PICUS

BLUE REPORT 2024

The State of Threat Exposure Management

Table of Contents

Introduction 3

Executive Summary 4

Key Findings 5

Key Recommendations 7

Methodology 8

Overall Prevention and Detection Effectiveness Performance 10

Real-World Performance of Cybersecurity Products 13

Uncovering Critical Defensive Gaps with Automated Penetration Testing 15

Detection Rule Effectiveness 17

Performance by Industry 19

Performance by Region 23

Performance by Attack Vector 26

Performance by MITRE ATT&CK Tactic 28

Performance by Threat Group 30

Spotlight on Ransomware Attacks 32

Spotlight on Vulnerabilities 34

Introduction

Now in its second year, the 2024 edition of the Blue Report provides key findings and practical recommendations for cybersecurity professionals by evaluating the effectiveness of current detection and prevention practices. Conducted by Picus Labs, this annual study uses over 136 million attack simulations on The Picus Security Validation Platform to assess the real-world performance of leading security products. These simulations cover a diverse variety of attack vectors, threat groups, ransomware attacks, vulnerabilities, and more – highlighting both progress and ongoing challenges in threat detection and prevention.

This year's report introduces results from the Attack Path Validation (APV) and Detection Rule Validation (DRV) products on the Picus platform, offering deeper observations into organizational preparedness against automated penetration tests and the effectiveness of detection rules in SIEM systems.

The Blue Report 2024 serves as a crucial resource for cybersecurity professionals and decision-makers. It provides perspective into the current state of cybersecurity and recommends Continuous Threat Exposure Management (CTEM) for those working to adopt a holistic approach. By addressing these defensive gaps and optimizing detection and prevention strategies, organizations can enhance their resilience against even the most advanced cyber threats.

Executive Summary

The Blue Report 2024 emphasizes the need for a holistic approach to Continuous Threat Exposure Management (CTEM) to strengthen defenses against cyber threats. While we've seen significant advancements since the 2023 Blue Report, several critical vulnerabilities persist, underscoring the necessity for continuously optimizing your organization's defenses.

Automated penetration tests conducted by Picus Attack Path Validation (APV) revealed that 40% of tested environments had paths leading to domain administrator access, posing severe risks of compromised total network control.

The analysis of attack simulations performed by the Picus Security Control Validation (SCV) revealed notable variability in the real-world performance of leading cybersecurity products. Even top performers in controlled evaluations like MITRE ATT&CK showed differing effectiveness in operational environments, underscoring how critically important it is to continuously validate and fine-tune your security controls.

A bright spot, organizations exhibited significant improvement in prevention effectiveness from last year's report, with scores rising from 59% in 2023 to 69% in 2024. However, detection effectiveness presented mixed results with log scores improving from 37% to 54% year over year, but alert scores actually declining slightly from 16% to 12%. This signals a pressing need for security teams to enhance visibility and alert mechanisms in SIEMs and EDRs. A deeper dive into SIEM system detection rules with Picus Detection Rule Validation (DRV) revealed that most issues are related to log collection (38%) and performance (33%).

Key recommendations from the report include enhancing exposure management through comprehensive validation and continuous fine-tuning of security measures. We strongly suggest organizations adopt a "proactive security" mindset to better manage their exposure to cyber threats. By adopting these strategies, organizations can more effectively protect themselves against evolving cyber threats and enhance their overall security posture.

Key Findings

The Blue Report 2024 provides a comprehensive examination of the current state of threat exposure management. This year's findings reveal several critical vulnerabilities and underscore cybersecurity teams' challenges in maintaining robust defenses against evolving cyber threats. Below are some of the most significant findings from the report:

- **High-Risk Attack Paths**
  The report reveals a significant vulnerability across 40% of tested environments, where attack paths could lead to domain administrator access. Such access gives attackers control over user accounts, security settings, and overall network management, much like having a master key to the network.

- **Prevention vs. Detection Effectiveness**
  Despite achieving a higher Log Score, which rose from 37% to 54%, indicating better data capture and monitoring, the Alert Score fell to 12% from 16% from last year's report. This reduction suggests that increased logging has not translated to improved visibility and faster threat detection. The disparity points to a need for organizations to prioritize optimization across their entire detection engineering pipeline.

- **Variability in Cybersecurity Product Performance**
  We observed a significant variability between the performance of cybersecurity products in controlled environments versus real-world settings. Products that score 100% in evaluations like MITRE ATT&CK can unfortunately exhibit significant effectiveness variability once deployed across diverse operational environments. This underscores the necessity for continuous validation and ongoing fine-tuning.

- **Detection Rule Challenges in SIEM Systems**
  The majority of issues we identified in the detection rules of SIEM systems were related to log collection (38%) and performance (33%). Improper log source consolidation affected 23% of cases, while unavailable (10%) and broken log sources (5%) further deepened detection challenges.

- **Endpoint Security Gaps**
  We found that macOS endpoints were significantly more likely to be misconfigured or correctly operate without Endpoint Detection and Response (EDR) tools. As a result, they prevented only 23% of simulated attacks, compared to 62% and 65% for Windows and Linux endpoints, respectively. This underscores a substantial gap in IT and security teams' skill sets and strategies for securing macOS environments.

- **Ransomware Defense Challenges**
  We found that BlackByte was the most challenging ransomware variant to defend against, with only 17% of organizations successfully preventing it. BabLock and Hive followed closely behind, with prevention rates of 20% and 30% respectively, indicating the need for organizations to develop even stronger ransomware defense strategies.

- **Easy to Crack Passwords**
  In 25% of environments, attackers could successfully crack at least one dumped password hash, converting it into a cleartext password.

Key Recommendations

The Blue Report 2024 highlights several critical areas that require attention to enhance organizations' cybersecurity defenses. Based on our in-depth findings and analysis, we propose the following key recommendations for organizations to strengthen their threat exposure management:

✔ Adopt a Proactive Security Mindset

If you haven't already, it's definitely time to shift from a reactive to a proactive and continuous approach to cybersecurity. This involves constantly identifying and mitigating potential threats and vulnerabilities before they can breach, infiltrate, or otherwise attack or compromise your organization.

✔ Implement Continuous Threat Exposure Management (CTEM)

Establish a comprehensive CTEM program to continually identify, prioritize, validate and fix exposures. This helps in maintaining a robust security posture even as the threat landscape continues to evolve.

✔ Enhance Detection and Prevention Mechanisms

Improve detection capabilities by optimizing the entire detection engineering pipeline, including log collection, performance, and alert mechanisms in SIEM and EDR systems. Regularly review and update detection rules to ensure they remain effective against the latest threats.

✔ Strengthen Ransomware Defenses

Implement the latest, most effective backup and recovery solutions and ensure that all endpoints have up-to-date security controls. Conduct regular simulations of ransomware attacks to test and improve the effectiveness of your response strategies.

✔ Improve Endpoint Security Configuration

Ensure that security controls on all endpoints, including macOS systems, are properly configured and that appropriate EDR tools are in place. Conduct regular audits and endpoint security assessments to identify and fix any misconfigurations.

✔ Enhance Log Management and Analysis

Address common issues in log collection and performance to improve the effectiveness of detection rules in SIEM systems. Double check proper log source consolidation and availability.

✔ Prioritize Password Security

Implement strong password policies and confirm that your password hashing methods are robust to prevent easy cracking of password hashes. Regularly audit and enforce your compliance with best practices for password security across your organization.

Methodology

The findings in this report are based on the results of simulated attack scenarios executed by Picus Security customers from January to June 2024. The data has been anonymized and aggregated from over 136 million attack simulations. Research and analysis was completed by Picus Labs and Picus Data Science teams.

Definitions

Prevention Effectiveness evaluates an organization's ability to block potential cyberattacks through its security controls. This metric is the percentage of successfully prevented attacks out of all simulated attacks executed. For example, an effectiveness score of 80% means that 80 out of every 100 simulated attacks were effectively prevented. A high prevention effectiveness score indicates strong security controls that significantly lower the risk of successful breaches. Conversely, a low score highlights gaps in an organization's security measures, suggesting the need for security teams to conduct a thorough review and enhance their controls.

Detection Effectiveness assesses an organization's capability to identify potential cyber threats through its existing security controls. This report uses two key indicators for evaluating detection performance: Log Score and Alert Score.

- **Log Score:** This measures the percentage of simulated attacks where the attackers' behavior was logged. A higher log score demonstrates the efficacy of monitoring controls like SIEMs in capturing a large volume of events and identifying threat indicators. Effective logging is crucial for maintaining a comprehensive security posture and understanding attack patterns.

- **Alert Score:** This indicates the percentage of simulated attacks that generate alerts. High alert scores are crucial for ensuring that security teams are promptly informed of any and all threats, enabling them to take immediate action to neutralize potential risks. Alerts serve as critical triggers for initiating a timely and effective response to attacks.

Scoring Legend

Results are color-coded and categorized into five distinct levels of threat exposure management: Inadequate, Basic, Moderate, Managed, and Optimized (see table below). This classification provides a clear, visual representation of an organization's cybersecurity effectiveness, facilitating easy benchmarking and identification of areas for improvement.

Legend	Range	Description
Optimized	90-100%	Organizations with optimized security controls continuously monitor, refine, and update them to keep up with the evolving threat landscape and maintain their edge in exposure management.
Managed	70-89%	Managed security controls offer a high level of protection against a wide range of threats, significantly reducing the risk of successful attacks. Organizations at this level should maintain their strong security posture, regularly assess the effectiveness of their controls and address identified gaps in exposure management.
Moderate	40-69%	Moderate security controls provide a reasonable level of protection against various threats. Organizations at this level should continue to refine their security controls and consider additional measures to further reduce their threat exposure.
Basic	20-39%	Basic security controls offer limited protection against a narrow range of threats. Organizations at this level should invest in enhancing and expanding their security controls to achieve a more effective threat exposure management program.
Inadequate	0-19%	Inadequate security controls provide almost no protection to minimal protection against threats, leaving the organization highly vulnerable to attack. At this level, only a few basic security measures are in place. Organizations with this level of exposure need to urgently review and improve their security posture.

