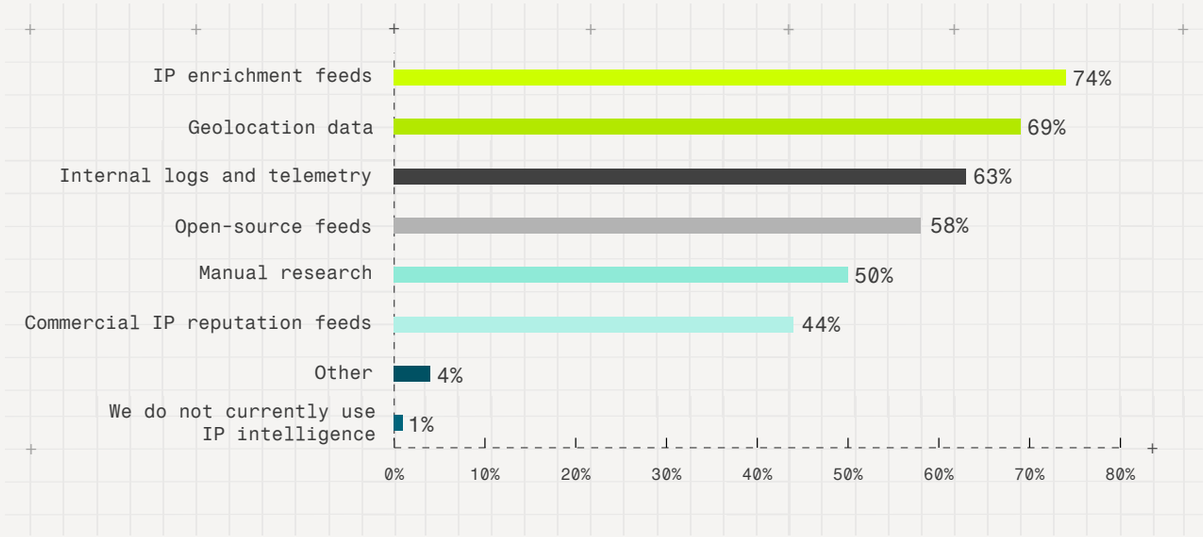
Organizations rely on a combination of external data sources and internal telemetry to analyze IP activity *(Chart 11)*. The most commonly used data sources include:



Nearly half still rely on a combination of tools and manual research. Although some manual research may always be required, tooling should help correlate findings, aid in investigations, and reduce investigation times. Interestingly, commercial IP reputation feeds are the least-used tool type.

