World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

The cost of fragmentation: Measuring time, spend and risk in personal cybersecurity tool stacks

Ifrah Arif [1,*], Anas Tariq [1] and Bogdan Barchuk [2]

[1] *Pure Square, Office 2001, Nassima Tower, Trade Center 1st, SZR, Dubai, UAE.*
[2] *CQR Cybersecurity LLC, San Francisco, California, USA.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 16(03), 334-363

Publication history: Received on 11 August 2025; revised on 14 September 2025; accepted on 18 September 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.16.3.1350

Abstract

This study investigates the underexplored hidden costs of cybersecurity tool fragmentation at the individual user level. While prior research focuses on enterprise environments, the proliferation of personal security applications—such as antivirus, VPNs, and password managers—creates significant burdens for consumers who lack dedicated IT support. To quantify this, we conducted original primary research through a quantitative survey (n=50) of individual users and supplementary qualitative interviews. Our findings reveal that users manage an average of 3.4 tools, incurring a substantial "time tax" of 2.3 hours per month on maintenance. Furthermore, 44% face overlapping alerts, 38% sometimes ignore notifications, and 29-34% leave tools disabled or miss paid features, leading to redundant spending averaging 24% of an annual USD 92 tool cost. When valued at USD 20-30/hour, the total per-user burden is estimated at USD 574-850 annually. We conclude that tool fragmentation directly drives operational inefficiency, financial waste, and increased security risk for individuals, underscoring the critical need for consolidated, user-centric solutions and providing a model for evaluating personal cybersecurity return on investment.

Keywords: Cybersecurity; Cybersecurity Tools; Cybersecurity Tool Fragmentation; Online Security; Individual Cybersecurity; Alert Fatigue

1. Introduction

In everyday personal security, individual users assemble their own "stack" of apps—such as antivirus software, VPNs, password managers, and browser extensions—often from different vendors. Fragmentation at this level results in increased logins and consoles, overlapping features and alerts, and uneven configuration across devices. Without a SOC (Security Operations Center), time and attention costs are borne directly by the user, turning security into a recurring "time tax" and, in many cases, a source of risky inaction.

This study, therefore, focuses on individual users, quantifying personal tool sprawl, duplicated notifications, cognitive load, and out-of-pocket costs. We further estimate per-user monetary/operational impact of fragmentation across three verticals: access, alerts, and functionality.

1.1. Scope of the Problem

While much of the existing research focuses on enterprise environments, fragmentation also directly affects individual users. Home networks, personal devices, and remote work setups expose end-users to similar inefficiencies, redundant tools, and alert fatigue. These impacts are compounded by varying levels of technical proficiency and heterogeneous device ecosystems, making individual-level analysis essential.

* Corresponding author: Ifrah Arif

Industry surveys highlight how this problem has emerged in enterprise security operations. Reports indicate that security teams are increasingly relying on dozens of separate tools, often sourced from multiple vendors, to address evolving threats [1]. This tool proliferation illustrates how complexity itself becomes a risk factor. However, the issue is not confined to enterprises. Individual users face a parallel challenge: assembling their own patchwork of protective technologies such as VPNs, antivirus software, password managers, and identity-monitoring services. Unlike enterprises, individuals rarely benefit from centralized dashboards, automation, or expert staff. Instead, they must manage overlapping interfaces and redundant alerts independently, often with limited technical support.

Consequently, tool fragmentation—whether in organizations or at the individual level—creates inefficiencies, increases cognitive burden, and may even reduce overall security effectiveness. This study, therefore, shifts attention from the enterprise lens toward the underexplored domain of individual-user security tool management.

1.2. Research Objective

This study aims to validate the hypothesis that tool fragmentation incurs hidden costs across three key dimensions—access, alerts, and functionality. Prior anecdotal evidence and theoretical arguments suggest: (1) Fragmented access to many disparate tools causes friction and slows response (we term this inertia), (2) Fragmented and uncoordinated alerts from multiple systems lead to alert fatigue and lack of action, and (3) Fragmented functionality (siloed or overlapping capabilities) results in security gaps and blind spots. We seek to substantiate these hypotheses with quantitative data (e.g., frequency of tool usage, percentage of ignored alerts, incident rates), behavioral analysis (e.g., how humans respond to fragmented workflows, cognitive overload, fatigue), and monetary impact estimates (e.g., cost of breaches linked to these issues, wasted spending on unused tools, productivity loss in dollar terms).

1.3. Significance

For individual users, fragmentation converts directly into time tax, cognitive overload, and wasted out-of-pocket spend—without dedicated IT support. Quantifying these per-user monetary and operational impacts clarifies that consolidated choices (minimal stacks, integrated suites) deliver a better personal return on investment and reduce the risk of unsafe inaction.

1.4. Structure

The remainder of the paper is organized as follows. The Literature Review (Section 2) examines existing research and reports on security tool complexity, alert management, and integration challenges. The Methodology (Section 3) outlines how data were gathered from secondary sources and the criteria for inclusion. The Results (Section 4) are presented in three sub-sections corresponding to the verticals of fragmented access, alerts, and functionality, each detailing evidence of the problem's scope, behavioral implications, and cost impact. A Discussion (Section 5) then synthesizes these findings, exploring interrelationships between the verticals and potential mitigation strategies (such as tool consolidation, automation, and process changes). The paper concludes with a Conclusion (Section 6) that summarizes key insights and recommends future work.

2. Literature Review

The majority of prior research on cybersecurity tool fragmentation has centered on enterprise environments. Industry surveys and academic studies consistently document issues such as tool sprawl, alert overload, and functional silos. However, there is limited empirical evidence quantifying these dynamics at the level of individual users. This section reviews the enterprise-focused literature as a benchmark, highlighting key themes and gaps. Our primary research addresses the underexplored dimension of end-user impacts.

2.1. Tool Sprawl and Complexity

The phenomenon of "tool sprawl" in cybersecurity is well-documented in industry literature. Organizations have continually added new security products over time—such as endpoint protections, network monitors, cloud security tools, identity management systems, and threat intelligence feeds—often in response to new threats or compliance demands. Cisco describes this accumulation as tools "stacking up" one by one until teams are juggling dozens of siloed solutions [2].

Surveys support this pattern: Cisco's 2019 CISO Benchmark study reported that 37% of organizations used more than 10 security vendors [1]. A 2020 IBM-Ponemon survey indicated that companies averaged 45 security tools, with those deploying more than 50 tools reporting lower confidence in their ability to detect and respond to incidents [3].

Researchers and practitioners have highlighted the challenges of integration. Tools that do not share data or alerts force analysts to manually correlate information across systems. This constant context-switching imposes cognitive costs, delaying response times. Productivity studies outside security suggest that each task switch can take over 20 minutes to recover from, implying measurable operational inefficiencies [4]. In a cybersecurity context, such delays can translate directly into slower threat response and higher risk of oversight.

Taken together, the literature indicates that while adding tools may increase coverage, it also introduces diminishing returns and, at scale, negative impacts on visibility, analyst efficiency, and security posture. However, these findings are almost entirely enterprise-centric. Quantitative evidence for comparable dynamics at the level of individual users remains limited and is addressed later in this paper (Section 4).

2.2. Alert Overload and Analyst Fatigue

Another well-established enterprise challenge is alert overload. Modern detection systems such as IDS/IPS, SIEM, and EDR can generate thousands of alerts daily. Vectra AI (2023) reported that SOC teams receive approximately 4,484 alerts per day, of which nearly two-thirds are ignored due to overwhelming volume and false positives [5]. Similarly, a Forrester study cited in 2020 noted SOCs managing up to 11,000 alerts daily, with nearly 28% of security alerts never being addressed [6].

The term “alert fatigue” has entered the lexicon to describe how analysts become desensitized or overburdened by the incessant stream of warnings, many of which turn out to be benign. Empirical surveys support this: in an IDC/FireEye study of 350 security professionals, one-third of the respondents said they disregard some alerts due to overload. Moreover, the managed security service providers (MSSPs) in the survey reported false positive rates over 50%, which contribute heavily to alert fatigue [7].

Although alert fatigue is well-documented in organizational contexts, little is known about how consumers experience similar dynamics when managing multiple personal security tools. This research gap is addressed in our primary findings (Section 4).

2.3. Fragmentation of Functionality and Security Gaps

A third theme in the literature concerns fragmented functionality. Fragmented tooling often results in fragmented data and visibility; critical information about assets or vulnerabilities may not be aggregated. Panaseer’s 2022 report highlighted that only 36% of security leaders were very confident their controls were working as intended, despite virtually all agreeing that having comprehensive visibility into controls is valuable [8].

Overlapping functionality compounds the problem. Cisco’s analysis found that many security tools deliver redundant features, leading to duplicated spending and confusion over which outputs to trust [2]. In patch management, for example, vulnerabilities may persist when scanners and deployment tools are poorly integrated, a weakness confirmed by Poniman data showing that 60% of breaches involved unpatched, known vulnerabilities [9].

A particularly salient issue is the dual-vector exploitation that arises from siloed tool functionality. Fragmented defenses enable attackers to leverage one weakness as an entry point while simultaneously exploiting adjacent gaps, amplifying overall impact. Enterprise studies show that such overlaps—where tools operate in isolation without coordinated coverage—allow adversaries to exploit coverage gaps. Coalition’s Cyber Threat Index 2025 found that two-thirds of insured businesses had at least one exposed login service [10], while Google Cloud found that nearly half of cloud compromises involved weak or reused passwords alongside unprotected admin ports [11]. SpyCloud reported hundreds of millions of stolen credentials, with many originating from malware-infected endpoints, illustrating how attackers exploit this dual exposure [12]. Human error further amplifies the risk, with Verizon’s DBIR indicating that 60% of breaches involve some form of user or administrator misstep [13].

These findings underscore the need for holistic protection that addresses both credentials (“keys”) and network access points (“doors”).

While most research focuses on enterprises, the patterns highlight potential vulnerabilities for individual users, motivating our study to quantify the effects of fragmented functionality and overlapping protections at the personal level (see Section 4).

2.4. Summary of Gaps in Literature

Existing literature provides extensive evidence of fragmentation-related costs in enterprise security—tool sprawl, alert fatigue, and siloed functionality. Yet, quantification at the level of individual users remains scarce. In particular, few studies estimate per-user monetary or operational impacts, such as time spent managing tools, redundant personal expenditures, or risks arising from misconfiguration and under-use.

This paper contributes to filling this gap. While enterprise studies are retained here as contextual benchmarks, the Results section (Section 4) introduces original primary research quantifying how fragmentation manifests for individual consumers.

3. Methodology

This study employs a mixed-methods design that combines meta-analytic literature review with original primary research at the individual-user level: a quantitative online survey (n = 50) and semi-structured interviews/focus groups. The goal was to quantify the hidden costs of security tool fragmentation at the individual level, while situating these findings within the broader enterprise context.