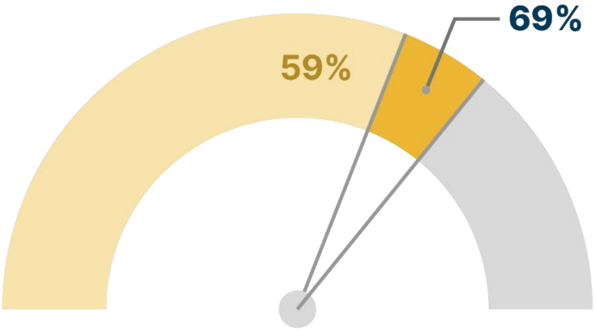
Threat Exposure Management Scoring Legend

Overall Prevention and Detection Effectiveness Performance

This year's report highlights a complex landscape for cyberattack prevention and detection within organizations. While there was noticeable progress in some areas, other critical aspects reveal ongoing challenges for even sophisticated global organizations. And while we saw promising advancements which reflect organizations' efforts to enhance their cyber defenses, the deficiencies we've identified underline the fact that for most organizations, there is still a long road ahead. This is likely less about the quality or capability of the security controls they have in place and more about how effectively these organizations are utilizing the tools in their cybersecurity arsenal. This is usually due to factors such as skill gaps and challenges in integrating and managing disparate security technologies.

Prevention Effectiveness

In 2024, we observed a significant improvement in organizations' overall ability to prevent cyberattacks. The average prevention effectiveness score rose from 59% in 2023 to 69% this year. This indicates that preventive security controls, such as IPS, NGFW, and WAF solutions are now preventing nearly seven out of every ten simulated attacks. This positive trend means that organizations are successfully refining their preventive measures, and improving their overall threat exposure management. To sustain and build on this progress, we strongly recommend organizations to continually identify and address any remaining gaps in their security controls.



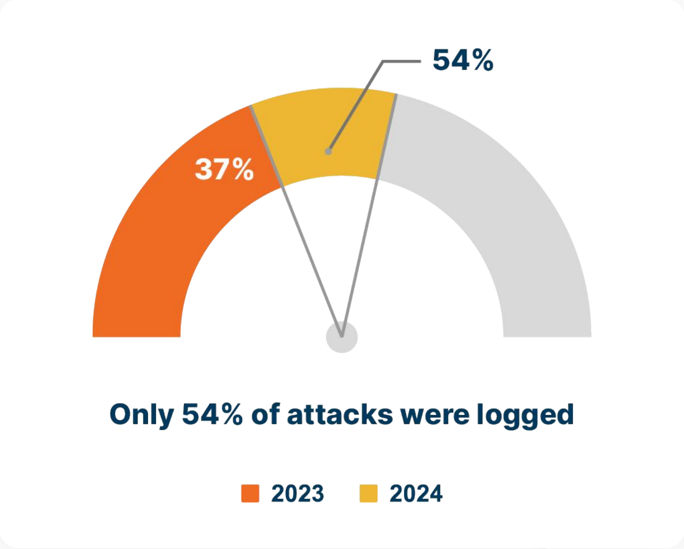
Only 69% of attacks were prevented

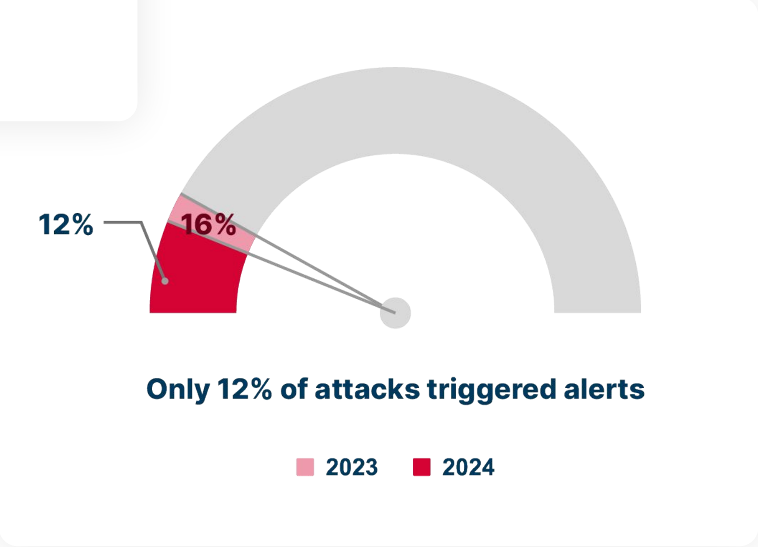
Detection Effectiveness

In 2024, the state of detection effectiveness among security organizations exhibited both progress and setbacks across the various levels of threat exposure management. On the positive side, there was a noticeable improvement in the logging of attacks, with the average log score increasing from 37% to 54%. This improvement suggests that over half of the simulated attacks are now being successfully logged after infiltrating environments, moving many organizations from the "basic" level into the "moderate" category of detection effectiveness.

However, this advancement in logging capabilities was accompanied by a decline in alerting effectiveness. The alert score fell to a concerning 12%, down from 16% in 2023. This means that less than 1 in 8 attacks successfully trigger alerts, which significantly decreases security teams' ability to identify and respond promptly to potential threats. This drop off points to a significant lag in detective security controls to manage the increased log volume and sheer number of attacks detected.

Despite the improved logging capabilities, the failure to convert these logs into actionable alerts is a glaring issue that requires immediate attention. Enhancing alert mechanisms is crucial to ensure that security teams are adequately informed of potential threats, enabling them to quickly and effectively respond.





Addressing the Gaps

Based on our experience with security validation, we feel many organizations might be driven by a false sense of security. Despite improvements in logging attacks, the significant decline in alerting effectiveness underscores a critical gap:

More logs do not necessarily equate to more visibility or better security outcomes.

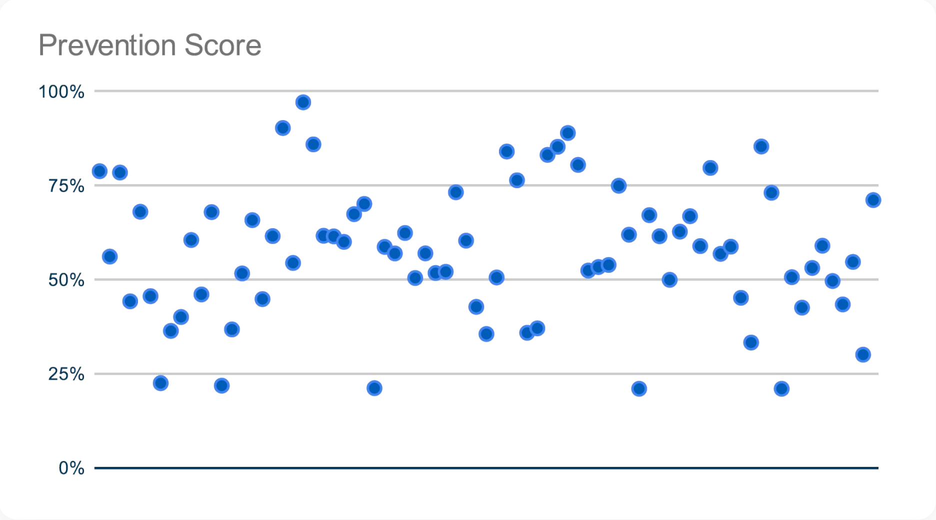
While organizations have improved the data layer, detection engineering remains deficient, highlighting the urgency for security teams to enhance alert mechanisms to ensure they’re quickly identifying and responding to potential threats.

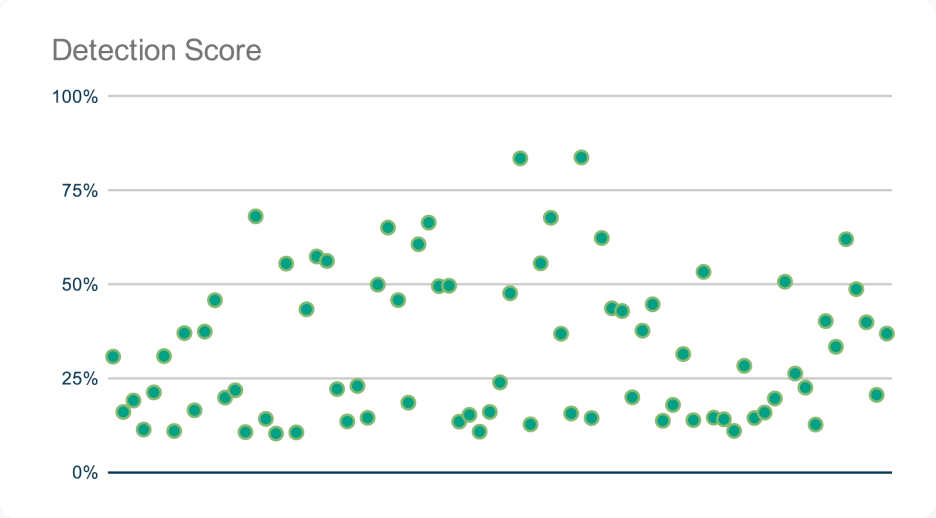
Organizations should adopt an "assume breach" mindset to bridge these gaps in their cybersecurity strategy. This approach emphasizes the importance of not only relying on your organization’s preventive controls but also ensuring that your detection and response mechanisms are strong enough to manage breaches when they occur. Proactive measures, continuous monitoring, and regular evaluations of both logging and alerting systems are vital to achieving higher levels of threat exposure management and solidifying your security posture.

Real-World Performance of Cybersecurity Products

In the competitive cybersecurity landscape, products usually undergo rigorous evaluations to assess their effectiveness against simulated attack scenarios. One such highly regarded benchmark set is the MITRE Engenuity ATT&CK® Evaluations, where numerous security products have achieved a commendable 100% in both prevention (protection) and detection coverages. However, real-world performance data from various production environments unfortunately tells a different story, illustrating significant variability in the effectiveness of these security solutions.