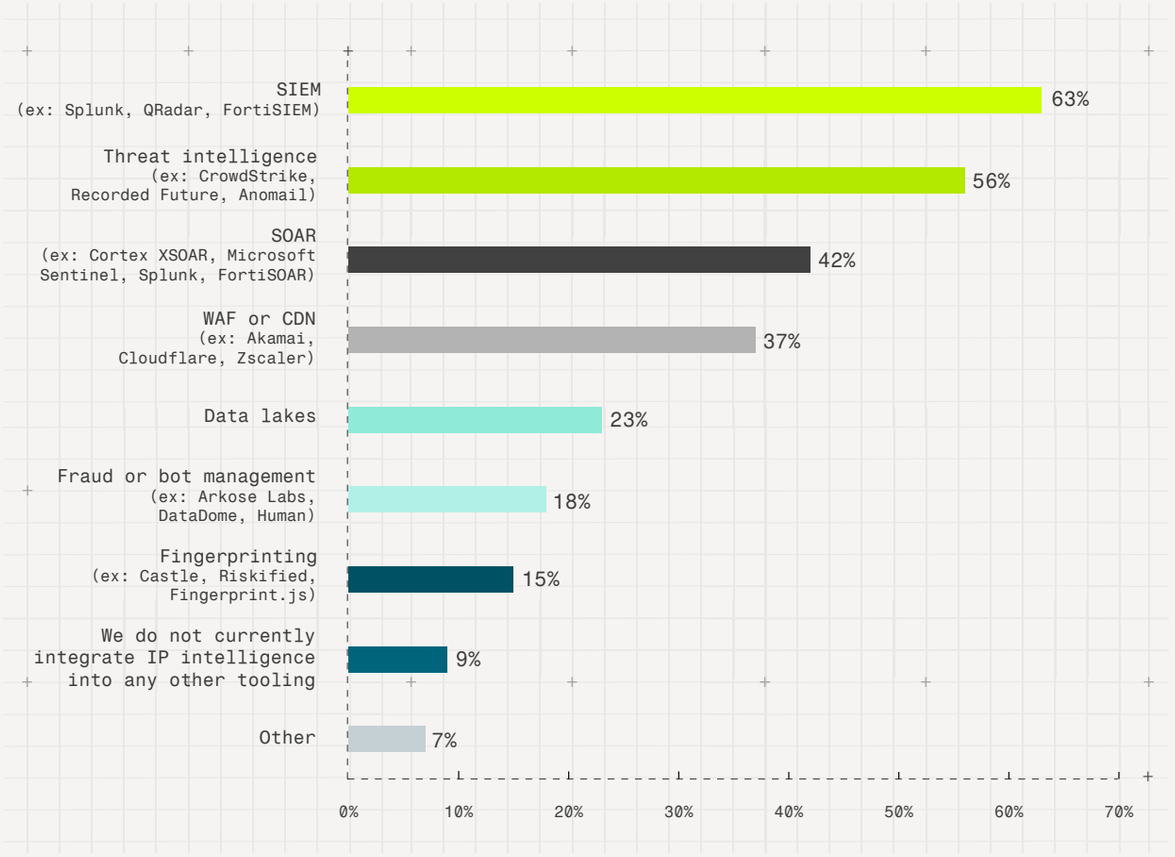
Chart 11: IP intelligence tooling

What tools or data sources do you currently use to gather IP intelligence?



Unsurprisingly, respondents are integrating their IP intelligence predominantly into their **SIEM (63%)**, followed by **threat intelligence platforms (56%)** and **SOAR (42%)** *(Chart 12)*.

Chart 12: Integration points for IP intelligence



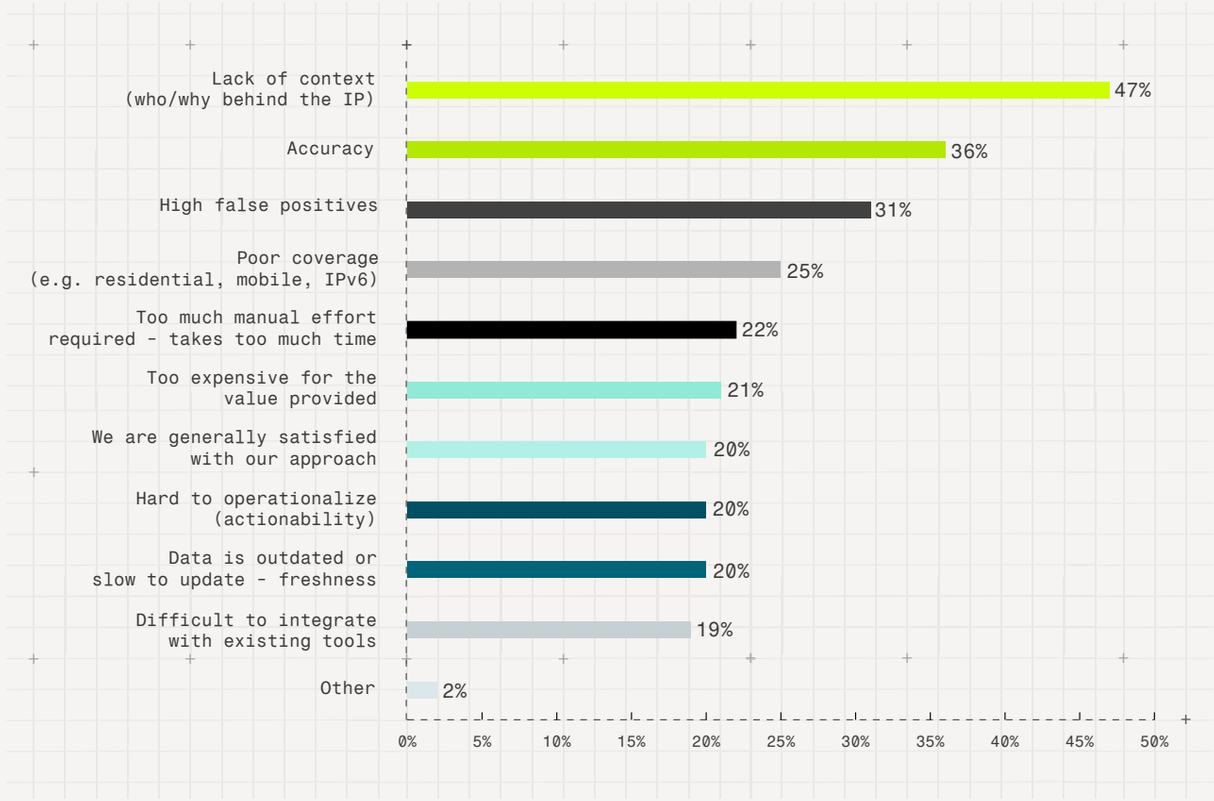
Finding 6

Lack of context is the biggest challenge for security teams analyzing IP activity.