3.1. Primary Research

To address the gap in individual user-level evidence, we conducted a two-part primary research effort:

Quantitative Survey: An online questionnaire (10–15 items, n = 50) targeting diverse individual user profiles segmented by age, technical proficiency, and VPN usage frequency. Questions focused on tool usage patterns, overlapping alerts, user trust, cognitive overload, and skipped security actions.

Qualitative Interviews/Focus Groups: Sixteen semi-structured interviews and small group discussions that explored personal experiences with fragmented cybersecurity tools, alert fatigue, confusion, and preferences for tool consolidation.

Per-user variables captured (definitions).

- Tool count (avg # of security/privacy tools).
- Duplicate alerts (% receiving overlapping alerts).
- Cognitive overload (% reporting overload managing tools).
- Ignored/dismissed alerts (% reporting this behavior).
- Time tax (avg hours/month on updates/logins/checks).
- Annual spend (S) on tools (USD).
- Redundancy rate (r): % paying for overlapping services.
- Under-use (u): disabled/unconfigured tools; unaware of paid features.

Sampling methods, survey instruments, and anonymized excerpts are detailed in Appendix C.

The study explicitly avoids applying enterprise-centric cost models. Instead, it prioritizes metrics that reflect individual realities—time spent on maintenance, personal financial outlays, and perceived risk in home networks, remote work environments, and personal online activities.

3.2. Secondary Sources

Source Collection: We performed systematic searches for relevant statistics and findings related to security tool fragmentation, using academic databases and search engines. Keywords included combinations of terms like “security tool sprawl,” “security alerts fatigue statistics,” “multiple security tools breach cost,” “SOC complexity survey,” and specific known sources (e.g., “Ponemon security tools 50” or “Cisco CISO study integration”). We also leveraged known high-quality industry reports and vendor research blogs to gather commentary and context (with caution to rely on the data points more than vendor opinions).

Inclusion Criteria: We prioritized sources that offered quantitative data. To validate “hidden costs,” we looked for measurable indicators: e.g., number of tools, percentages of alerts ignored, time taken for tasks, percentage of breaches with certain causes, cost figures, etc. Only data from 2015 onward was included, as the security tooling landscape shifts quickly, and older data might not reflect current complexities. Preference was given to the most recent data (2019–

2025). In cases where multiple sources provided similar metrics, we included the most widely cited or methodologically sound source.

Data Extraction and Validation: From each source, key findings were extracted verbatim or summarized. We cross-validated statistics when possible. Divergences are discussed to give a nuanced view. We also ensured that monetary figures were adjusted or cited with context. All monetary values are in USD, as that was the common unit in reports. We harmonized units (USD) and flagged where local wage rates are needed to value time for individuals.

Organization by Vertical: We mapped each extracted data point to one of the three research verticals: Access/Inertia, Alerts/Inaction, or Functionality/Gaps. In cases where sources touched on multiple areas, the data is discussed in the most relevant section but cross-referenced as needed. We structured the Results section explicitly around these verticals to maintain clarity. In each Results subsection, we present individual-level metrics and costs first, followed by enterprise benchmarks for context.

3.3. Per-User Impact Modeling

We estimate the indicative per-user annual impact using variables from our primary research.

Direct spend waste: with annual spend S and redundancy r plus under-use u

$$W = S \times (r + u)$$

Time tax: with t hours/month and hourly value w

$$T = (12 \times t) \times w$$

Alert review time: with A alerts/month, m minutes per alert

$$H = (A \times m \times 12) / 60\ hours;\ value = H \times w$$

Ignored-alert rework (optional): with A= alerts/month, Typical values: p = 1–10% of alerts (ignored → later rework); r_m = 1–10 min for quick resets.

$$R = (A \times p \times r_{\mathrm{m}} \times 12) / 60\ hours;\ value = R \times w$$

3.4. Indicative total

$$I = W + T + (H \times w) + (R \times w)$$

Default inputs (replace with local data where available): S = USD 92, r = 0.24, p = 0.01–0.10, or$_m$= 6 minutes representing a small share of ignored alerts requiring brief remediation, u = 0.10–0.20, t = 2.3 h/mo, A = ~15/mo, m =~3 min, w = USD 20–30/h.

These reflect our Appendix C findings (S, r, t) and conservative alert volumes to avoid overstating costs. We report ranges and include sensitivity notes in Results by vertical.

3.5. Ethical Considerations and Limitations

For primary research, participation was voluntary with informed consent; no directly identifying data were collected. Survey responses were aggregated; interview excerpts were anonymized. Demographics were limited to broad categories (age band, proficiency, VPN use). Data is stored securely and reported in aggregate.

Limitations in secondary sources include potential self-report bias in surveys and heterogeneity in secondary data methodologies. We mitigated these by triangulating across independent sources and distinguishing between perception-based and empirical measures. Enterprise statistics were cited only as contextual benchmarks, not extrapolated to individuals.

4. Results

4.1. Vertical 1: Fragmented Access = Inertia

Fragmented access refers to the dispersion of security-relevant information and controls across multiple tools, apps, and interfaces, each with its own login, console, and isolated data view. For individual users, this fragmentation manifests in juggling antivirus software, VPNs, password managers, and browser add-ons across devices, each requiring separate management.

Without centralized oversight (such as a SOC), the time and attention cost of switching contexts falls entirely on the user, creating inertia—delays or skipped actions—even when risks are recognized. Our findings strongly support this hypothesis, showing that fragmented toolsets correlate with slower responses and productivity loss at the individual level. Enterprise data are used here only as a benchmark, highlighting how similar inefficiencies scale down to personal environments.

4.1.1. Individual User Burden: App Hopping and Time Tax

We found that individual users employ an average of 3.4 security/privacy tools (e.g., antivirus, VPN, password managers, browser add-ons). Notably, 68% of respondents use three or more tools, and 44% have experienced overlapping alerts for the same threat across multiple tools. Among respondents, 46% described cognitive overload from managing multiple applications.

The maintenance burden is measurable. Our data shows users spend an average of 2.3 hours per month on tasks such as installing updates, re-authenticating logins, or re-enabling disabled protections. This recurring effort constitutes a clear "time tax", reducing productive hours and increasing the likelihood of postponed or skipped actions.

Direct financial costs are also apparent. On average, respondents spend USD 92 annually on security and privacy applications, with 24% attributable to redundant subscriptions. When combined with the estimated time tax (27.6 hours/year) valued at an average wage of USD 20–30/hour, the total annual impact can be expressed as

$$\boldsymbol{Annual\ Impact} = (\boldsymbol{S} \times \boldsymbol{r}) + (\boldsymbol{t} \times \boldsymbol{w})$$

Where S is the annual direct spend, r is redundancy, t is time spent managing tools, and w is the hourly wage. Applying the observed averages (S = USD 92, r =0.24r, t =27.6, w = USD 20–30) yields an estimated individual burden of ≈ USD 574–850 per year, excluding any additional incident-related costs.

Inputs are based on primary data; wage valuation is illustrative and should be localized for precision.

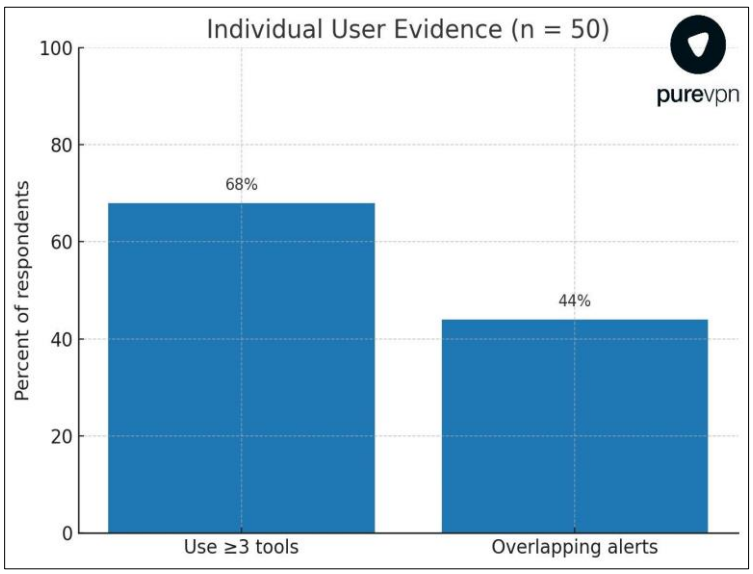

Figure 1 Individual user evidence — share of respondents using ≥3 security tools and experiencing overlapping alerts

4.2. Behavioral Impacts: Inertia and Inaction

Beyond measurable time and cost, fragmented access drives behavioral inertia among individual users. Interviews revealed that users frequently skip security tasks when managing multiple tools becomes effortful. For instance, less-proficient participants often dismissed pop-ups or delayed updates entirely, whereas advanced users reported workflow interruptions caused by updates or conflicting tool messages (e.g., antivirus flagging VPN activity).

Even small inefficiencies—such as repeated re-authentication across tools—discouraged routine maintenance, creating a pattern of delayed or abandoned actions. Unlike enterprise teams with SOC support or automated playbooks, individual users lack coordinated guidance, meaning these delays translate directly into heightened personal exposure and risk.

Taken together, the survey and interview data demonstrate that fragmented tool ecosystems impose not only a measurable time and financial burden but also behavioral friction that increases the likelihood of inaction in the face of security threats.

4.2.1. Enterprise Benchmarking

To provide context, enterprise studies show similar inefficiencies at scale. An IBM study found that environments with 50+ security tools experienced slower incident response and reduced detection performance, 7–8% lower on average than less fragmented environments. Over the prior two years, organizations with less complex security processes were less likely to experience major security disruptions (39% vs. 62%) [3].

Operational overhead has grown alongside tool proliferation. A Pana seer 2022 report revealed that security teams spent 54% of their time on manual reporting and tool coordination—up from 40% two years prior [8]. This leaves limited bandwidth for proactive tasks.

Fragmented toolsets also correlate with slower containment of security incidents. Industry reports and case studies, such as Suffolk County's 2022 ransomware breach, illustrate how alert fatigue and tool fragmentation can delay responses, increasing financial impact [14]. A Vectra AI report estimated that manual alert triage and coordination cost U.S. organizations USD 3.3 billion annually, primarily due to fragmented processes requiring human intervention [5].

Enterprise benchmarking thus highlights that the inefficiencies observed at the individual level mirror patterns in large organizations, albeit without the complexity and scale of SOC operations.