MITRE ATT&CK® Evaluations provide a controlled environment to assess a product's capabilities against predefined tactics and techniques. And while these evaluations are critical to understanding the potential efficacy of different security solutions, they do not fully capture the unique complexities and diverse conditions found in the wild within actual operational environments.





Real-world data shows that even best-of-breed products that score 100% in controlled settings can exhibit a wide range of prevention and detection effectiveness once deployed. We attribute this variability to several factors:

1. **Environmental and Configurational Differences:** Each organization's network architecture, regulatory and compliance needs, threat landscape, and user behavior are all unique. These differing environments can significantly impact the performance of security products, leading to variations in effectiveness across different organizational deployments.

2. **Context and Deployment Nuances:** Where and how a cybersecurity solution is implemented, including its integration with other security tools, policies, and specific configuration settings, play a vital role in determining its real-world effectiveness. The same product might perform exceptionally well in one setup but face unexpected limitations in another.

3. **Dynamic Nature of Threats:** The cyber threat landscape is always morphing and mutating, with new TTPs emerging regularly. Security products need to be continuously validated against these latest global threats to ensure they remain effective. This requires companies regularly update and fine-tune their cybersecurity solutions to maintain the strongest, most effective posture.

Given this variability, organizations should have realistic expectations when implementing security solutions, even those that perform exceptionally well in standard evaluations. We strongly recommend you conduct comprehensive, context-specific evaluations. Then, pivot to continuously monitoring and tuning these tools to ensure they remain effective against the most current threats. This approach leads us to offer three critical recommendations:

1. **Continuous Validation:** Organizations must regularly test and validate their security products against the latest threats to confirm that they provide the expected level of protection. Regular attack simulations can help identify potential gaps and areas for improvement.

2. **Ongoing Fine-Tuning:** Security tools should not be considered set-and-forget. Continuous fine-tuning and updates are essential to adapt to changing threat landscapes and organizational needs. This includes adjusting configurations, updating threat intelligence feeds, and integrations with other security tools.

In conclusion, while achieving 100% protection and detection coverage in MITRE ATT&CK Evaluations signifies a product's potential, it does not guarantee absolute security in real-world deployments. Organizations must remain vigilant, continuously validate their security measures, and adapt to the evolving threats to ensure their cybersecurity defenses remain robust and effective.

Uncovering Critical Defensive Gaps with Automated Penetration Testing

Recent assessments utilizing the Picus Attack Path Validation (APV) have yielded critical insights into the security postures of various organizations. Picus APV, a cutting-edge automated penetration testing solution, identifies the shortest paths that attackers might exploit to gain domain administrator privileges and mimics real-world adversarial actions to validate these paths as exploitable. Given the elevated access that domain administrators hold - managing user accounts, modifying security settings, and overseeing entire network environments- the compromise of these credentials poses severe risks such as data exfiltration, malware deployment, or operational disruptions.

In a sobering revelation, Picus APV was able to successfully achieve domain administrator status in 24% of the tests conducted. To put this into perspective, out of every 100 tests performed, Picus APV managed to gain domain administrator rights in 24 of those tests. This statistic underscores the significant defensive gaps lurking within a substantial portion of the organizations we assessed. These findings suggest that a quarter of the evaluated scenarios revealed weaknesses severe enough to allow an attacker to reach the highest level of privileged accounts.

Even more alarming, automated penetration test assessments performed by Picus APV revealed that in 40% of the tested environments, there was at least one instance where domain administrator access was achieved. Put another way, for 40 out of every 100 organizations assessed, there was a successful path for an attacker to gain domain administrator rights.

Typically, these attack paths begin with actions like dumping a regular user's hash and cracking it, followed by privilege escalation. The attacker then moves laterally to other machines using the newly obtained privileges. Each step in this process acts like a domino, setting off a chain reaction of compromises that culminates in creating a new domain administrator user. This sequence exemplifies how automated tools, coupled with the cumulative effect of many small vulnerabilities, can lead to a full compromise of the network, highlighting widespread critical security issues rather than isolated incidents.

Picus APV incorporates the capability to crack dumped password hashes, a technique often employed by malicious actors to gain unauthorized access to systems. An eye-opening 25% of the environments tested revealed that attackers were able to successfully crack these password hashes, converting them into cleartext passwords. The fact that a quarter of organizations had their password hashes cracked points to serious deficiencies in their existing password policies. Weak, easily guessable passwords leave systems exposed to such attacks. Once attackers obtain cleartext passwords, they can use them to move laterally within the network or escalate privileges, compounding the threat.

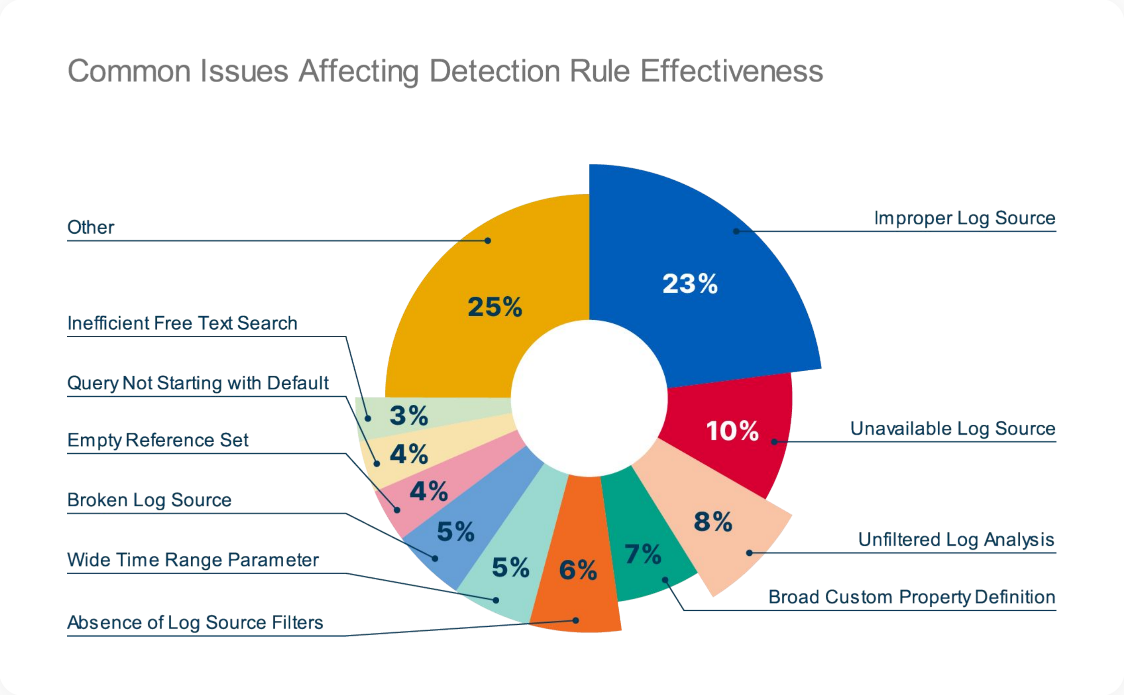
Much like real-world Advanced Persistent Threat (APT) attacks designed to evade detection, Picus APV employs an Intelligent Decision Engine. This AI-powered algorithm identifies the shortest and most high-risk paths an evasive attacker might exploit, mirroring the behavior of today's most sophisticated attackers. By operating covertly and effectively, Picus APV highlights the significant challenges involved in detecting and mitigating these types of threats in real-time scenarios.

Overall, these findings underscore the urgent need for organizations to reassess and strengthen their security controls, focusing particularly on the critical areas of privilege escalation, credential access, and lateral movement.

Detection Rule Effectiveness

Detection rules are crucial for threat identification and response in Security Operations Centers (SOCs), acting as the "eyes and ears" of cybersecurity. Ensuring these rules function correctly can be challenging due to the lack of advanced validation mechanisms in SIEMs, which can result in undetected threats and a dangerously false sense of security.

In the analysis of common issues in detection rules, and the issues impacting detection rules in Security Information and Event Management (SIEM) systems, we identified several concerns as both particularly prevalent and critical. This section synthesizes these findings, highlighting the most significant issues, their frequency, and their potential impact on performance and security.



Common Issues Affecting Detection Rule Effectiveness

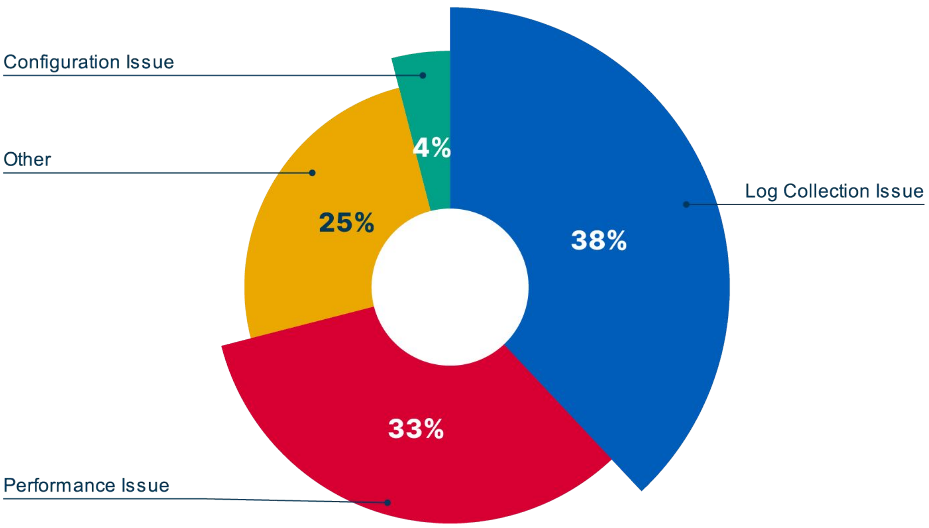
The most common issue we found was **Improper Log Source Consolidation**, affecting 23% of the study’s cases. This problem occurs when event coalescing is enabled for specific log sources such as DNS systems, proxy servers, Windows servers, and endpoints, leading to data loss. While disabling event coalescing can address this issue, it may negatively impact system performance and increase your storage needs.