The most frequently cited challenge with IP intelligence is the **lack of contextual information** – the who and why behind the IP address itself – **at 47%**, followed by **data accuracy issues (36%)**, and a **high rate of false positives (31%)** *(Chart 13)*.

Chart 13: Biggest challenges with current IP approach

What are the biggest challenges with your current IP intelligence approach?



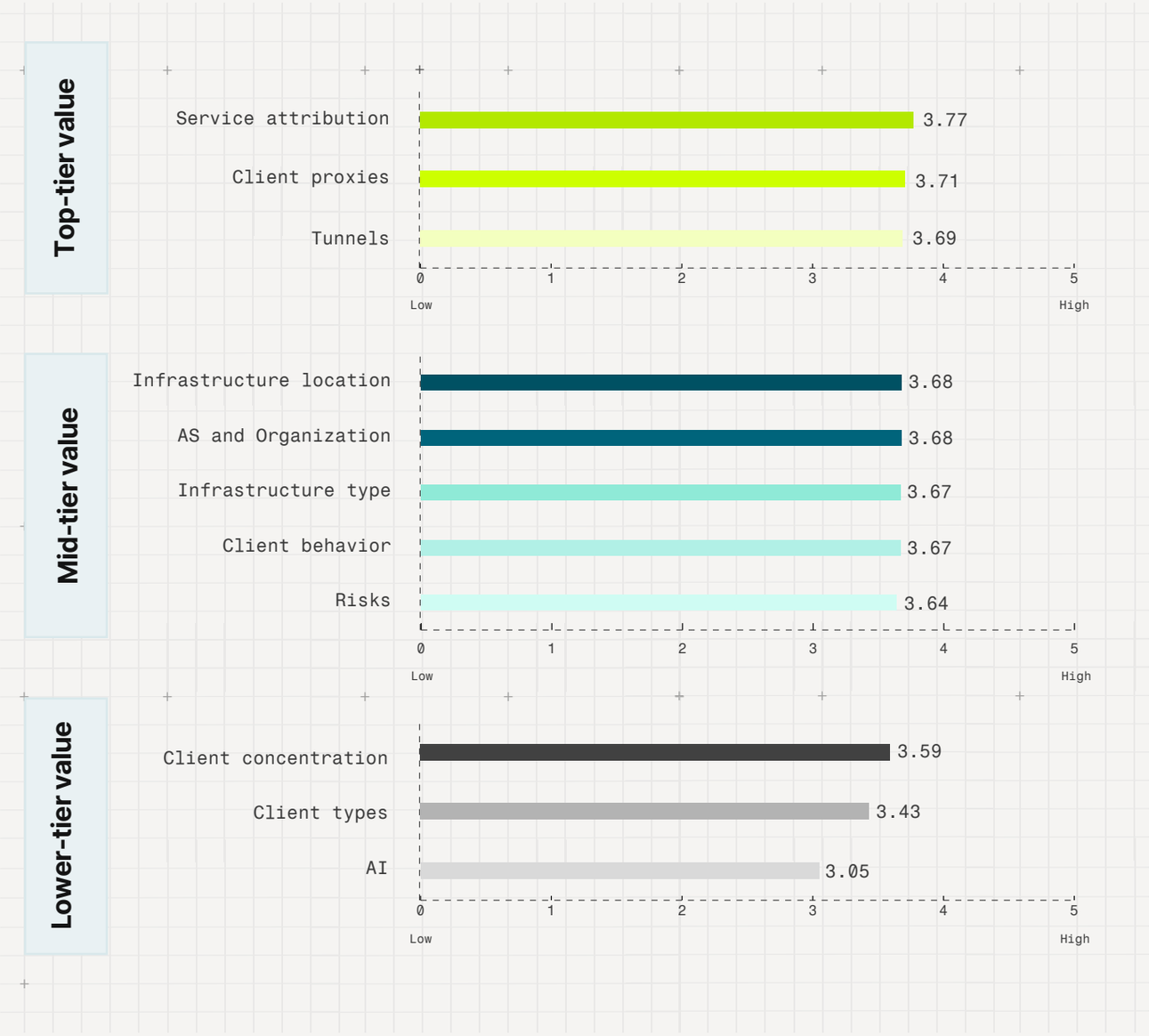
With these concerns, satisfaction with existing IP intelligence sources is therefore varied. When asked to rate their value on a scale of 0 (low) to 5 (high) respondents rated signals this way *(Chart 14)*:

- **Top-tier signals (3.7+)**, including service attribution, client proxies, and tunnels. These are directly actionable infrastructure signals. They tie closely to detection and decision-making.
- **Strong but slightly less differentiated (3.64–3.68)**, including infrastructure and behavioral context (e.g., location, ASN, behavior, and risks). These attributes are valuable but often supporting signals, not primary decision drivers.
- **Lower perceived value areas**, including client types and concentration.