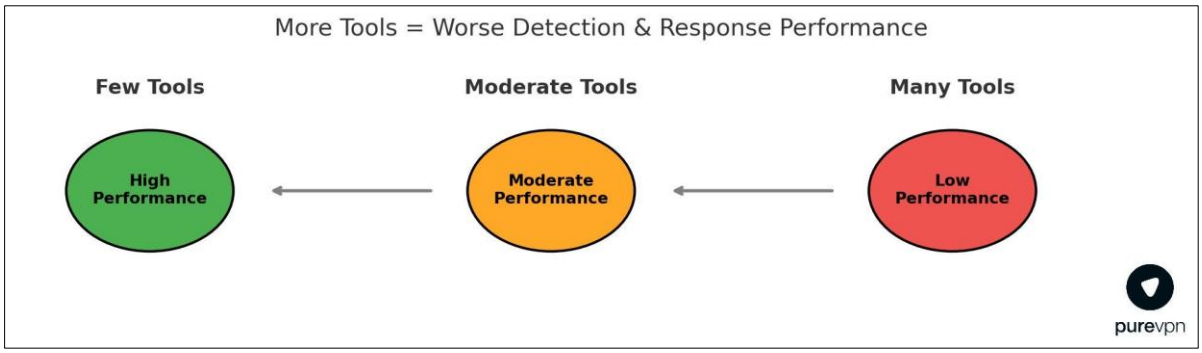

Figure 2 Self-assessed detection and response performance as a function of toolset size

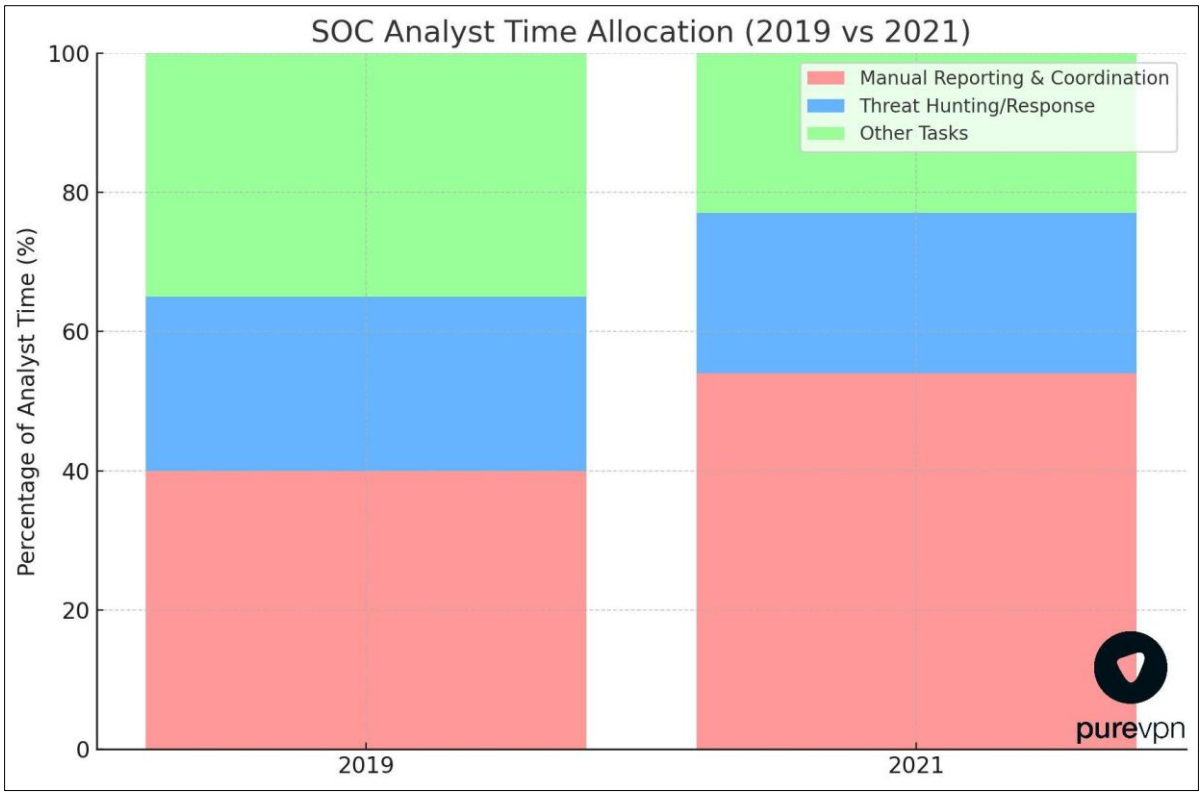

Figure 3 Increase in time spent on manual reporting and tool coordination (2019 vs 2021)

4.3. Vertical 2: Fragmented Alerts = Inaction

Fragmented alerts refer to duplicate, conflicting, or excessive notifications across multiple security tools (antivirus, VPNs, browser extensions, OS alerts) without centralized triage. For individual users, this often results in ignored or dismissed alerts, confusion over next steps, and elevated personal risk. Our interviews indicate that users commonly skip warnings or abandon actions when confronted with conflicting guidance from multiple tools, illustrating how alert fragmentation creates behavioral inaction even when risks are recognized.

4.3.1. Individual User Burden: Alert Fatigue and Monetary Impact

At the individual level, alert fragmentation creates measurable time and financial costs. We found that users spend an estimated 9 hours per year reviewing alerts (e.g., 15 alerts/month × 3 minutes/alert), valued at USD 20–30/hour, equating to USD 180–270 annually. Additional costs arise when ignored or misunderstood alerts later require remediation ("rework"), ranging from minor fixes to multi-hour interventions. Applying duplication and rework factors to survey data (44% report duplicates; 38% sometimes ignore alerts) suggests a conservative annual impact of ≈USD 180–300+ per user in wasted time alone, excluding extended consequences from actual security incidents.

The total annual impact can be expressed as

$$Annual\ Impact = (H \times w) + (R \times w)$$

Where $H=(A \times m \times 12)/60$ is the annual hours spent reviewing alerts, A= average alerts/month, m = minutes per alert, w = hourly wage, $R=(A \times p \times \boldsymbol{r}_{\mathrm{m}} \times 12)/60$ is the annual hours spent on rework where p = share of ignored alerts requiring remediation, rm = minutes per rework incident. Using observed averages (A = 15, m = 3, w = USD 20–30, $p \approx 0.05$, $r_{\mathrm{m}} \approx 6$ min) yields an estimated individual burden of ≈USD 180–300+ per year, consistent with survey evidence.

Inputs are based on primary data; wage valuation is illustrative and should be localized for precision.

4.3.2. Behavioral Impacts: Inability to Act on an Alert

Beyond measurable time and financial burdens, fragmented alerts drive the inability to act effectively on an alert. Fragmented alerts that surface in isolation deprive users of context, making it difficult to connect signals into a coherent

narrative. This effect is compounded by the use of multiple tools, eroding trust, fostering false confidence, and heightening the risk of unsafe inaction, as users are unable to link an alert to the appropriate follow-up action. Qualitative interviews indicate that users often prioritize only the most urgent alerts and defer ambiguous or low-priority signals, reflecting patterns observed among SOC analysts at the enterprise level.

Cognitive overload, alert fatigue, and emotional stress collectively reinforce hesitation. Without consolidated, actionable context, moving between applications to verify alerts is effortful, leading to skipped or deferred responses. Users often rationalize ignoring alerts based on perceived severity— "if it were serious, I'd know"—demonstrating that decisions are shaped as much by psychological factors as by technical constraints. Inconsistent notifications across apps or devices compound doubt, creating a reliance on only familiar or seemingly urgent signals. This coping strategy, while rational under cognitive load, leaves users exposed to subtle but critical threats.

4.3.3. Enterprise Benchmarking

At the enterprise level, fragmentation creates similar but amplified effects. SOC studies show that roughly two-thirds of daily alerts are ignored: A Vectra AI report found 67% unaddressed [5], FireEye/IDC reported one-third intentionally ignored [7], and MSSP surveys indicate 62% remain uninvestigated [15]. Duplicate and conflicting alerts increase analyst fatigue: Advanced Threat Analytics (ATA) reported that 53% of MSSP alerts are false positives [16], while a Devo report found that up to 84% of analysts within organizations unknowingly investigate the same incidents multiple times per month [17]. This duplication further contributes to fatigue, wasted effort, and slower response times.

Alert fragmentation at scale drives both inefficiency and cost. According to IBM, 52% of executives cite complexity across security solutions and vendors as the biggest impediment to security operations. Platformized organizations, those with more integrated security stacks, detect incidents 72 days faster and contain them 84 days faster on average [18].

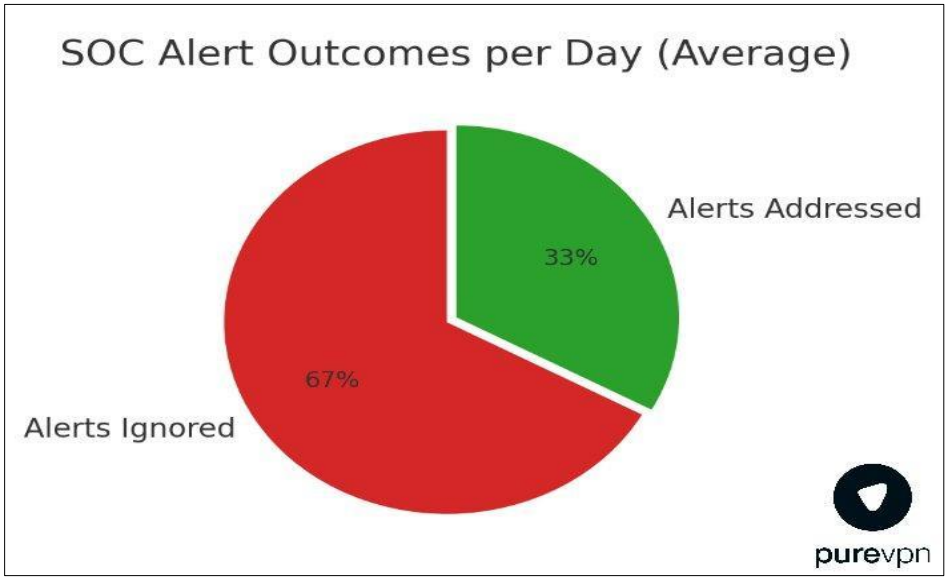

Figure 4 Daily Security Alert Outcomes in an average SOC. Studies indicate that roughly two-thirds of alerts are ignored or not investigated due to high volumes and noise. Only about one-third of alerts receive attention ("Alerts Addressed"). This highlights the extent of alert fatigue and inaction

4.4. Vertical 3: Fragmented Functionality = Security Gaps

Fragmented functionality arises when security tools operate in silos, providing partial, redundant, or missing coverage. At the individual level, this creates blind spots—areas where users may believe they are protected but remain exposed—and fosters false confidence in their defenses.

Such fragmentation can lead to under-deployment (features left disabled or unconfigured), under-use (paid capabilities never activated), and heightened vulnerabilities due to exposed gaps (arising from partial or no overlap as tools operate in silos), increasing personal risk while reducing the value of security investments. Behavioral effects include skipped or delayed tasks, misallocated attention, and reliance on perceived rather than actual protection.

4.4.1. Individual User Burden: Coverage Gaps and Monetary Impact

Survey results indicate that 29% of users have at least one installed tool disabled or unconfigured, and 34% are unaware of paid features available in their existing tools. This discrepancy between purchased and actively used protections creates a measurable financial burden. On average, users spend USD 92 per year on security tools. Of this, approximately 24% (≈ USD 22) is redundant due to overlapping capabilities, while an additional 10–20% (≈ USD 9–18) of the spend is effectively unused because features are disabled or unnoticed.