Log source availability issues also stood out, with **Broken Log Source** and **Unavailable Log Source** errors appearing in 5% and 10%of cases, respectively. Both issues are marked by high criticality. Unavailable Log Source problems arise when log sources stop sending logs due to various reasons, such as network or log service disruptions. Similarly, Broken Log Source issues occur when log sources are disabled, rendering the related detection rules ineffective. Both scenarios significantly decrease the ability to generate alerts and can leave organizations unaware of – and vulnerable to – undetected threats.

Performance-related problems were another critical area we identified, and though individually, they were relatively uncommon, they collectively made up a substantial portion of our observed issues. **Unfiltered Log Analysis**, found in 8% of cases, degrades system performance by examining large volumes of logs without proper filters. **Broad Custom Property Definition** (7%) and **Absence of Log Source Filters** (6%) both also contribute to unnecessary resource consumption and decreased system efficiency. Similarly, **Wide Time Range Parameters** (5%) and queries that do not start with **Default Fields** (4%) delay response times and negatively impact performance. **Free Text Search** (3%), another performance-related issue, further strains resources and slows system operations.

Lastly, a notable configuration issue, **Empty Reference Set**, was identified in 4% of cases. This high-criticality problem occurs when reference sets used within rules are empty or not dynamically updated, leading to malfunctioning rules and again, potential security gaps.

Common Issue Types in Detection Rules



The dataset for these statistics is sourced from Picus Detection Rule Validation (DRV), which includes a continuously updated checklist identifying over 50 common issues in detection rules. The data underscores the varied challenges in maintaining effective detection rules within SIEM systems. The prevalence of **log collection issues** (38%), **performance problems** (33%), and other problems (29%) such as **configuration errors**, reinforce the need for continuous testing, fine-tuning, and updating your security rules to ensure optimal performance and security posture. By addressing these common issues, security teams can significantly improve the efficiency of their detection apparatus.

Performance by Industry

In this section, we examine the prevention and detection effectiveness across various industries, highlight significant changes, year on year, and identify the most and least successful industries. Our analysis offers a comprehensive view of how different sectors are performing in their efforts to prevent and detect cyberattacks.

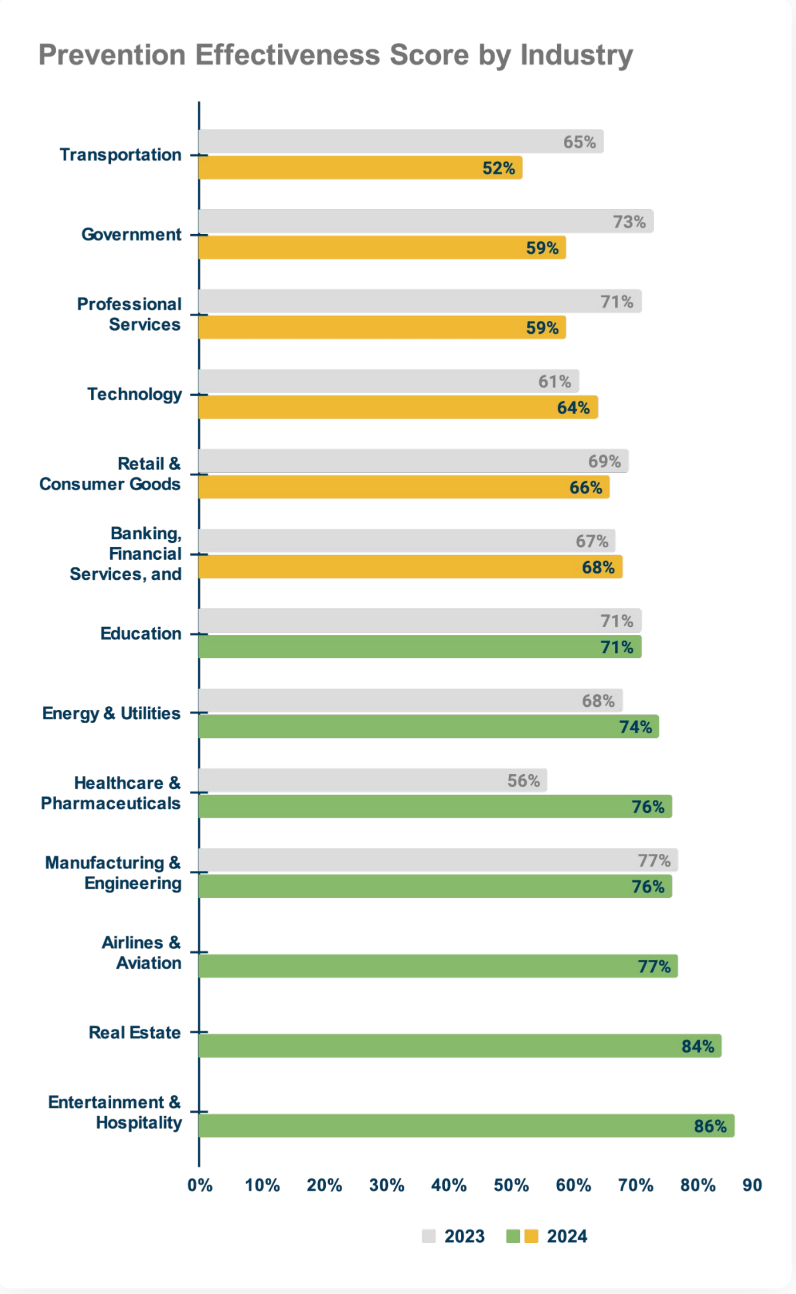
Prevention Effectiveness

In 2024, we observed notable shifts in prevention effectiveness across various industries. The **Healthcare and Pharmaceuticals** sector showed the most dramatic improvement, increasing from 56% in 2023 to 76% in 2024 – an impressive 20% leap. Similarly, the **Energy and Utilities** sector saw a smaller but still significant rise from 68% to 74%. Both sectors highlight the impact of companies' effective security validation on their overall security posture.

On the other hand, some sectors experienced unfortunate declines. Worryingly, **Government** dropped significantly from 73% to 59%, and **Professional Services** fell from 71% to 59%.

Several sectors performed exceptionally well, with **Entertainment & Hospitality** leading the way at 86%, followed by **Real Estate** at 84%. **The Airlines/Aviation** sector also scored strongly at 77%, implying effective preventive measures in these areas.

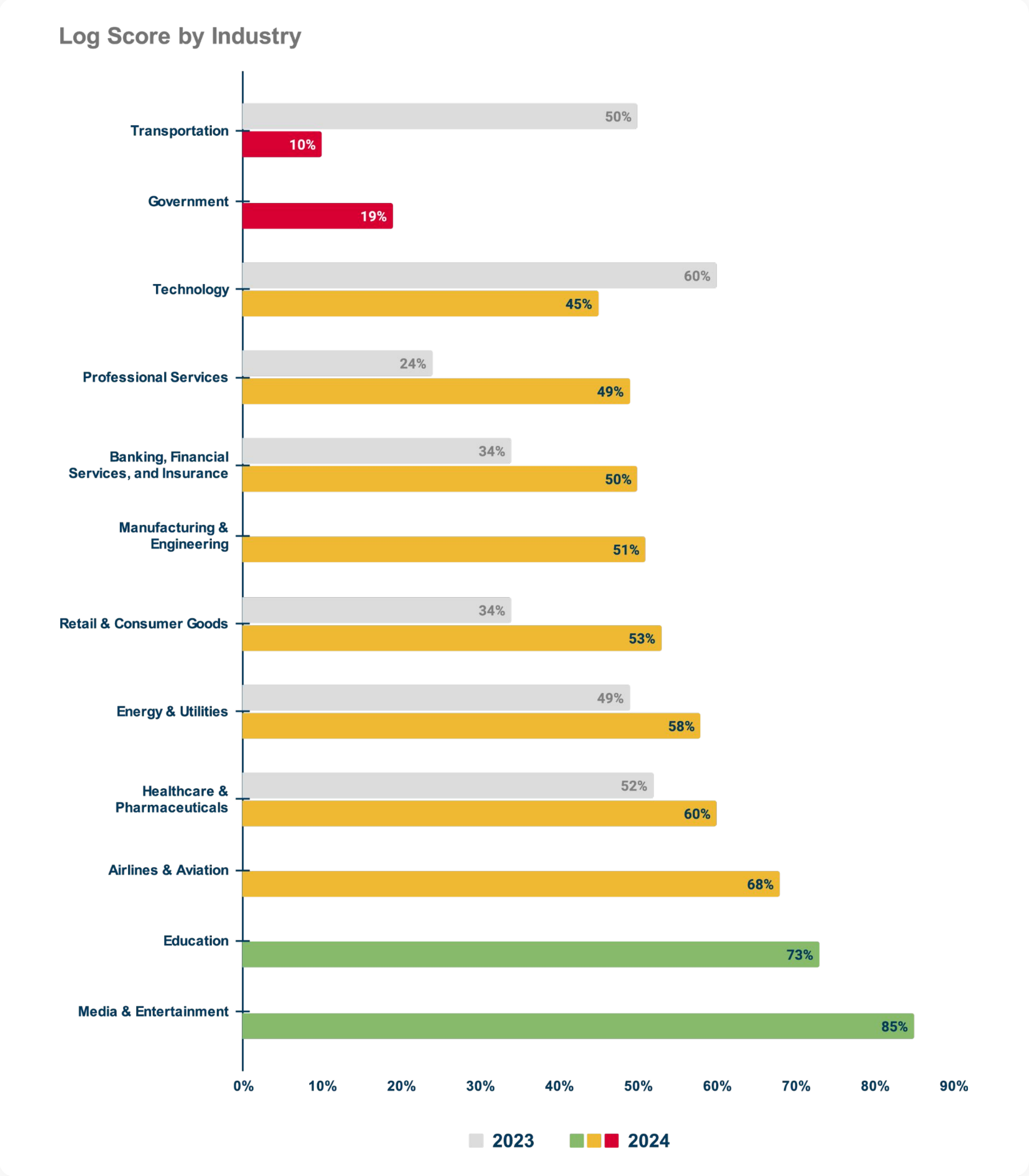
Other sectors maintained steady performance, such as **Education**, which held a consistent score of 71% across both years, and **Banking, Financial Services, and Insurance (BFSI)**, which saw a slight increase from 67% to 68%.