Interestingly, AI is the outlier with the lowest score at 3.05, but 46% of companies don't get this data at all. **With the increase in AI and automation-related traffic, and AI use of residential proxies, this is a gap that must be closed quickly.**

Chart 14: Value received from existing IP intelligence sources by area

Please rate the value you are currently getting from existing IP intelligence sources in these areas.



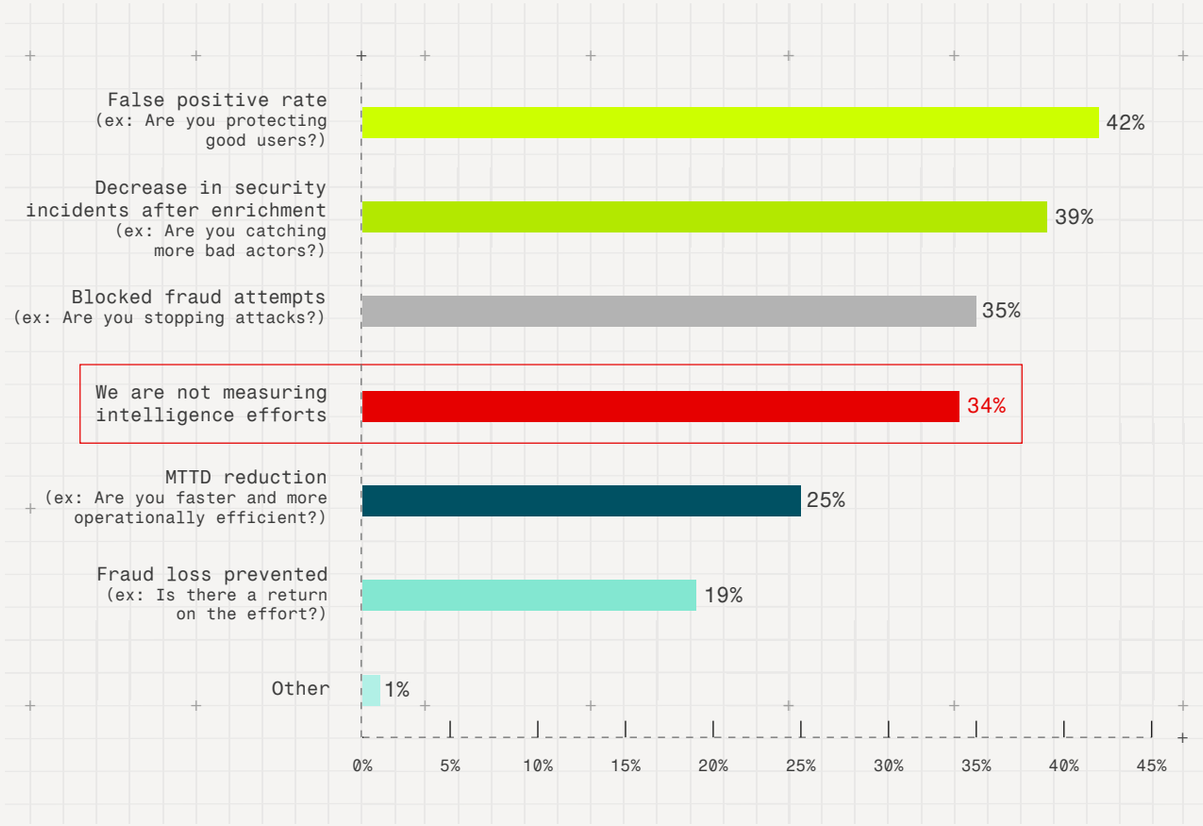
Finding 7

Many organizations do not measure the effectiveness of their IP intelligence programs but acknowledge that the biggest operational impact of poor IP intelligence is slower investigations.

Despite widespread adoption in some form or another, many organizations do not formally measure the performance of their IP intelligence programs. When they do measure the effectiveness of their programs, the most common metrics include false positive rate (42%), followed by decrease in security incidents after enrichment (39%). **Interestingly, more than a third of respondents (34%) are not measuring their IP intelligence efforts at all** *(Chart 15)*.