4.4.2. The combined direct financial impact can be calculated as

$$Annual\ Waste\ =\ S\ \times\ (r\ +\ u)$$

Where S = annual spend, r = redundancy, u = fraction of under-used features. Applying survey averages (S = 92, r = 0.24, $u \approx 0.10–0.20$) yields an estimated individual burden of USD 31–40/year, excluding any incident-related costs from gaps in coverage.

Inputs are based on primary data; wage valuation is illustrative and should be localized for precision.

Beyond the financial burden, these gaps represent real security risks. Leaving tools disabled or unconfigured (29% of users) or ignoring available paid features (34%) creates blind spots where users may believe they are protected but remain exposed to malware, credential theft, or other threats. These misconfigurations amplify personal risk, translating directly into a heightened likelihood of security incidents.

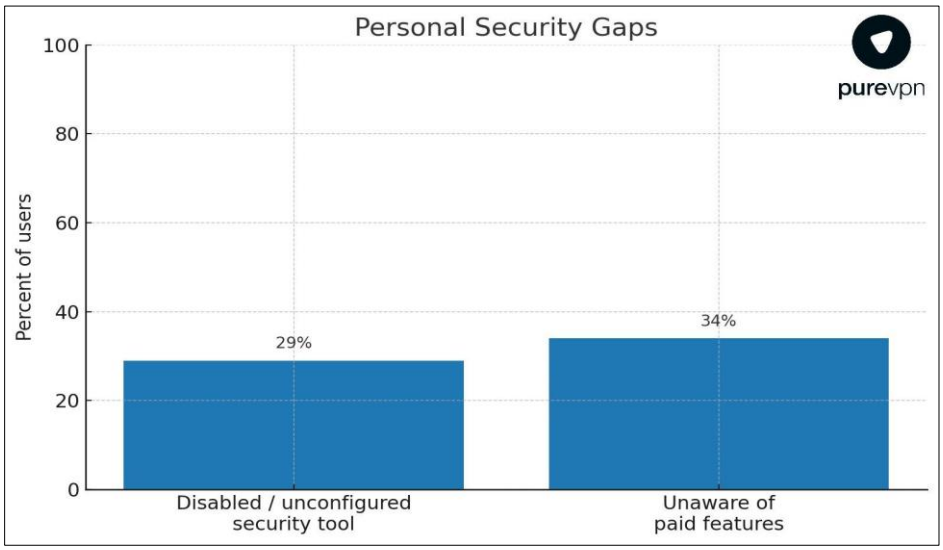

Figure 5 Personal security gaps — share of users with disabled/unconfigured

4.5. tools and unaware of paid features

4.5.1. Behavioral Impacts: False Confidence and Missed Actions

Fragmented functionality not only imposes a financial burden but also influences user behavior. Survey and interview evidence indicate that users often assume they are fully protected when tools are installed, even if key features are disabled or unconfigured. This false sense of security can lead to skipped updates, ignored alerts, and delayed remediation actions.

For instance, 29% of users with at least one disabled tool reported occasionally postponing security tasks, while 34% were unaware of paid features assumed automatic coverage. Interviews revealed that users relied on the mere presence of multiple tools to gauge protection, rather than verifying actual configurations, gap coverage or feature activation. This reliance on perceived rather than actual security contributes to coverage gaps and increases the probability of exposure to threats such as malware, phishing, or credential theft.

Cognitively, managing multiple partial and overlapping tools adds complexity and decision fatigue, reinforcing avoidance behaviors. Users often prioritize convenience over thorough maintenance, skipping non-urgent tasks or

assuming that redundant tools compensate for unconfigured ones. The combined effect is a behavioral pattern that magnifies the risks created by fragmented functionality, turning gaps in coverage into tangible security vulnerabilities at the individual level.

4.5.2. Enterprise Benchmarking

At the enterprise level, fragmented functionality produces analogous but amplified effects. Large organizations often deploy dozens of security tools, yet visibility and coverage remain incomplete. Panaseer reported that even with a quarter of organizations utilizing 76 security tools, 70.5% of security leaders admitted to not evaluating a security tool based on its impact on reducing cyber risk [19]. Furthermore, just 36% of security leaders felt confident that all controls were fully deployed and effective, indicating widespread gaps despite substantial tool investment [20].

The pattern is clear: multiple tools do not guarantee complete protection. Overlapping capabilities can create redundancy, while misconfigured, siloed, or unmonitored features leave blind spots. These enterprise-level observations mirror personal-level findings: both show that fragmented functionality can foster overconfidence, missed protections, and heightened risk exposure.

Real-world breaches underscore this risk. Organizations are frequently compromised despite assuming controls were in place—a phenomenon sometimes called "surprise breaches." Verizon's DBIR 2025 shows a 34% increase in attackers exploiting vulnerabilities to gain initial access and cause security breaches compared to the previous year, highlighting lapses in patching and configuration management [13]. Such breaches carry significant financial consequences: the global average cost of a data breach is estimated at USD 4.44 million, illustrating how gaps in tool deployment and coordination directly translate into both security and economic risk [18].

4.6. User Case Studies — Real-World Experiences of Tool Fragmentation

Each case pairs a short narrative with an individual-level Monetary Snapshot and a Cost tag. Snapshots use our per-user model (time tax, alert-review time, and direct spend waste), while enterprise figures elsewhere remain benchmarks only.

To illustrate the lived experiences behind the survey and interview statistics, the following short case studies summarize individual user scenarios. Each highlights different dimensions of how cybersecurity tool fragmentation affects personal security.

These narratives align with our survey: duplicated alerts (44%), cognitive overload (46%), and alert dismissal (38%) emerge repeatedly as drivers of hesitation and unsafe simplification.

4.6.1. Case Study 1: The Overwhelmed Guardian

Profile: Age 55, Basic technical proficiency, VPN used occasionally.

This user installed four separate security tools—an antivirus suite, a VPN, a password manager, and a browser extension—on the recommendation of friends and online articles. Within weeks, overlapping alerts and renewal prompts became a constant annoyance. When faced with simultaneous warnings from two tools about the same website, the user simply ignored both, assuming it was a glitch. This hesitation left the system potentially exposed. The case underscores how excessive, uncoordinated alerts can result in risky inaction.

4.6.2. Monetary Snapshot

- **Time tax (maintenance):** ~2.3 h/month → 27.6 h/year → USD 552–828/year (valued at USD 20–30/h).
- **Alert review time:** baseline example 15 alerts/month × 3 min → ~9 h/year → USD 180–270/year.
- **Direct spend waste:** USD 92 × (24% redundancy + 10–20% under-use) → ~USD 31–40/year.
- **Indicative annual impact:** ~USD 763–1,138 per user (sum of the above), excluding incident losses.
- **Cost tag (annual, indicative):** USD 763–1,138 in time + wasted spend driven by duplicates and ignored alerts (case aligns with 44% duplicates, 38% ignored; see Appendix C).

4.6.3. Case Study 2: The Diligent Tech Enthusiast

Profile: Age 28, Advanced technical proficiency, VPN used daily.

Determined to cover all bases, this user maintains six different cybersecurity and privacy tools, including device-based firewalls, a dedicated anti-malware scanner, and IoT monitoring software. Monthly, they spend over five hours on updates, troubleshooting compatibility issues, and verifying whether overlapping features are necessary. Despite their expertise, they acknowledge frustration at paying for redundant services, noting that integration could save both time and money. This scenario highlights the personal cost of fragmentation, even for skilled users.

4.7. Monetary Snapshot

- Time tax (maintenance): ≥5 h/month → ≥60 h/year → ≥USD 1,200–1,800/year (at USD 20–30/h).
- Alert review time (baseline): ~9 h/year → USD 180–270/year.
- Direct spend waste: USD 92 × (24% + 10–20%) → ~USD 31–40/year *(likely higher if multiple paid tools are maintained; scale W = S × (run) with actual spend).*
- Indicative annual impact: ~USD 1,411–2,110+ per user (time + alerts + spend), excluding incident losses.
- Cost tag (annual, indicative): USD 1.4k–USD 2.1k+ primarily from time (≥5 h/month upkeep) plus redundant/under-used subscriptions; reflects case narrative on six tools and compatibility troubleshooting.

4.7.1. Case Study 3: The Disillusioned Minimalist

Profile: Age 67, Intermediate technical proficiency, no VPN usage.

After years of juggling multiple tools and dealing with frequent false positives, this user decided to uninstall all but one security product. While this reduced interruptions, it also eliminated layers of protection, potentially increasing vulnerability. The decision was driven by a desire for simplicity over completeness, demonstrating how poor user experience can lead to reduced security posture.

These case studies humanize the statistical trends, showing that fragmentation's hidden costs are not abstract metrics but tangible obstacles to effective personal cybersecurity.

4.8. Monetary Snapshot

- Time savings (if consolidation reduces upkeep): with a monthly reduction of Δt h, annual savings = 12 × Δt × USD w;
- *Example:* if $\Delta t \approx 1.5$ h/month, savings ≈ 18 h/year → USD 360–540/year (at USD 20–30/h). Direct spend: fewer tools may lower S, but coverage gaps can impose unpriced risk if protections are missing or misconfigured.
- Risk note: any single incident can dominate annual savings; minimalist stacks require explicit coverage checks (password, anti-malware, browser, OS, backups).
- Cost tag (annual, indicative): USD 360–540 saved on time if upkeep drops by ~1.5 h/month, but exposure increases without layered controls; quantify locally using I = W + T + (H×w) + (R×w).
- These individual snapshots quantify how fragmentation converts into personal time and money—or, in minimalist setups, how reductions in time can trade off with coverage risk. We expand on trade-offs and ROI of consolidation in Section 5.

5. Discussion

Across all three verticals, fragmentation translates directly into personal time tax, alert fatigue, and wasted out-of-pocket spend for individual users who lack SOC support. Our study quantifies per-user impacts, referencing enterprise data only as a benchmark for context. The remainder of this section synthesizes these findings, focusing on individual behaviors, costs, and practical paths to reduce fragmentation.

5.1. Interplay of Vertical Issues

For personal users, alert noise (Vertical 2) fuels inertia (Vertical 1) and leaves functionality gaps (Vertical 3)—for example, duplicated or conflicting alerts erode trust, users defer updates, and some protections remain disabled or unconfigured. This creates a self-reinforcing loop of inaction and exposure.

Although enterprise studies show similar patterns—alert fatigue, misconfigured controls, and fragmented toolsets—the implications for individuals are often more immediate. Without centralized IT support, individuals rely on guesswork or habitual behavior to interpret alerts, which increases the likelihood of risky inaction or reliance on a single familiar tool, regardless of its effectiveness.