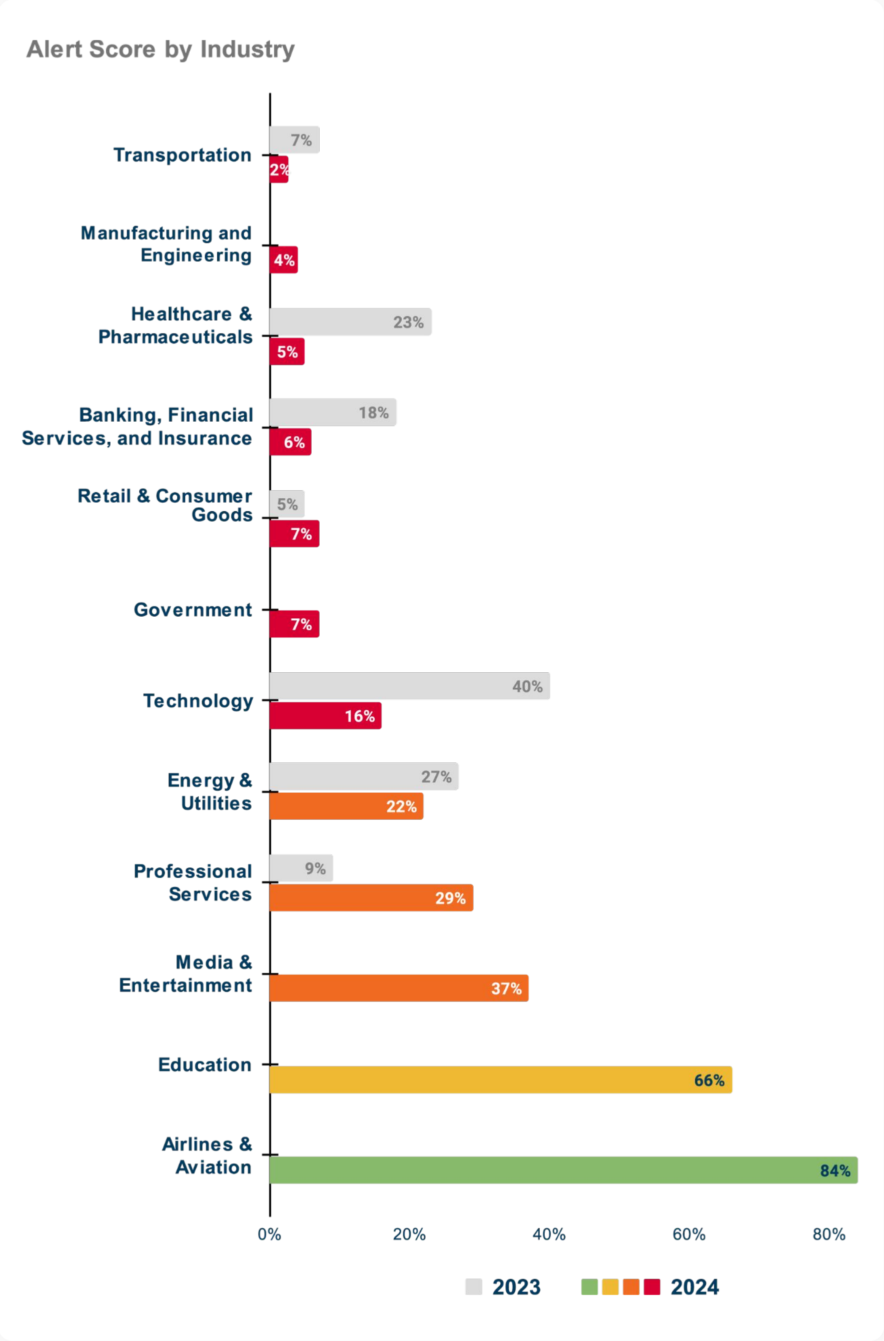
Detection Effectiveness

Similar to prevention effectiveness, detection scores across industries are shaped by regulatory requirements, the sensitivity of the data being examined, organizations' level of technological adoption, their cybersecurity expertise, and organizational culture. Industries that face higher risks generally have more stringent regulations, demonstrate a solid commitment to cybersecurity, and typically exhibit better scores, reflecting their enhanced cyber defense capabilities.

Detection effectiveness is measured by organizations' ability to log and alert on attacks. As previously noted, the average security organization only logs 54% of attacks and alerts on 12% of attacks. However, there are significant differences in detection proficiency between industries.



Reflecting on the past year, there have been significant shifts in the cybersecurity landscape across various industries. The results continue to show a broad disparity in the capacity of different sectors to detect and respond to cyber threats.



The **Healthcare and Pharmaceuticals** industry, which led in detection effectiveness in 2023, has continued to perform strongly in 2024. Its log score increased from 52% to 60%, though its alert score decreased markedly, from 23% to 5%. This drop in alert score is quite concerning and indicates a growing gap between threat logging and actionable alerts, a trend we're unfortunately seeing across several industries this year.

Notably, the **Media and Entertainment** industry emerged as the leader in detection effectiveness in 2024 with an impressive log score of 85% and an alert score of 37%. This surge may reflect an increased focus on cybersecurity due to rising threats against high-profile media assets and intellectual property.

Meanwhile, industries such as **Transportation and Logistics**, which had already shown low detection performance in 2023, have sadly seen a further decline. The transportation industry's log score plummeted to a worrying 10% and its alert score to a meager 2%. This significant drop from the previous year's figures of 50% and 7% respectively, signifies pressing challenges that are not being addressed to enhance security controls.

The **Professional Services** industry has made substantial improvements, with a log score rising to 49% from 24% and an alert score increasing to 29% from the previous 9%.

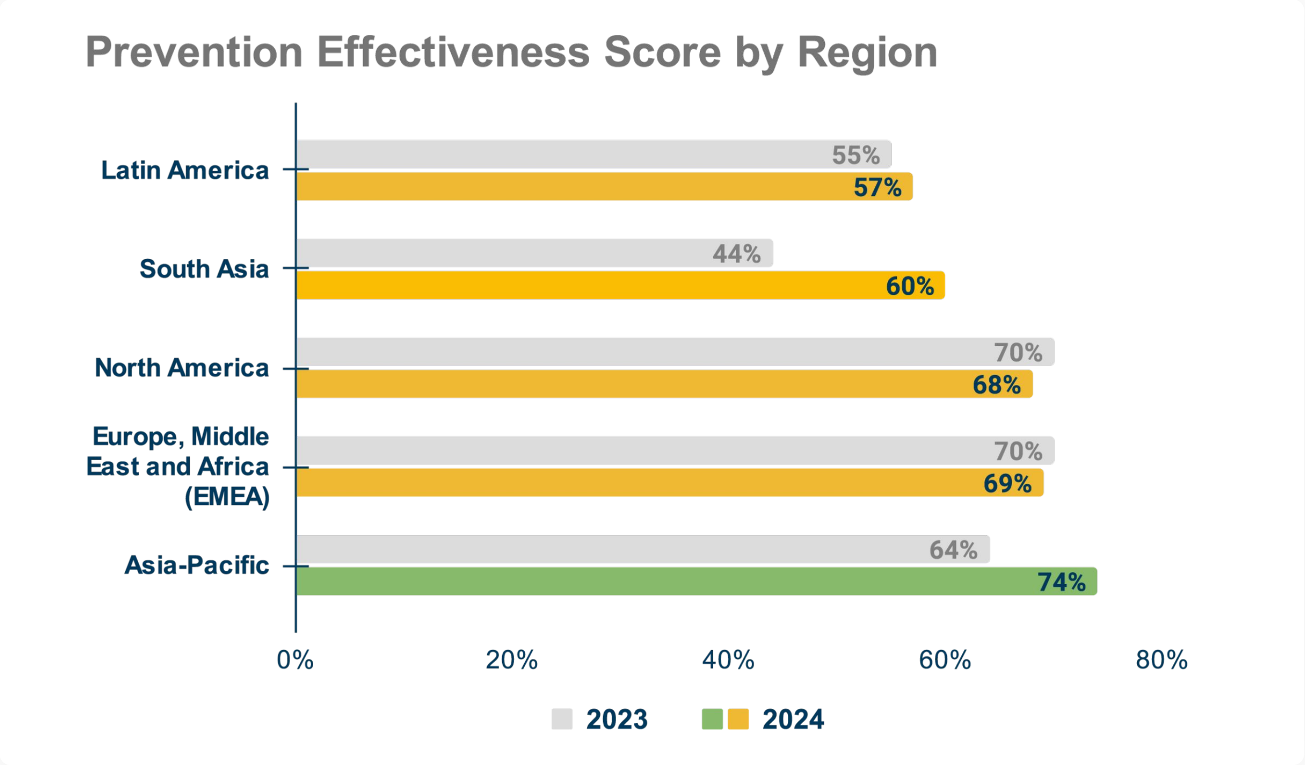
Industries like **Education and Aviation** have achieved high log scores of 73% and 68% respectively and also exhibit alert scores of 66% and 84%. This trend indicates that these sectors are proficient both in recording threat activities and converting those log scores to actionable alerts.

In conclusion, while 2024 has seen improvements in log scores across many sectors, the decline in alert scores and the persistent log-alert chasm present ongoing challenges. These findings underscore the importance for organizations to not only log threats effectively but also to convert these logs into actionable intelligence quickly and efficiently, ensuring the strongest holistic cybersecurity posture.

Performance by Region

Prevention Effectiveness

The 2024 data surfaced notable regional disparities in threat readiness, influenced by factors such as uneven economic development, varying digital maturity, access to skilled professionals, and governmental focus on cybersecurity regulations.