Chart 15: KPIs used to measure IP intelligence effectiveness

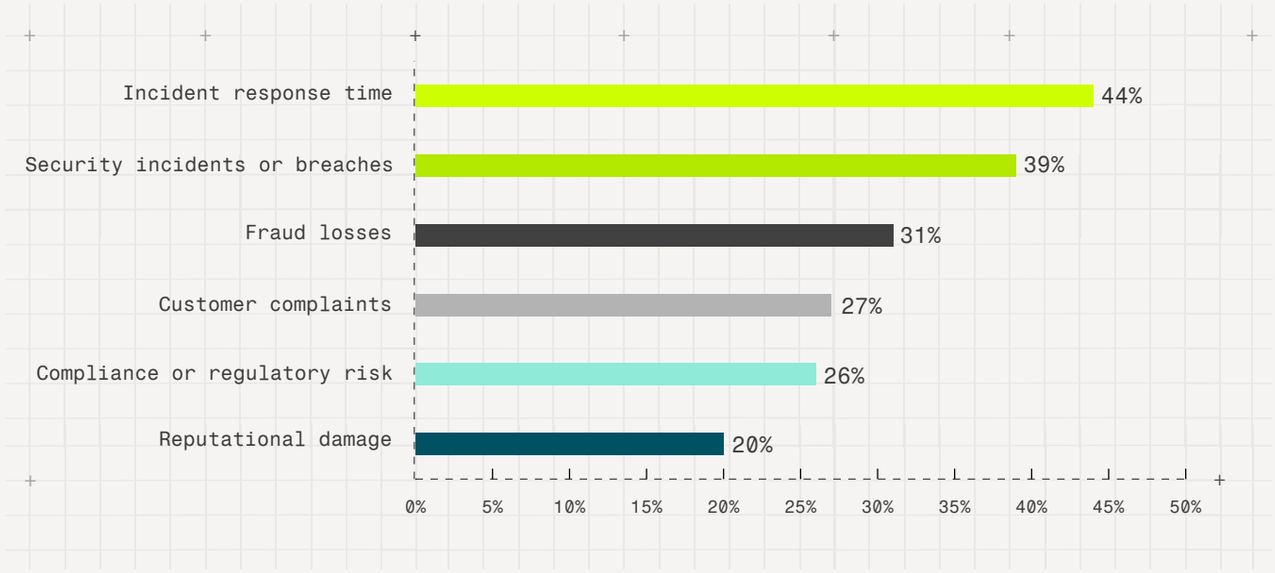
What key performance indicators (KPIs) is your organization using to measure the effectiveness of current IP intelligence efforts?



The use of ineffective, low fidelity IP intelligence has resulted in an increase or significant increase across all major risk factors, including an especially high **44% increase in incident response times** *(Chart 16)*.

Chart 16: Impact of ineffective IP intelligence

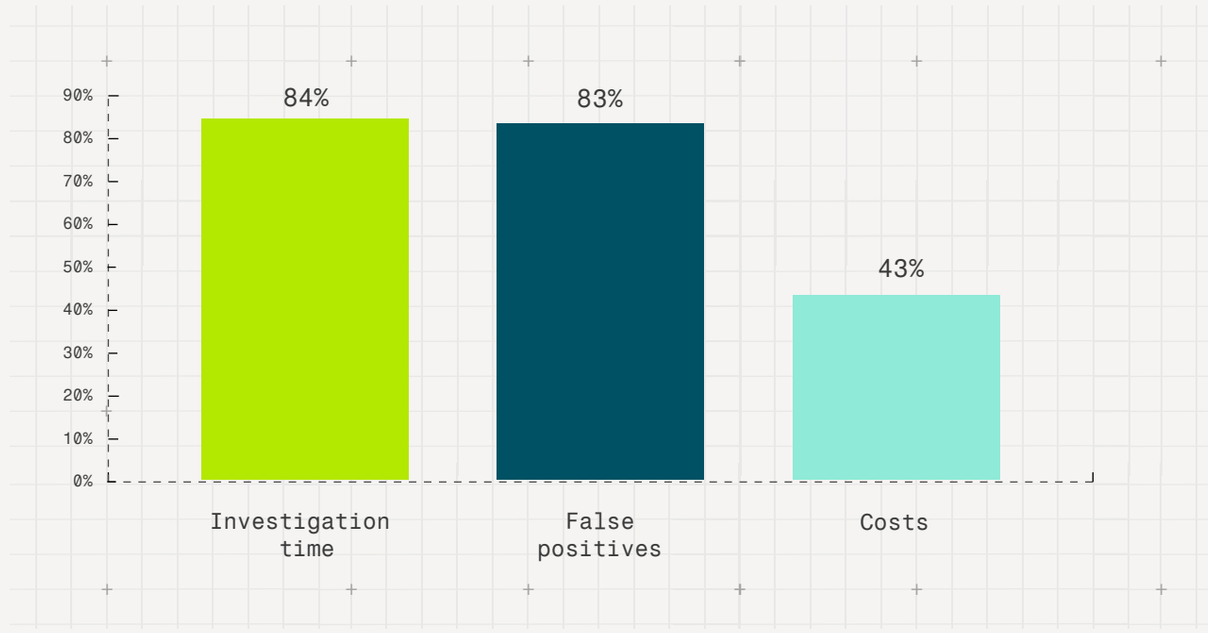
Which risk factors have increased because of ineffective IP intelligence in the last year?