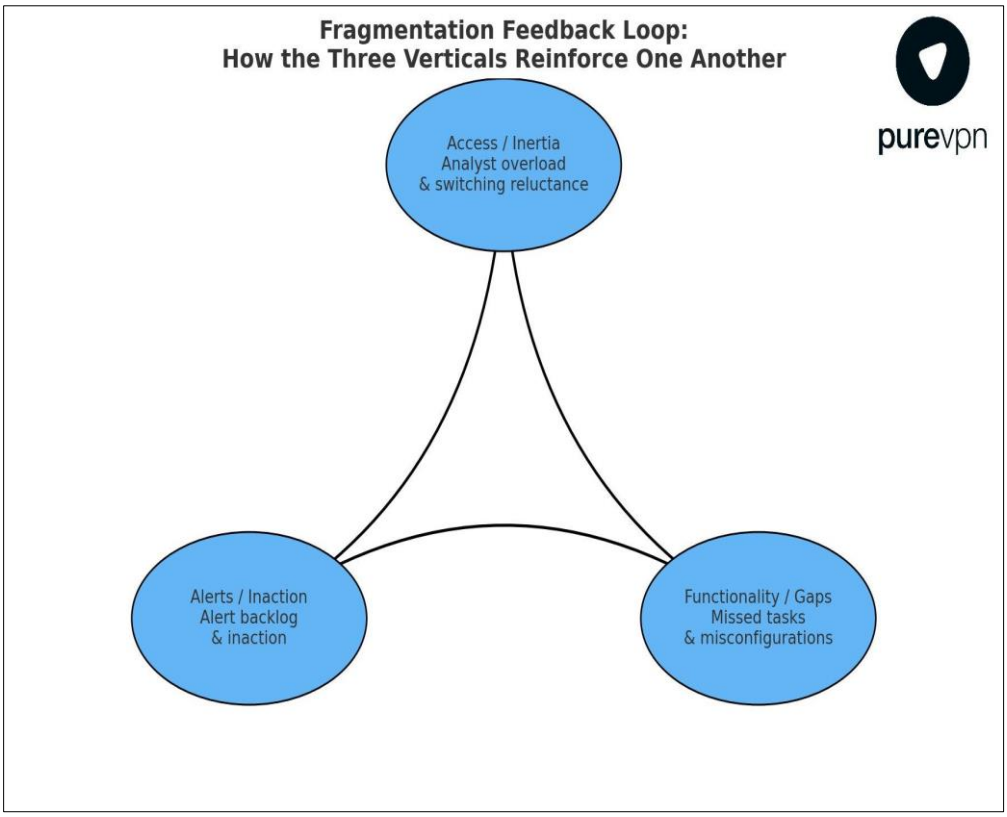

Figure 6 Interdependency between the three vertical fragmentation issues: Inertia, Inaction, and Gaps

5.2. Human Factors and Security Efficacy

Human factors are central to effective security. Individual users face a unique set of challenges: unlike organizations, they operate without formal policies, structured training, or access to incident response teams. This means that security decisions often rely on intuition, habit, or incomplete understanding, rather than standardized procedures.

Information overload, unclear alerts, and fragmented interfaces directly affect personal security decisions. For example, users may ignore or dismiss repeated warnings, postpone updates, or fail to configure tools correctly simply because the process is confusing or time-consuming. Even when a user has multiple security tools, the lack of integration and guidance can create blind spots, leaving critical assets exposed.

These human-centered challenges compound each other: alert fatigue can lead to inaction, inaction can create gaps in protection, and gaps increase the likelihood of security incidents. Recognizing the role of usability, mental load, and behavior is therefore essential—not just for designing better tools, but also for empowering users to make consistent, informed security choices.

5.2.1. Practical mitigations for individual users include

- Consolidating to fewer, better-integrated tools.
- Muting non-critical notifications while keeping high-severity alerts active.
- Running a monthly 30–45-minute maintenance window (updates, license audit, configuration checks).
- Auditing paid features to avoid overlap and cancel redundant subscriptions.

These steps reduce time tax, confusion, and the risk of leaving protections disabled or underused.

Users often face a choice between multiple specialized ('best-of-breed') tools or a smaller, integrated suite. While best-of-breed tools may offer advanced capabilities, they can increase alert fatigue, maintenance time, and functional overlap. These trade-offs must be considered alongside human factors to ensure that security efforts are practical and effective.

At the enterprise level, the same dynamics scale differently. Human analysts have cognitive and temporal limits. When those limits are exceeded (by asking them to use 70+ different tools or investigate 1000+ alerts a day), security ultimately suffers. Burnout, stress, and fatigue are not merely human resources concerns—they are direct contributors to operational security failures—a missed attack here, a misconfiguration there. Organizations, therefore, need to view simplification and integration of tools as a way to enhance human performance. Streamlining interfaces and reducing context switches can free analysts to do deeper analysis on important issues rather than superficial triage on too many issues.

5.2.2. ROI of Consolidation

- Reducing fragmentation produces measurable benefits for individual users. For example,
- Reducing time spent managing alerts from 2.3 hours/month to 1.0 hour/month saves ~15.6 hours/year. At USD 20–30/hour, this equates to USD 312–468/year.
- Minimizing redundant spending from 24% of USD 92 (~USD 22) to 10% (~USD 9) saves ~USD 13/year.
- Reducing under-use of features from 10–20% to 5–10% adds ~USD 5–9/year.

Together, these measures yield an estimated per-user ROI of USD 330–490/year in time and money alone, excluding avoided security incidents.

It can be expressed as

$$\boldsymbol{I} = \boldsymbol{W} + \boldsymbol{T} + (\boldsymbol{H} \times \boldsymbol{w}) + (\boldsymbol{R} \times \boldsymbol{w})$$

For context, enterprise benchmarking suggests that consolidation and tool integration can accelerate incident detection and containment (e.g., 72–84 days faster per IBM) and improve ROI. While these figures are not directly applicable to individual users, they illustrate the potential value of reducing fragmentation and optimizing tool use [14].

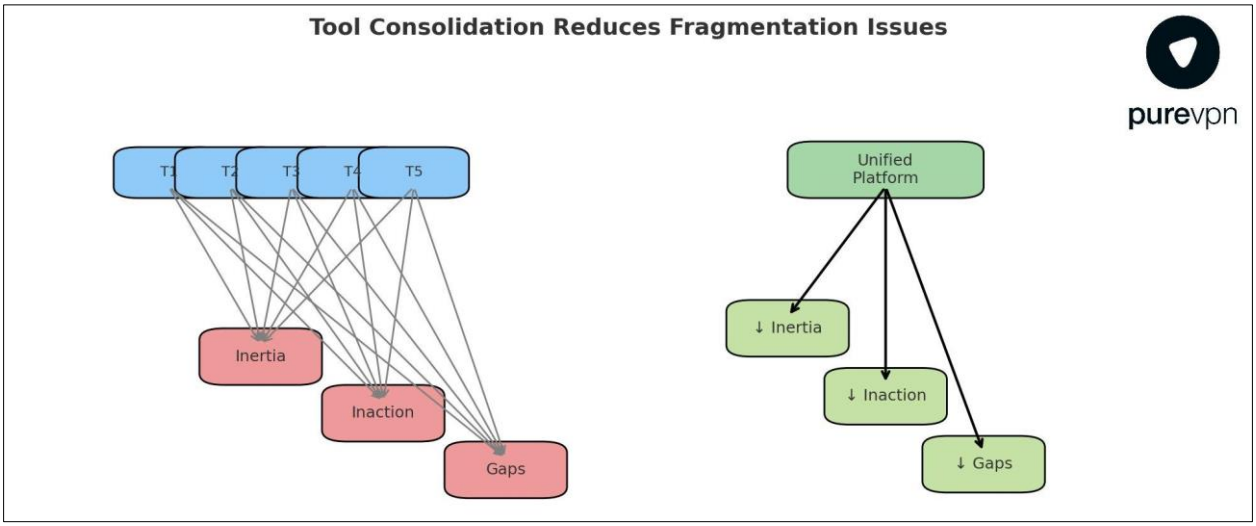

Figure 7 Unified security platform addressing all three vertical fragmentation issues

5.3. The Limit of Best-of-Breed

Individual users must decide when to keep a specialized tool. Keep a best-of-breed tool only if it (1) provides a unique, needed capability, (2) does not conflict with your suite, (3) adds ≤15 min/month upkeep, and (4) has clear alerts you can act on. Otherwise, consolidate into the suite. (Prevents false confidence from overlap.)

A counterpoint often raised is that using multiple specialized tools ("best of breed") can be better than an integrated suite that might have some weaker components. While specialization can have benefits, our findings suggest a tipping point where the complexity outweighs the marginal benefit of any single superior tool. If a best-of-breed tool isn't

utilized fully or its alerts get lost, its superiority is moot. It might be better to have a 90%-effective tool that is consistently used than a 99%-effective tool that is too cumbersome to use properly. This doesn't mean individuals or enterprises should settle for poor capabilities, but it means integration and usability should be considered part of what makes something "best."

5.4. Policy and Training Implications

For individual users: Habits and defaults.

- **Monthly one-page check:** updates ON, protections enabled on all devices.
- **Alerts:** keep high-severity; mute noise categories.
- **Spend:** review and cancel overlaps quarterly.
- **Backups and passwords:** ensure automatic backups; use a password manager you actually maintain.

For enterprises, addressing fragmentation involves process and training improvements. For example, establishing rigorous incident response playbooks (something IBM found many organizations lacked) can mitigate fragmentation by at least providing clear steps on which tools to consult and when. If everyone knows the procedure when an alert comes in (which systems to check, how to cross-verify), there is less floundering across tools. Regular drills can ensure that multiple tools are used in a cohesive manner rather than ad hoc. Also, training staff on the full capabilities of existing tools could reduce the tendency to buy new ones and decrease shelfware. Some respondents blamed underutilization on insufficient understanding of tools within IT. Investing in training might unlock features in current tools that make other tools redundant (for instance, discovering that a SIEM could do a function that a separate script was being purchased for).

5.5. Limitations and Future Research

The addition of primary individual user research addresses prior limitations related to the exclusive use of secondary enterprise data. However, the individual user-focused findings are subject to constraints, including self-reported data biases and sample size limitations for qualitative interviews.

Our consumer sample (n=50) and self-reported measures (time, alert behavior, spend) may under- or over-estimate true values; hourly rates also require localization for precise cost modeling. While the sample size is modest, the findings serve as a hypothesis-generating foundation. Future studies can build on this work using this study as a stepping-stone toward more generalizable insights.

5.5.1. Future work should include

- Longitudinal per-user logging of alert volumes/actions and time-on-task;
- A/B field trials: integrated suite vs. best-of-breed on $I = W + T + (H \times w) + (R \times w)$;
- Segmented analysis by proficiency and device mix (home IoT, mobile).

5.5.2. Holistic Security Architecture

For individual users, a holistic security approach emphasizes a minimal, coherent toolset with clear defaults, coverage across devices, browsers, identity, and backups, and a single interface for acting on critical alerts. Consolidation reduces cognitive load, alert fatigue, and redundant features, improving both usability and security outcomes.