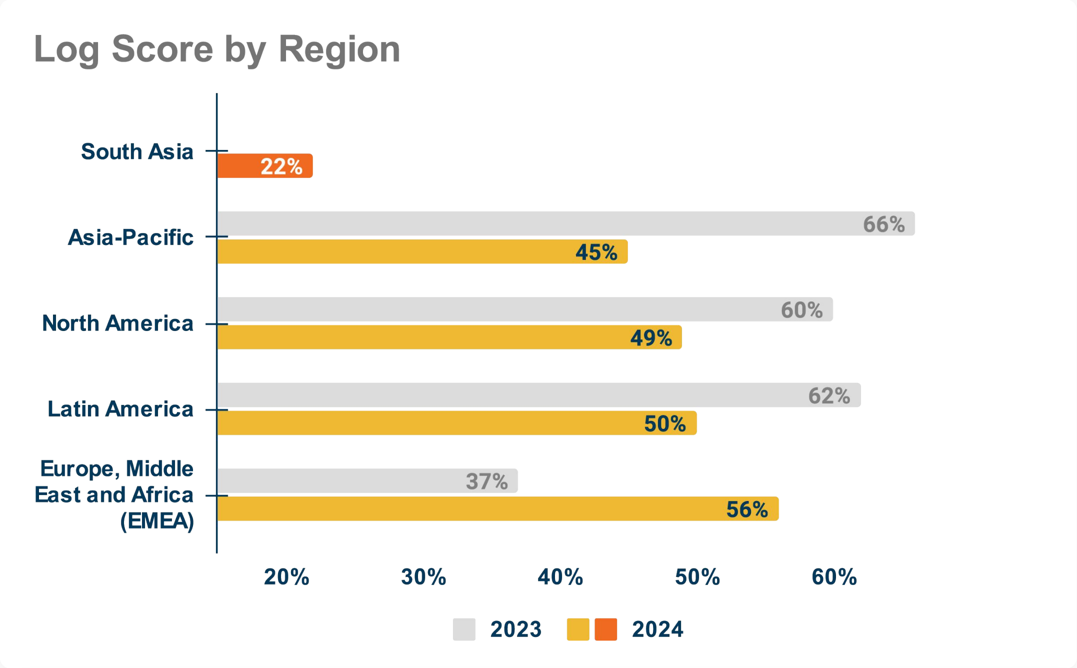
South Asia showed the most significant improvement, with prevention effectiveness rising from 44% in 2023 to 60% in 2024. This indicates progress in strengthening security defenses, although we believe further enhancements are still needed.

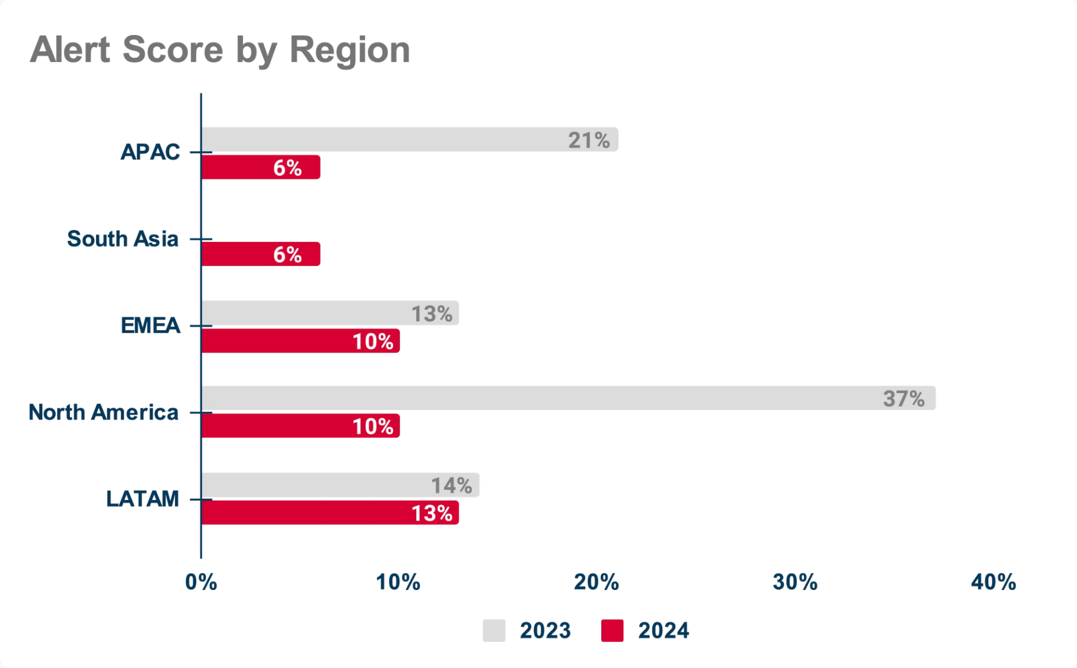
Asia-Pacific (APAC) also demonstrated considerable progress, increasing from 64% to 74%. This improvement positions the region as a leader in threat protection, reflecting its growing digital maturity and commitment to cybersecurity. Conversely, **North America** and **Europe, Middle East and Africa (EMEA)** saw slight declines, from 70% to 68% and 69%, respectively. Despite the minor drops, these regions maintain a managed level of threat protection, emphasizing the need for ongoing investment to stay ahead of evolving threats.

Latin America (LATAM) experienced a modest increase, improving from 55% to 57%. While positive, this small improvement underscores the need for continued efforts to enhance regional cybersecurity measures.

Detection Effectiveness

This year's assessment of detection effectiveness across different regions reveals noticeable shifts compared to 2023.





Asia-Pacific (APAC) saw a considerable decline in its detection capabilities. The log score dropped significantly across the region from 66% in 2023 to 45% in 2024. The alert score also fell, from 21% to 6%. This decline suggests that APAC organizations may have faced challenges in maintaining their detection mechanisms or that new threats and vulnerabilities have not been adequately addressed, necessitating a more focused investment in alerting systems and thorough log evaluation.

Newly included in this year's analysis, **South Asia** reported a concerning initial log score of 22% and an alert score of 6%. These low scores highlight the need for significant improvements in the region's cybersecurity infrastructure and practices. We recommend organizations in South Asia prioritize strengthening their logging and alert systems to better detect and respond to cyber threats.

The **Europe, Middle East and Africa (EMEA)** region displayed promising improvements in logging capabilities, with the log score increasing from 37% in 2023 to 56% in 2024. However, the already low alert score decreased slightly from 13% to 10%, emphasizing a persistent challenge in converting logged incidents into actionable alerts. This suggests that while EMEA organizations are getting better at monitoring, their alerting mechanisms need further optimization to ensure timely threat response.

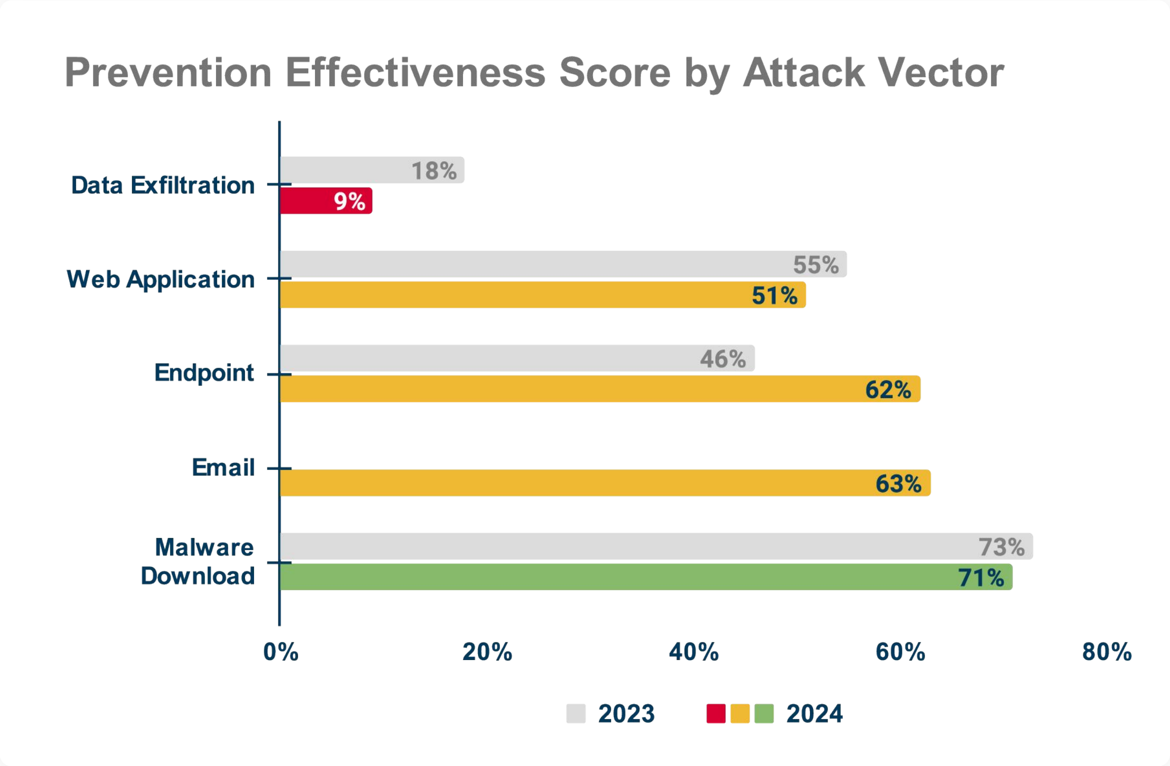
North America recorded a notable decrease in both logging and alerting abilities. The log score fell from 60% in 2023 to 49% in 2024, and the alert score plummeted dangerously, from 37% to 10%. This significant drop indicates that, as a group, North American organizations need to revisit their detection controls and bolster their monitoring and alerting systems.

The **Latin America (LATAM** region also experienced declines, though they were less severe. The log score fell from 62% to 50%, and the alert score clicked down from 14% to 13%. While LATAM's decreases are less drastic than other regions, they still reflect a need for ongoing investment in improving detection and alerting capabilities.