When asked where improved IP intelligence would deliver the most value, respondents believe overwhelmingly that **improved IP intelligence would decrease or significantly decrease investigation time (84%) and false positives (83%)** *(Chart 17)*.

Chart 17: Operational impact of improved IP intelligence

How has or would improved IP intelligence most benefit your team?



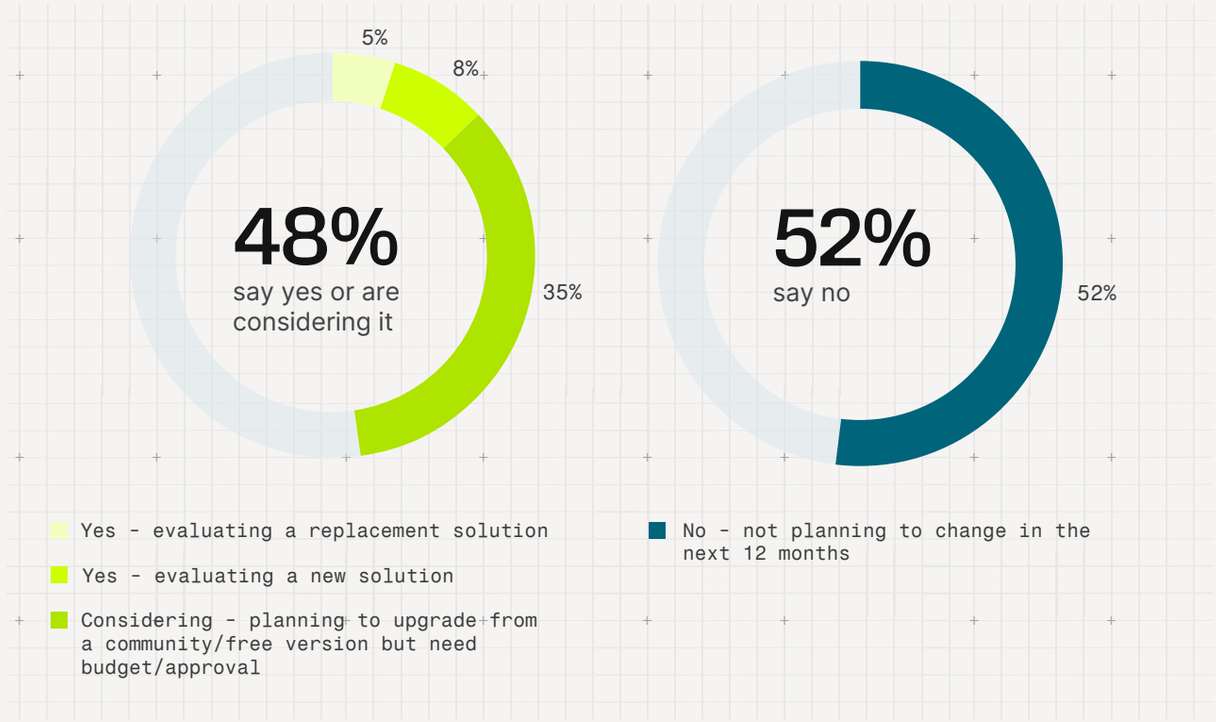
Finding 8

Budget constraints slow adoption, but many organizations expect change within 12 months.

Considering relatively high rates of dissatisfaction with current tooling and sources, it's not surprising that nearly **half of buyers (48%) are looking to upgrade their IP intelligence solution in the next 12 months** *(Chart 18)*.

Chart 18: Adoption plans for IP intelligence tools

Are you planning to implement, upgrade, or purchase a commercial IP intelligence solution in the next 12 months?



However, the biggest barrier to adopting a new IP intelligence solution is **budget (51%)** followed by a **lack of resources (33%)** *(Chart 19)*. Organizations must seek strong business cases and ROI metrics.