Prioritizing signal over noise ensures important alerts are noticed while non-essential notifications are minimized. Guided defaults, streamlined dashboards, and periodic maintenance reviews help users maintain consistent protection without excessive effort.

This approach also provides tangible economic benefits: minimizing overlap and inefficiency saves time, reduces unnecessary spending, and lowers the risk of missed protections. Overall, reducing fragmentation enhances both personal security and efficiency.

Per-user impacts and actionable steps are summarized in Section 6.

6. Conclusion

6.1. Summary of Findings

This study provides empirical evidence that individual users typically manage 3.4 security/privacy tools (antivirus, VPN, password managers, browser add-ons), with 68% using three or more tools. Overlapping alerts are common (44%), and 46% report cognitive overload from managing multiple applications.

Maintenance effort constitutes a clear time tax: users spend 2.3 hours per month (≈27.6 hours/year) on tasks such as updating software, re-authenticating logins, or re-enabling disabled protections. When valued at USD 20–30/hour, this translates to USD 552–828/year.

Direct financial costs are also substantial. Average annual spend is USD 92, of which 24% (≈USD 22) is redundant. Additionally, 10–20% (≈USD 9–18) of spend is effectively unused due to disabled tools or unrecognized paid features.

Alert fragmentation further increases burdens: reviewing alerts consumes an estimated 9 hours/year (≈USD 180–270), and ignoring or mismanaging alerts adds USD 180–300+ annually in rework. Combining time, redundancy, and underused features, the total per-user annual impact is approximately USD 574–850, excluding potential costs from actual security incidents.

6.1.1. Breaking it down by vertical

- V1 — Access ⇒ Inertia: context switching and multiple consoles create a time tax (updates/logins/checks).
- V2 — Alerts ⇒ Inaction: duplicates and noise drive alert fatigue and skips.
- V3 — Functionality ⇒ Gaps: disabled/unconfigured tools, siloed functionality and unaware paid features create coverage gaps and under-realized value.

These data confirm that fragmentation at the individual level imposes measurable operational, cognitive, and financial costs.

6.1.2. Implications

Fragmentation shifts time, money, and risk to users. High-ROI mitigation strategies include consolidation, alert tuning, and monthly maintenance.

Although enterprise benchmarks show similar patterns (e.g., slower incident response in fragmented SOCs), the primary contribution here is the quantitative assessment of per-user impacts, highlighting how fragmentation affects personal security decisions and behaviors.

Recommendations For Individual Users

Based on survey evidence, individual users face measurable time, financial, and operational burdens from tool fragmentation. Recommendations focus on reducing duplication, optimizing alert management, and maximizing feature utilization.

6.2. Key Practices

- Inventory: List all security/privacy tools and paid plans; identify overlapping capabilities.
- Configure: Ensure core protections (antivirus, VPN, password manager, backups) are active across all devices.
- Alerts: Retain only high-severity notifications; mute repetitive or low-value alerts.
- Spend: Cancel redundant subscriptions; prioritize integrated or minimal toolsets.
- Time Management: Schedule 30–45 minutes/month for updates, verification, and maintenance.

KPIs: Time tax (h/month), duplicate alerts (%), ignored alerts (%), redundant spend (%), under-use (%).

Outcome Targets: Reduce duplicate alerts by ≈50%; limit time tax to ≤1 hour/month.

Per-User Monetary Snapshot (Annual)

- Direct spend (S): USD 92 avg; redundancy ≈24% ⇒ USD 22 waste.
- Under-use (u): 10–20% of S (proxied by 29% disabled and 34% unaware) ⇒ ≈USD 9–18 of value not realized.
- Time tax: ≈2.3 h/month ⇒ 27.6 h/year; valued at USD 20–30/h (localize), that's USD 552–828.
- Indicative annual impact: ≈ USD 583–868 per user, excluding additional incident-related losses.

Formula

$$Annual\ Impact = (S \times r) + (S \times u) + (t \times w)$$

Where S = annual spend, r= redundancy fraction, u = under-use fraction, t = annual hours spent managing tools, w = hourly wage.

6.2.1. Monetary Lens by Vertical

- V1 Access: Time tax → USD via hourly value; reduce via consolidation.
- V2 Alerts: Alert review hours + rework; reduce via noise tuning.
- V3 Functionality: Financial loss = S × (redundancy + under-use); reduce via consolidation and enabling features.

6.2.2. Contextual Benchmarking for Organizations

- Integration Strategy: Inventory tools, assess overlap/gaps, and centralize dashboards via APIs or unified platforms.
- Vendor Consolidation: Remove marginal tools while maintaining essential functionality; reduce license costs and training overhead.
- Automation and Orchestration: Apply SOAR (Security Orchestration, Automation, Response) /playbooks to triage routine alerts and merge duplicates.
- Metrics and Validation: Track mean time to detect/respond, alerts per analyst/day, tool adoption rates, and impact on ROI and risk reduction.

6.3. Conclusion Statement

This study demonstrates that individual users face significant hidden costs due to cybersecurity tool fragmentation, encompassing time lost, redundant financial expenditure, and exposure to security gaps. Survey evidence quantifies these impacts at approximately USD 583–868 per user annually (combining time tax and redundant or under-used spend), excluding potential additional losses from unresolved alerts or security incidents.

6.3.1. Key findings indicate that fragmentation manifests across three domains

- Access: Multiple tools and interfaces create operational inertia, increasing the likelihood of delayed updates or skipped maintenance.
- Alerts: Duplicates and alert fatigue can result in ignored or postponed notifications, thereby increasing the risk of undetected threats.
- Functionality: Disabled or unconfigured tools, siloed functionality along with unused paid features, produce coverage gaps and under-realized value.

The evidence supports actionable steps for individual users: consolidating toolsets, optimizing alerts, enabling all paid features, and maintaining a regular update schedule. Implementing these measures reduces both monetary and operational burdens while mitigating personal security risk.

For enterprises, the findings provide contextual benchmarks: fragmented access, alerts, and functionality also produce measurable inefficiencies and risk exposure at scale. However, these challenges are addressable through strategic integration, tool consolidation, process optimization, and targeted automation.

Ultimately, recognizing fragmentation itself as a risk factor enables a more coherent cybersecurity posture—whether for individual users or organizations. A minimal, well-configured, and integrated security stack ensures that every tool and alert serves a clear purpose, maximizing resilience, reducing waste, and improving the efficacy of human decision-making in security management.

Compliance with ethical standards

Acknowledgments

The authors would like to thank M. Murtaza, Ramsha Sadiq Khan, and Saba Hasan for their valuable contributions to refining this manuscript. Their efforts in proofreading and editing greatly improved the clarity and quality of the paper.

Disclosure of conflict of interest

The authors would like to thank M. Murtaza, Ramsha Sadiq Khan, and Saba Hasan for their valuable contributions to refining this manuscript. Their efforts in proofreading and editing greatly improved the clarity and quality of the paper.

Statement of informed consent

Informed consent was obtained from all subjects involved in the study prior to their participation. The study's purpose, procedures, potential risks, and benefits were clearly explained. Participants were informed that their participation was voluntary, that they could withdraw at any time without penalty, and that all data would be anonymized and reported only in aggregate to ensure confidentiality.

Data Availability Statement

The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy and ethical restrictions.

Funding

This research was funded by Pure VPN (a part of Pure Square) through its internal research and development program. The funder provided financial support for the study but had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Author Contributions

Conceptualization, I.A. and A.T.; Methodology, I.A. and A.T.; Software, I.A.; Validation, I.A. and A.T.; Formal Analysis, I.A.; Investigation, I.A.; Resources, A.T.; Data Curation, I.A.; Writing – Original Draft Preparation, I.A.; Writing – Review and Editing, I.A. and A.T.; Visualization, I.A.; Supervision, A.T.; Project Administration, A.T.

References

[1] Cisco. Caution Security Startups, Investors, and Standalone Solutions—Cisco 2019 CISO Benchmark Study Reports Increased Vendor Consolidation. Available online: https://newsroom.cisco.com/cisco-2019-cisco-benchmark-study (accessed on 29 August 2025).

[2] Outshift by Cisco. The hidden cost of cybersecurity tool sprawl. Available online: https://outshift.cisco.com/blog/hidden-cost-of-cybersecurity-tool-sprawl (accessed on 29 August 2025).

[3] IBM Security; Ponemon Institute. IBM Study: Security Response Planning on the Rise, But Containing Attacks Remains an Issue. Available online: https://newsroom.ibm.com/2020-06-30-IBM-Study-Security-Response-Planning-on-the-Rise-But-Containing-Attacks-Remains-an-Issue (accessed on 29 August 2025).

[4] Mark, G.; Gudith, G.; Klocke, U. The Cost of Interrupted Work: More Speed and Stress. 2008. Available online: https://ics.uci.edu/~gmark/chi08-mark.pdf (accessed on 29 August 2025).

[5] Vectra AI. 2023 State of Threat Detection. Available online: https://www.vectra.ai/resources/2023-state-of-threat-detection (accessed on 29 August 2025).

[6] Forrester Consulting; Palo Alto Networks. 2020 State of Security Operations. Available online: https://www.paloaltonetworks.com/blog/2020/09/state-of-security-operations/ (accessed on 29 August 2025).

[7] Cybersecurity Dive. One-third of analysts ignore security alerts, survey finds. Available online: https://www.cybersecuritydive.com/news/security-alert-analyst-SOC-idc-fireeye/595111/ (accessed on 29 August 2025).

[8] Panaseer. 2022 Security Leaders Peer Report. Available online: https://panaseer.com/resources/reports/2022-security-leaders-peer-report (accessed on 29 August 2025).

[9] Ponemon Institute; ServiceNow. Costs and Consequences of Gaps in Vulnerability Response. Available online: https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html (accessed on 29 August 2025).

[10] Coalition. Coalition's Cyber Threat Index 2025 Finds Most Ransomware Incidents Start with Compromised VPN Devices. Available online: https://www.coalitioninc.com/announcements/cyber-threat-index-2025 (accessed on 29 August 2025).

[11] Google Cloud Security. H2 2024 Threat Horizons Report. Available online: https://services.google.com/fh/files/misc/threat_horizons_report_h2_2024.pdf (accessed on 29 August 2025).

[12] SpyCloud. 2025 SpyCloud Annual Identity Exposure Report. Available online: https://spycloud.com/resource/report/spycloud-annual-identity-exposure-report-2025/ (accessed on 29 August 2025).

[13] Verizon. 2025 Data Breach Investigations Report. Available online: https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf (accessed on 29 August 2025).

[14] Suffolk County Legislature's Special Cyber Intrusion Investigation Committee. Report On The 2021-2022 Cyber-Attack on Suffolk County. Available online: https://www.scnylegislature.us/DocumentCenter/View/118502/09122024-Report-On-The-2021-2022-Cyber-Attack-On-Suffolk-County-PDF (accessed on 29 August 2025).