Across all regions, the data highlights a consistent trend: alert scores are almost universally significantly lower than log scores. This gap suggests that while many organizations are capturing threat events, they are not effectively converting these logs into actionable alerts. Issues such as an overwhelming number of false positives, improper tuning of alerting mechanisms, and difficulty in correlating and prioritizing security events could all be contributing factors.

Performance by Attack Vector

Organizations' ability to prevent attacks continues to vary widely depending on the type of cyberattack being targeted. The 2024 data presents a mixed picture, indicating both improvements and areas that still need urgent attention.

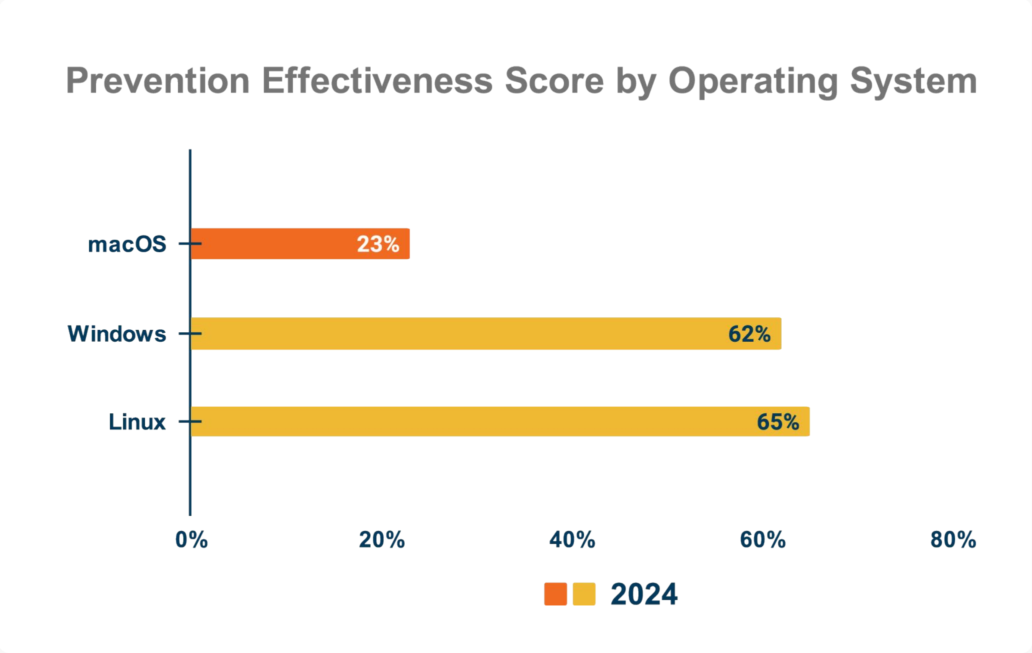


One of our most concerning findings relates to **Data Exfiltration**. The effectiveness rate in preventing these attacks dropped drastically from an already low 18% in 2023 to just 9% in 2024. This worryingly low score underscores the ineffectiveness of current cybersecurity controls in stopping the unauthorized export of sensitive data. Given the severe financial, legal, and reputational repercussions of data breaches, we believe that enhancing defenses against data exfiltration should absolutely be a top organizational priority.

Happily, we saw significant improvements in several other attack vectors. **Endpoint** attacks showed notable progress, increasing from 46% to 62% in 2024. This improvement suggests that organizations are becoming better equipped to handle complex, multi-stage attacks, which are growing in both prevalence and sophistication.

Email attacks have a prevention effectiveness score of 63%, indicating a reasonably solid stance against email-based threats, which are among the most common vectors for phishing and malware distribution.

However, not all attack vectors saw significant improvements. **Web Application** attacks experienced a slight decline from 55% in 2023 to 51% in 2024. And given that web platforms are fundamental to modern business operations, this dip is unsettling and suggests that security teams need to focus more on securing web applications against increasingly sophisticated threats. **Malware Download** attacks remained relatively stable, with a score of 71% in 2024, which was a slight decrease from 73% in 2023. This consistency indicates that organizations have maintained an effective defense against these types of attacks, although ongoing vigilance is still required.

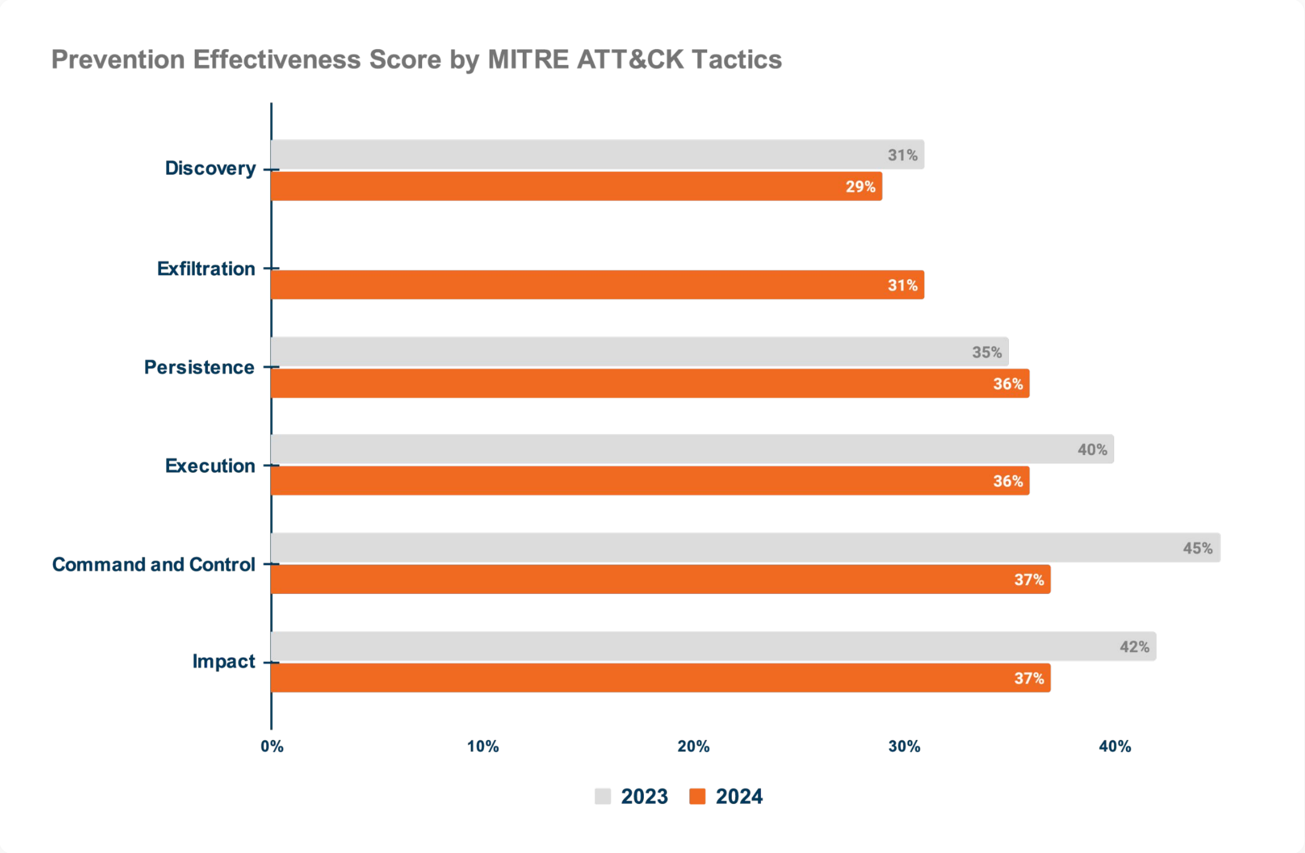


When breaking down **Endpoint** attack prevention performance by operating system, the data reveals varied outcomes. In contrast, **macOS** attacks show a concerning prevention effectiveness score of 23%. This highlights a potential gap in endpoint security controls on modern macOS environments that needs immediate attention. In contrast, **Windows** attacks showed substantial improvement, achieving a prevention effectiveness score of 62%, and **Linux** attacks scored 65%, both indicating strong defensive measures in these environments.

Overall, the 2024 figures suggest that while organizations have made progress in defending against certain types of cyber threats, substantial gaps still remain. The drastic drop in data exfiltration prevention effectiveness is especially troubling and highlights most organizations' need for dedicated resources and strategies to address this critical vulnerability area. The declines in web application defenses and the low score for macOS endpoint attacks call for a renewed focus on securing these key areas. Organizations need to find new ways to better manage and mitigate evolving threats across all attack vectors.

Performance by MITRE ATT&CK Tactics

Many modern security organizations rely on the MITRE ATT&CK framework to understand attack behaviors and evaluate their own threat readiness. In our analysis, we examined organizations' ability to defend against the 14 attacker tactics outlined in the MITRE ATT&CK enterprise matrix.



In 2023, the **Discovery** tactic proved to be the most challenging for organizations to defend against, with a prevention effectiveness of only 31%. In 2024, discovery dropped further to 29%, indicating a slightly increased vulnerability in this already troubled area. The consistent struggle with Discovery suggests a need for new detection measures to identify and counter bad actors' reconnaissance activities. We recommend enhancing network monitoring and deploying advanced threat detection technologies as crucial steps organizations need to take to address this gap.