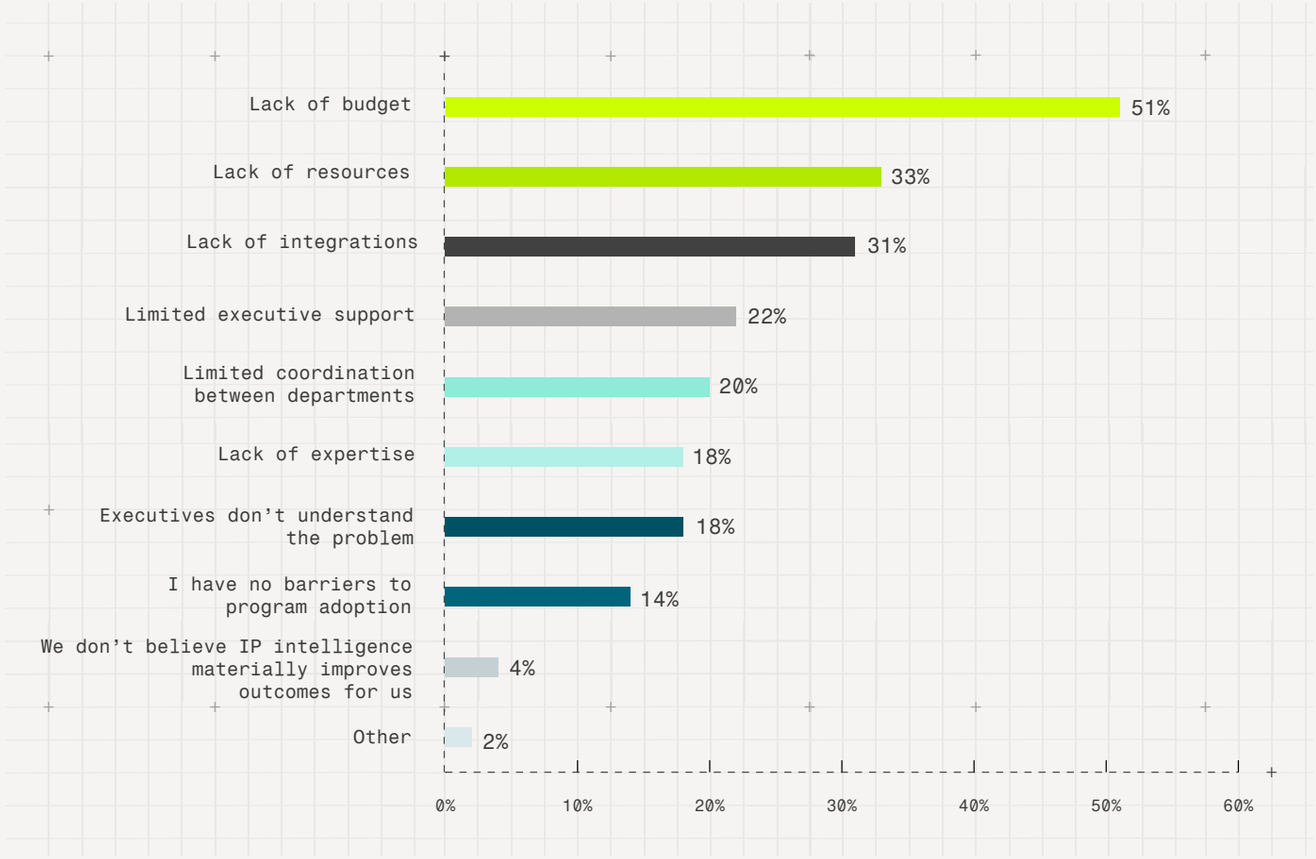
Based on the survey findings, organizations are demanding:

- **Improved contextual visibility into IP activity.** Teams need better attribution signals to understand who is behind suspicious infrastructure.
- **Expanded automation and proactive enforcement.** IP intelligence should inform security decisions earlier in the detection pipeline.
- **Strengthened internal network visibility.** Organizations must address blind spots related to proxy usage and employee device access.

How do organizations make this happen? Move from reactive enrichment to proactive, intelligence-driven decision making.

Chart 19: Barriers to adoption

What are the barriers to adopting or growing your IP intelligence program?



Best-Practice Recommendations for Security Teams to Advance Their IP Intelligence Programs

The results of this study suggest that organizations are entering a new phase in how IP intelligence is used across security operations. The organizations that treat IP intelligence as a strategic capability rather than a simple enrichment tool will be best positioned to reduce investigation workload, improve detection accuracy, and respond more effectively to emerging threats. Here's how to make that happen:

01

Move beyond reactive enrichment toward proactive decisioning

Most respondents currently use IP intelligence primarily for investigation and alert triage, rather than proactive controls. Organizations should expand IP intelligence into real-time security decisioning, where IP signals influence authentication, access control, and fraud prevention workflows. Use IP intelligence as an input into risk-based authentication, fraud detection models, and adaptive access policies.