[15] MSSP Alert. MSSP Market News: Survey Shows 62% of SOC Alerts are Ignored. Available online: https://www.msspalert.com/news/mssp-market-news-survey-shows-62-of-soc-alerts-are-ignored (accessed on 29 August 2025).

[16] Corporate Compliance Insights. MSSP Incident Responders Overwhelmed by False-Positive Security Alerts. Available online: https://www.corporatecomplianceinsights.com/mssp-incident-responders-overwhelmed-false-positive-security-alerts/ (accessed on 29 August 2025).

[17] Devo. Navigating the Alert Avalanche: 5 Signs Your SOC is Stuck in the Past. Available online: https://www.devo.com/blog/navigating-the-alert-avalanche-5-signs-your-soc-is-stuck-in-the-past/ (accessed on 29 August 2025).

[18] IBM Security. Capturing the cybersecurity dividend. Available online: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/unified-cybersecurity-platform (accessed on 29 August 2025).

[19] PR Newswire. Basic Visibility, Tool Overload and Manual Reporting Revealed as Top Concerns in Panaseer's First Security Leader's Peer Report. Available online: https://www.prnewswire.com/news-releases/basic-visibility-tool-overload-and-manual-reporting-revealed-as-top-concerns-in-panaseers-first-security-leaders-peer-report-300871467.html (accessed on 29 August 2025).

[20] Help Net Security. Control failures are behind a growing number of cybersecurity incidents. Available online: https://www.helpnetsecurity.com/2021/12/01/control-failures-cybersecurity/ (accessed on 29 August 2025).

[21] IBM Security. Cost of a Data Breach Report 2025. Available online: https://www.ibm.com/reports/data-breach (accessed on 29 August 2025).

Appendix A — Survey Instrument

Individuals-First Instrument (Monetary and Operational Focus).

This survey captures per-user time, spend, and behavior needed to estimate individual impact from tool fragmentation. Questions feed the following derived metrics (not shown to respondents): $W = S \times (r + u)$, $T = 12 \times t \times w$, $H = (A \times m \times 12)/60$, $R = (A \times p \times r_m \times 12)/60$. Values are reported in aggregate only.

Consent and Privacy. Participation is voluntary; no directly identifying data are collected. Responses are anonymized and aggregated. You may skip any question.

Section 1 — Demographics and Segmentation

Age Group

☐ 18–29

☐ 30–49

☐ 50–69

☐ 70+

Self-Rated Technical Proficiency

☐ Basic User – I use technology for essential tasks and require guidance for setup/configuration.

☐ Intermediate – I can manage most device and software settings independently.

☐ Advanced/IT Professional – I am comfortable with complex configurations and troubleshooting.

VPN Usage Frequency

☐ Never

☐ Rarely – a few times per year

☐ Sometimes – a few times per month

☐ Regularly – at least weekly

☐ Daily

Country/Region

☐ …

Local Currency (e.g., USD, EUR, PLN) — *for reporting only*

[free text / dropdown]

Approximate hourly value of your time (choose a band you feel matches your time value for routine tasks)

☐ <$10 ☐ $10–$19 ☐ $20–$29 ☐ $30–$49 ☐ $50+ ☐ Prefer not to say

Devices you personally secure (select all)

☐ Windows PC ☐ macOS ☐ Linux ☐ iOS/iPadOS ☐ Android ☐ Home IoT/Smart devices

Primary contexts (select all)

☐ Personal/home use ☐ Remote work on personal device ☐ Shared household device

Section 2 — Tool Usage Patterns

Security/Privacy Tools Used Regularly (Select all that apply)

☐ Antivirus/Anti-malware software

☐ VPN service

☐ Password manager

☐ Firewall (hardware or software)

☐ Browser security extensions (e.g., ad blocker, anti-tracker)

☐ Identity theft/credit monitoring service

☐ Other: _____

How many security/privacy tools do you use monthly?

Total: [number] Paid: [number] Free: [number]

How many different vendors are these tools from? [number]

List any paid plans and monthly cost (approximate)

[free text / repeating rows: Tool/Plan | Monthly cost]

Monthly maintenance time on security tools (updates, logins, checks)

☐ <30 min ☐ 30–59 min ☐ 1–2 h ☐ 2–4 h ☐ >4 h

(or) Enter hours/month: [number]

Section 3 — Fragmentation and Overlap

Have you ever received duplicate or overlapping alerts or notifications about the same security issue from different tools?

☐ Never

☐ Once or twice

☐ Occasionally

☐ Frequently

When a security tool gives you a warning or recommendation, how often do you take immediate action?

☐ Always

☐ Often

☐ Sometimes

☐ Rarely

☐ Never

Have you ever ignored or dismissed a security alert? (Select all that apply)

☐ Yes – I didn't understand the alert

☐ Yes – It didn't seem important/was probably a false alarm

☐ Yes – I get too many alerts (alert fatigue)

☐ Yes – Another tool already handled it

☐ Yes – Other reason: _____

☐ No – I never ignore important alerts

How often do you see conflicting alerts between tools (e.g., VPN says OK, AV blocks)?

☐ Never ☐ Rarely ☐ Sometimes ☐ Often ☐ Very often

Estimated duplicate share of your alerts (your best guess)

☐ 0% ☐ 1–25% ☐ 26–50% ☐ 51–75% ☐ 76–100%

When you receive an alert, how many tools do you usually check before deciding?

☐ 0 (I act on the first) ☐ 1 ☐ 2+

Average time per alert (including reading and any checks)

☐ <1 min ☐ 1–2 min ☐ 3–5 min ☐ 6–10 min ☐ >10 min

(or) Enter minutes/alert: [number]

Top reasons for not acting immediately (select all)

☐ Too many alerts ☐ Duplicate/conflicting alerts ☐ Unsure what to do ☐ Took too much time ☐ False positive ☐ Other___

Section 4 — Trust, Fatigue, and Preferences

How much do you trust the security tools you use to protect you effectively?

- Do not trust at all
- Slightly trust
- Moderately trust
- Mostly trust

Completely trust

Do you feel overwhelmed by having to manage multiple security tools?

☐ Strongly Agree

☐ Agree

☐ Neutral

☐ Disagree

☐ Strongly Disagree

Would you prefer a single, unified security solution over multiple separate tools?

☐ Yes

☐ No

☐ Not sure

If yes or no, why? (Open-ended): _____

Cognitive overload managing tools

Likert 1–5: 1 Not at all … 5 Extremely

Preference for consolidation

☐ Strongly prefer one integrated suite ☐ Somewhat prefer suite ☐ No preference ☐ Prefer best-of-breed mix

Section 5 — Costs and Actions

In the past year, have you ever decided not to follow a security recommendation or turned off a security feature because it was too confusing or inconvenient?

☐ Yes (please describe): _____

☐ No

Approximate time spent per month on security maintenance (updates, alerts, troubleshooting)

☐ Less than 1 hour

☐ 1–3 hours

☐ 3–5 hours

☐ More than 5 hours

Estimated annual spending on security/privacy tools

☐ $0 (only free tools)

☐ Less than $50

☐ $50–$100

☐ $101–$200

☐ More than $200

Do you pay for two or more tools that provide overlapping features (redundant subscriptions)?

☐ Yes

☐ No

Approximate total monthly spends (S) on security/privacy tools (local currency): [number]

Overlapping/duplicative subscriptions (r) — your best estimate

☐ 0% ☐ ~10% ☐ ~20% ☐ ~30% ☐ ≥40%

Under-use (u) — paid features you don't use / tools left installed but disabled/unconfigured

☐ 0% ☐ ~5% ☐ ~10% ☐ ~20% ☐ ≥30%

Alerts/month (A) you typically review across tools: [number]

Minutes per alert (m) *(if not answered in Q16)*: [number]

Ignored/dismissed alerts (p) *(at least sometimes)*

☐ 0% ☐ 1–10% ☐ 11–25% ☐ 26–50% ☐ >50%

If you ignore an alert, how much rework time later (r_m) (resets/cleanup)

☐ 0–2 min ☐ 3–5 min ☐ 6–10 min ☐ >10 min

In the past 12 months, any personal security incident?

☐ No ☐ Yes — How many? [number]

- Direct monetary costs (e.g., paid support, replacements) — approx total: [number + currency] Time spent resolving (hours): [number]
- Main cause(s) (select all): ☐ Phishing/credential theft ☐ Malware ☐ Account takeover ☐ Data loss ☐ Other:
- Did conflicting/duplicate alerts contribute? ☐ No ☐ Possibly ☐ Yes
- Interest in consolidation if it reduced your time by ≥1 h/month

☐ Not interested ☐ Maybe ☐ Likely ☐ Definitely

What would you remove/enable first to reduce duplicates and gaps? [free text]

Skip/Logic Notes (researcher)

- If Q12 >2 h/month or (Q23×Q24) > 60 min/month, route to a time-management probe (free text). If Q21 ≥30% or Q22 ≥20%, route to a redundancy/under-use probe (free text): "Which tools/features overlap or remain off?"
- If Q27 = Yes, capture incident narrative (free text) and whether consolidation/noise-tuning could have avoided rework.

Derived Variables (researcher)

$W = S \times (r + u)$; $T = (12 \times t) \times w$; $H = (A \times m \times 12)/60$; $R = (A \times p \times r_m \times 12)/60$; $I = W + T + (Haw) + (Row)$.

Appendix B — Interview/Focus Group Guide

Title: Individual User Experiences with Cybersecurity Tool Fragmentation — Semi-Structured Interview Guide (Individuals-First + Monetary and Operational Probes)

Purpose: Capture individual-level experiences of tool fragmentation and quantify per-user impact. Alongside narratives, collect light-weight numerical anchors to estimate

- Time tax (t, hours/month), alert volume (A) and minutes per alert (m),
- Spend (S), redundancy (r), under-use (u),
- Ignored-alert share (p) and rework minutes (r_m) after inaction.
- These inputs feed per-user models reported in the paper (see Methodology §3.2; Appendix C).

Section 1 — Introduction for Participants

- Thank the participants for their time.
- Explain that the discussion will focus on their personal experiences with cybersecurity and privacy tools.
- Emphasize that there are no right or wrong answers — we are interested in their honest perceptions and stories.
- Remind them that responses are confidential and will be anonymized in the final report.
- We'll ask for rough estimates of time and spend; exact figures are not required—ranges are fine.
- You may skip any question. We won't collect identifying financial details.
- If comfortable, please share the approximate value of your time (e.g., a band like $20–$30/hour) to help us translate hours into a monetary estimate.

Section 2 — Warm-Up Questions

Technology Use Context

- "Can you tell me a little about your typical daily technology use — devices, internet activities, and any security measures you already have in place?"

Security Tool Awareness

1. "What security or privacy tools are you currently using? How did you choose them?"

Quick Quant Anchors (ranges are fine):

- How many security/privacy tools do you use monthly? How many vendors?
- Paid plans and approx. monthly cost (S): which ones?
- Time per month (t): updates, logins, checks—about how many hours?