Moving IP intelligence earlier in the detection pipeline can significantly reduce investigation workload.

02

Build detection strategies for anonymizing infrastructure

The study shows that 63% of respondents encounter VPNs or residential proxies in most incidents, making anonymizing infrastructure a routine feature of modern attacks. Security teams should monitor for traffic originating from commercial residential proxy networks, consumer VPN providers, and Tor exit nodes, and implement controls that evaluate behavior rather than relying solely on IP reputation. Use signals such as session anomalies, geographic inconsistencies, and rapid IP rotation patterns.

Security programs should focus on behavioral detection rather than static blocklists when dealing with anonymizing infrastructure.

03

Address internal exposure from proxy-enabled employee devices

The research indicates that many organizations have limited visibility into proxy traffic originating from employee devices, particularly in BYOD or remote work environments. Organizations should treat internal proxy usage and residential network exposure as potential attack surfaces.

- Implement monitoring for outbound proxy or VPN usage from employee devices.
- Restrict or monitor consumer proxy services on corporate-managed devices.
- Apply network segmentation to limit access granted to unmanaged or personal devices.
- Incorporate IP intelligence signals into zero-trust access policies.

Improving internal visibility can reduce the risk of attackers exploiting trusted internal network access.

04

Prioritize contextual enrichment over raw IP data

Nearly half of respondents report that the biggest challenge with IP intelligence is the lack of contextual information about the IP address. Organizations should prioritize enrichment sources that provide behavioral and attribution context, rather than relying solely on reputation or geolocation.

Look for intelligence sources that provide:

- Infrastructure classification (hosting vs. residential)
- Proxy and VPN detection
- Behavioral indicators
- Historical activity patterns
- Known associations with botnets or campaigns

Contextual signals enable analysts to understand who is likely behind an IP address and why it is behaving suspiciously.

05

Establish measurable KPIs for IP intelligence programs

More than one-third of respondents report that they do not measure the effectiveness of their IP intelligence efforts. Without measurement, organizations may struggle to justify investment or optimize workflows.

The strongest perceived benefits of improved IP intelligence were reduced investigation time and fewer false positives. Organizations should prioritize investments that improve analyst efficiency, rather than focusing solely on threat blocking.

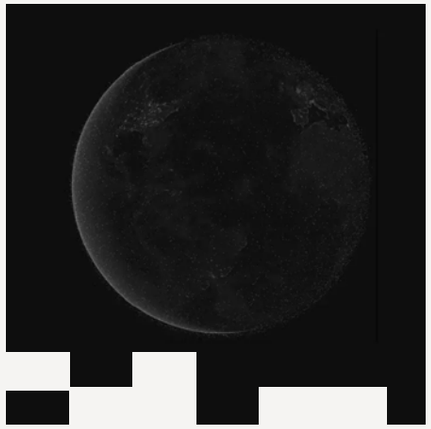
Track metrics such as:

- Investigation time per alert
- False positive rates
- Blocked fraud attempts
- Incident response time
- Automated vs. manual investigation rates

These metrics help security leaders demonstrate operational improvements driven by IP intelligence capabilities.

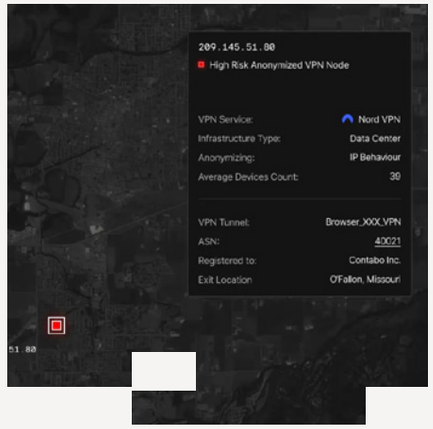
About Spur

Spur reduces the risk presented by anonymizing VPNs and residential proxies by delivering high-fidelity IP intelligence at scale that enables precise infrastructure attribution and real-time, risk-based decisions. With Spur, you can centrally:



Observe

Continuously observe global network traffic, anonymization infrastructure, and routing behavior across hundreds of millions of IP addresses and more than 1,000 VPN and proxy services.



Enrich

Analyze and classify each IP using 20+ technical attributes spanning geography, ASN, tunnel metadata, and behavioral signals.

Act

Distribute intelligence through flexible delivery options – API, on-prem data feeds, and edge session enrichment – and integrations into common security, fraud, and authentication tooling, ensuring the same fidelity and explainability everywhere.

To start a free trial and experience our high-fidelity IP intelligence in action, visit spur.us.