Section 3 — Main Discussion Topics

A. Usage Narrative

- "Can you walk me through how you use your security and privacy tools on a typical day or week?"
- Follow-up: "Are there any tools you use only occasionally? Why?"

B. Alert Experiences

Have you ever felt confused or overwhelmed by security warnings or alerts from your apps or tools? Can you share an example?"

Follow-up: "What did you do in that situation?"

Response Behavior

- "When a security tool notifies you of a potential issue, how do you usually respond?"
- Follow-up: "Can you recall a time when you ignored an alert? Why?"

Conflicting or Redundant Tools

- "Have you ever gotten mixed messages from different security tools — for example, one tool saying something is safe while another flags it?"
- Follow-up: "How did you decide what to do?"

Trust and Confidence

- "How much trust do you place in your security tools? Are there some you rely on more than others? Why?"

Security Fatigue

"Do you ever feel worn out or stressed by the number of security-related decisions or alerts you get?"

- Follow-up: "How do you handle that feeling?"

Management Challenges

- "What's the most frustrating part of managing your security tools?"
- Follow-up: "Have you ever disabled or removed a tool because of this frustration?"

Behavioral Trade-Offs

- "Have you ever taken a shortcut or ignored a recommendation that you knew might reduce your security because it was too inconvenient or confusing?"

Ideal Solutions

- "If you could redesign your personal cybersecurity setup from scratch, what would it look like?"

Time and Maintenance (Access/Inertia)

- "Across a typical month, how many hours (t) do you spend on updates, logins, checks, switching between apps?" *(ranges ok)*
- "Which steps consume the most time?" *(logins, re-enabling protections, cross-checking)*
- "If you consolidated tools, how much time could you save per month?" *(Δt h)*
- Moderator note: record t and Δt.

Alerts and Rework (Alerts/Inaction)

- "About how many alerts per month (A) do you notice across tools?"
- "On average, how many minutes per alert (m) to read/decide?"
- "What share are duplicates/conflicts?" (your best guess %)
- "Do you ever ignore/dismiss alerts? Roughly what share (p)?"
- "If ignored, how much rework time (r_m) later (password resets, cleanup)?"
- Moderator note: record A, m, p, r_m; mark duplicates if mentioned.

Spend, Redundancy and Under-Use (Functionality/Gaps)

- "Approximately, what's your monthly/annual spend (S) on security/privacy?"
- "Do any paid tools overlap? Rough % redundancy (r)?"
- "Any tools disabled/unconfigured or paid features you don't use? Rough % under-use (u)?"
- Moderator note: record S, r, u; probe why (confusion, conflicts, effort).

Incidents and Attributions

- "In the past 12 months, any personal security incidents?" (#, brief)
- "Approx direct cost? Hours to resolve?"
- "Did duplicate/conflicting alerts or disabled features contribute?"

Moderator note: capture incident count, $, hours, contributing fragmentation factors.

Section 4 — Closing

- Ask if there's anything else they'd like to share about their experiences with security tools.
- Thank the participant again and explain how their input will help shape the study's findings.
- If consolidation reduced your time by ≥1 h/month, would you switch to a simpler setup?
- *(No/Maybe/Likely/Definitely)*
- "First actions you'd take to reduce duplicates and gaps (remove/enable)? *(prioritize list)*

Moderator Notes (Coding and Quick Math)

Tag taxonomy: [Overload], [DupAlerts], [Conflicts], [Ignored], [Disabled], [UnderUse], [TimeTax], [Redundancy%], [UnderUse%], [HourlyValue], [Alerts/mo], [Min/Alert], [ReworkMin], [Incident$], [IncidentHrs].

Derived variables (for internal use)

$W = S \times (r + u)$, $T = (12 \times t) \times w$, $H = (A \times m \times 12)/60$, $R = (A \times p \times r_{\mathrm{m}} \times 12)/60$, $I = W + T + (H \times w) + (R \times w)$.

End-of-interview checklist: confirm t, A, m, p, r_{m}, S, r, u and (optionally) w (hourly value band).

(Use ranges; no exact accounting required.)

Appendix C — Appendix C — Sampling, Summary Statistics and Excerpts (Individuals)

What's in this appendix (Individuals-first).

- C.1 Sampling and Method — how we recruited and summarized individual users.
- C.2 Summary Statistics (Individuals) — core per-user metrics used in the paper.
- C.3 Monetary Variables and Derived Metrics — definitions and formulas for per-user impact.
- C.4 Qualitative Summary — thematic codes (overload, duplicates, inaction, gaps).
- C.5 Anonymized Excerpts — short quotes with tags.

Sampling and Method

Sample frame and recruitment

We recruited individual users (consumers) via online communities and personal networks. Inclusion: age ≥18, self-managing at least one security/privacy tool on a personal device. Exclusion: dedicated security professionals answering from a work/SOC context.

N = 50 participants; data collected via a short survey (instrument in Appendix A) and semi-structured interviews (guide in Appendix B). Responses were anonymized and aggregated.

Target Population

Individual end-users of cybersecurity and privacy tools, representing a range of demographics, technical proficiency levels, and VPN usage habits.

Inclusion Criteria

- Age 18+
- Uses at least one cybersecurity or privacy tool on a personal device

Segmentation Variables

- Age group (18–29, 30–49, 50–69, 70+)
- Self-rated technical proficiency (Basic, Intermediate, Advanced/IT Professional)
- VPN usage frequency (Never → Daily)

Sampling Method

- Purposive sampling through online forums, tech communities, and mailing lists, aiming for balanced representation across demographics and skill levels.

Sample Size

50 completed survey responses and 16 qualitative interviews.

Measurement focus (per-user)

We captured tool count, duplicates, overload, ignored alerts, time on maintenance, spend, redundancy, under-use. These map to variables $S, r, u, t, A, m, p, r_{\mathrm{m}}$ described in C.3.

Summary Statistics (Individuals) (n = 50)

Note: Enterprise figures in the paper serve only as benchmarks; all metrics below come from our individual sample.

Table C.1 Segment counts

Segment	Count	% of Total
Age 18–29	14	28%
Age 30–49	18	36%
Age 50–69	13	26%
Age 70+	5	10%
Basic Proficiency	15	30%
Intermediate	21	42%
Advanced/IT Pro	14	28%
VPN Daily	11	22%
VPN Regularly	8	16%
VPN Sometimes	13	26%
VPN Rarely/Never	18	36%

Table C.2 Core per-user metrics (survey)

Metric	Value	Notes
Average tools in use	~3.4	AV, VPN, password mgr, browser add-ons, etc.
Duplicate alerts (any)	44%	Self-reported
Cognitive overload (any)	46%	Self-reported
Ignore/dismiss alerts (at least sometimes)	38%	Behavior
Time on maintenance (t)	~2.3 h/month	Updates, logins, checks

Annual out-of-pocket spend (S)	$92	Average
Redundancy (r)	24% of S	Overlapping subscriptions
Under-deployment/Under-use (u)	10–20% of S	Proxy: 29% disabled; 34% unaware
Disabled/unconfigured (any tool)	29%	Binary incidence
Unaware of paid features	34%	Binary incidence

Footnote C.2: Alert throughput variables (A, m, p, r_{m}) are explicitly captured in the *instrument v2* (Appendix A updates). Where not reported in this cohort, we use conservative model defaults in the paper's examples (C.3).

Monetary Variables and Derived Metrics

Variables (from survey/interview)

S = annual spend; r = redundancy (% of S); u = under-use (% of S); t = hours/month on maintenance; w = hourly value; A = alerts/month; m = minutes/alert; p = share of ignored alerts; r_{m} = rework minutes per ignored alert.

Derived metrics

Direct waste: $W = S \times (r + u)$

- Time tax: $T = (12 \times t) \times w$
- Alert review hours: $H = (A \times m \times 12) / 60$; $value = H \times w$
- Ignored-alert rework: $R = (A \times p \times r_{\mathrm{m}} \times 12) / 60$; $value = R \times w$
- Indicative total: $I = W + T + (H \times w) + (R \times w)$

Model defaults for examples (replace with local data if available): S = \$92, r = 0.24, u = 0.10–0.20, t = 2.3 h/mo, $A \approx$ 15/mo, $m \approx$ 3 min, w = \$20–\$30/h, p = 0.01–0.10, r_{m} = 6 min.

Example (baseline):

$W \approx$ \$31–\$40, $T \approx$ \$552–\$828, $H \approx$ 9 h/year ⇒ \$180–\$270; I (baseline, excl. rework) ≈ \$583–\$868 per user/year.

- Average number of security tools used: 3.4
- % receiving overlapping alerts from multiple tools: 44% (n=22)
- % feeling cognitively overloaded by managing tools: 46% (n=23)
- % ignoring/dismissing alerts at least sometimes: 38% (n=19)
- Average monthly time spent managing security tools: 2.3 hours
- Average annual spends on security tools: $92
- % paying for overlapping/duplicative services: 24% (n=12)

Time valuation notes

We convert hours to currency using an illustrative hourly band (\$20–\$30/h) to avoid over-precision. Readers should localize w to regional wage proxies for more accurate per-user figures.

Qualitative Summary

Thematic codes (top)

- [**Overload**] tool upkeep and updates;
- [**Dup Alerts**] duplicates across AV/VPN/browser/OS;
- [**Conflicts**] contradictory messages ("safe" vs "blocked");
- [**Ignored**] clicking away/deferring low-salience alerts;
- [**Disabled/Under Use**] protections off; paid features unknown;
- [**Time Tax**] friction from multiple logins/consoles;

- [**Redundancy% / Under Use%**] perceived overlap and unused value.

Interviews Conducted 16

- 6 Basic proficiency
- 6 Intermediate
- 4 Advanced/IT Pro

Themes Identified

- **Alert Fatigue:** Many respondents felt "numb" to constant alerts.
- **Confusion from Conflicting Alerts:** Users sometimes ignored both tools when faced with contradictory warnings.
- **Tool Management Overhead:** Advanced users mentioned time-consuming updates and compatibility checks.
- **Desire for Consolidation:** Across all skill levels, participants expressed interest in having a single, integrated solution.

Anonymized Excerpts

- **P03 (Basic, Age 50–69):** "I just click away the pop-ups now. I figure if something was really wrong, my computer would tell me differently." *(Theme: Alert Fatigue)*
- **P14 (Intermediate, Age 30–49):** "My VPN tells me a site is fine, but my antivirus blocks it. I don't know which one to believe, so I just close the page and move on." *(Theme: Conflicting Alerts)*
- **P27 (Advanced, Age 18–29):** "Keeping all these tools updated is like a part-time job. One update breaks another program and I have to fix it." *(Theme: Management Overhead)*
- **P41 (Basic, Age 70+):** "I wish there was just one program that did everything, instead of four different ones that keep bothering me." *(Theme: Desire for Consolidation)*

Data Handling and Privacy

No directly identifying data were collected. Free-text was reviewed to remove accidental identifiers. Aggregated results are reported at group level; raw individual responses are not published.