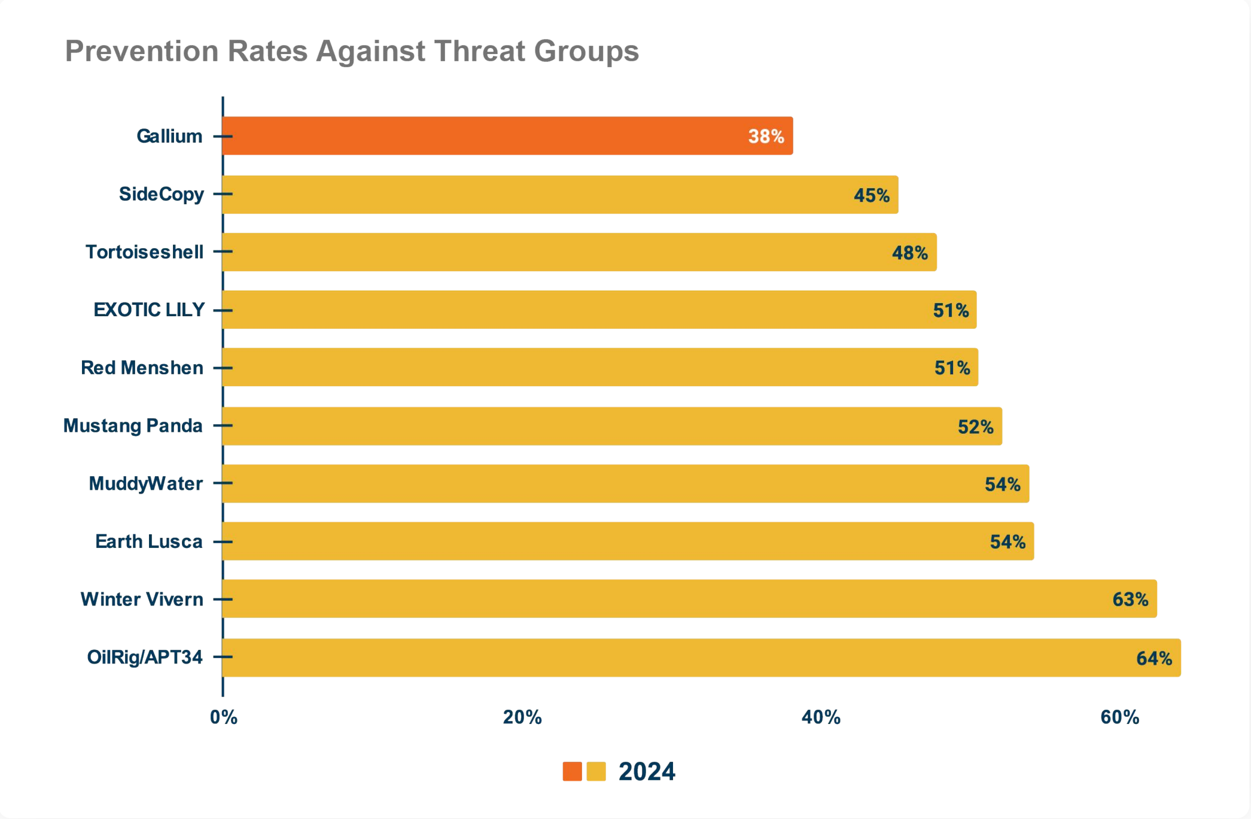
The 2024 data reveals a shift in the landscape, with **Exfiltration** joining the ranks of the least prevented MITRE ATT&CK tactics, scoring only 31% in prevention effectiveness. This poor performance in preventing Exfiltration highlights the urgent need for measures to protect sensitive data from unauthorized data transfer and removal. Organizations should invest in leading data loss prevention solutions and adopt stricter access controls to mitigate this risk.

In 2024, while **Persistence** showed a slight improvement from 35% to 36%, **Execution** saw a decline to 36% from 40%. **Command and Control** experienced a significant drop to 37% from 45%. The decline in Command and Control prevention effectiveness points to growing challenges in stopping attackers from maintaining control over compromised systems. Strengthening network segmentation, implementing strict egress filtering, and utilizing advanced intrusion detection systems can help mitigate this risk.

The **Impact** tactic, which dropped from a prevention effectiveness score of 42% in 2023 to 37% in 2024, points to serious vulnerabilities that need immediate attention. Impact tactics involve actions taken by adversaries to manipulate, interrupt, or destroy data or systems. This performance decline suggests that organizations are increasingly susceptible to actions that can negatively disrupt their operations, such as data destruction, data encryption, and service interruption. To address this, organizations should enhance their data backup systems and implement stringent access controls to mitigate the potential damage from successful attacks.

Performance by Threat Group

When analyzing the effectiveness of security devices to prevent cyber threats for the 2024 Blue Report, we recognize that organizations are finding it increasingly challenging to protect against certain sophisticated threat groups. The groups with the highest "success" rates generally were either state-linked, state-sponsored, or strongly financially motivated. These groups tend to employ highly advanced tactics, techniques, and procedures (TTPs) to evade many existing security defenses. Common techniques include sophisticated spear-phishing campaigns, exploitation of vulnerabilities, lateral movement within networks, and the use of defense evasion methods such as living-off-the-land binaries (LOLBins).



The **Gallium** group, with a prevention rate of 38%, exemplifies the challenge posed by such state-linked threat actors. Known for targeting telecommunications firms, **Gallium's** attacks often involve long-term campaigns aimed at strategically compromising an organization. Similarly, groups like **SideCopy** (45%) and **Tortoiseshell** (48%) demonstrate that their complex methodologies and focus on national security and financial sectors are particularly difficult to prevent.

EXOTIC LILY (50.52%) and **Red Menshen** (50.61%) are prime examples of how financially motivated groups are changing their methods. These groups often deploy a mix of social engineering and technical exploitation to achieve their goals, making it harder for traditional security solutions to flag their activities in real time.

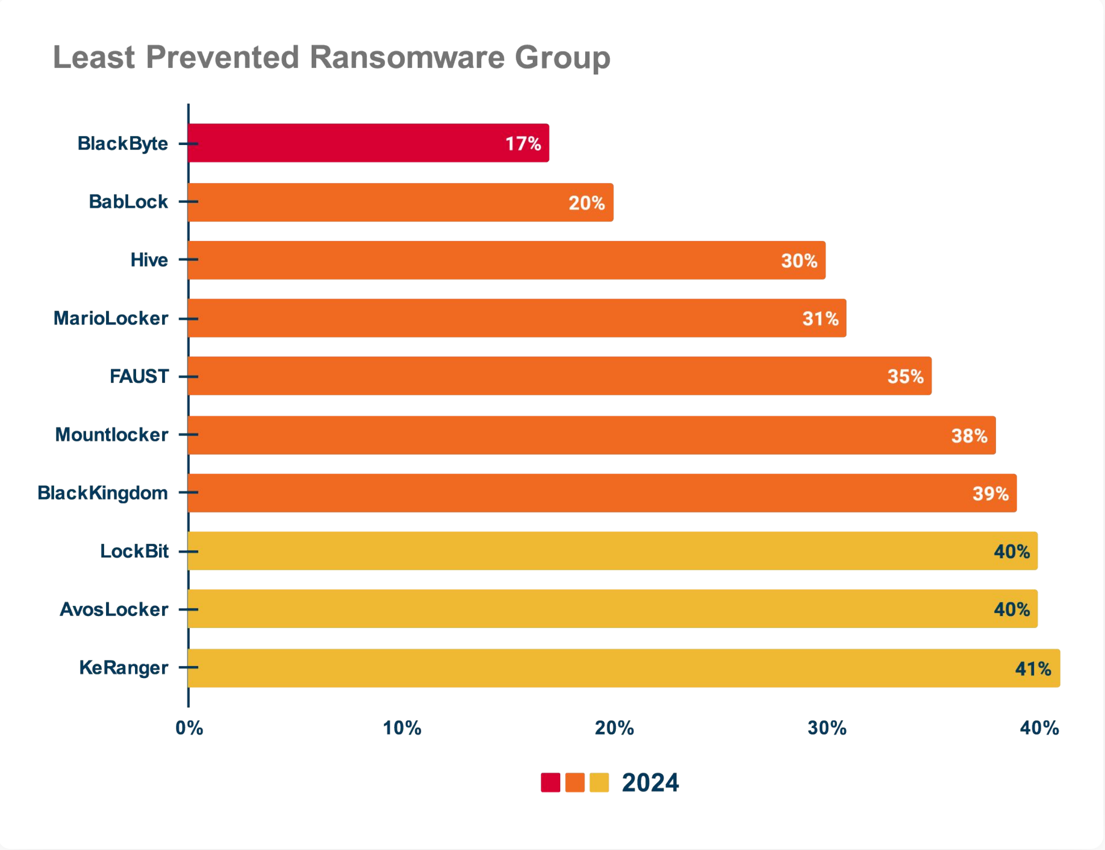
Another group with a disturbingly low prevention rate is **Mustang Panda** (52.18%), which has consistently shown its prowess in leveraging geopolitical tensions for state-sponsored campaigns. Their ability to blend cyber-espionage with tangible political impacts makes them particularly problematic for organizations and governments to defend against. **MuddyWater** (53%) represents a similar challenge, with its suspected links to Iranian state entities and its use of sophisticated TTPs that include exploiting public-facing applications and intricate spear-phishing attacks.

Moreover, the statistical data highlights that even as the prevention rates gradually improve with groups like **Earth Lusca** (54%) and **Winter Vivern** (63%), the underlying difficulty of dealing with such adversaries remains. These groups continuously adapt to counter-measures put in place, driving a constant need for updated security practices and vigilance. **OilRig** (64%) still presents significant challenges despite increasing prevention rates. This Iranian-linked group specializes in cyber-espionage within critical industries such as finance and telecommunications.

Spotlight on Ransomware Attacks

Ransomware remains one of the most formidable threats to organizations across various industries worldwide. Due to their disruptive impact, adaptability, and constant evolution, ransomware attacks are still a formidable challenge for organizations. Even well-equipped organizations are not immune, underscoring the need for all to adopt a proactive defensive posture.

In our 2024 analysis, we identified the ransomware attacks that organizations were **least able** to prevent. The top 10 ransomware strains with the lowest prevention effectiveness scores are:



Our results show that **BlackByte**, with a prevention effectiveness score of just 17%, was the most challenging ransomware for organizations to prevent in the first half of 2024. Known for its aggressive tactics and rapid encryption capabilities, **BlackByte** exploits vulnerabilities in public-facing applications and leverages social engineering to gain an initial foothold.

BabLock, with a score of 20%, employs sophisticated techniques to bypass traditional security measures, often utilizing double extortion methods to pressure victims into paying ransom.

Hive, scoring 30%, has been notorious for its swift evolution and multi-cell attack strategies, designed to maximize damage and evade detection. Hive often targets healthcare institutions, exacerbating its impact due to the critical nature of the data involved.

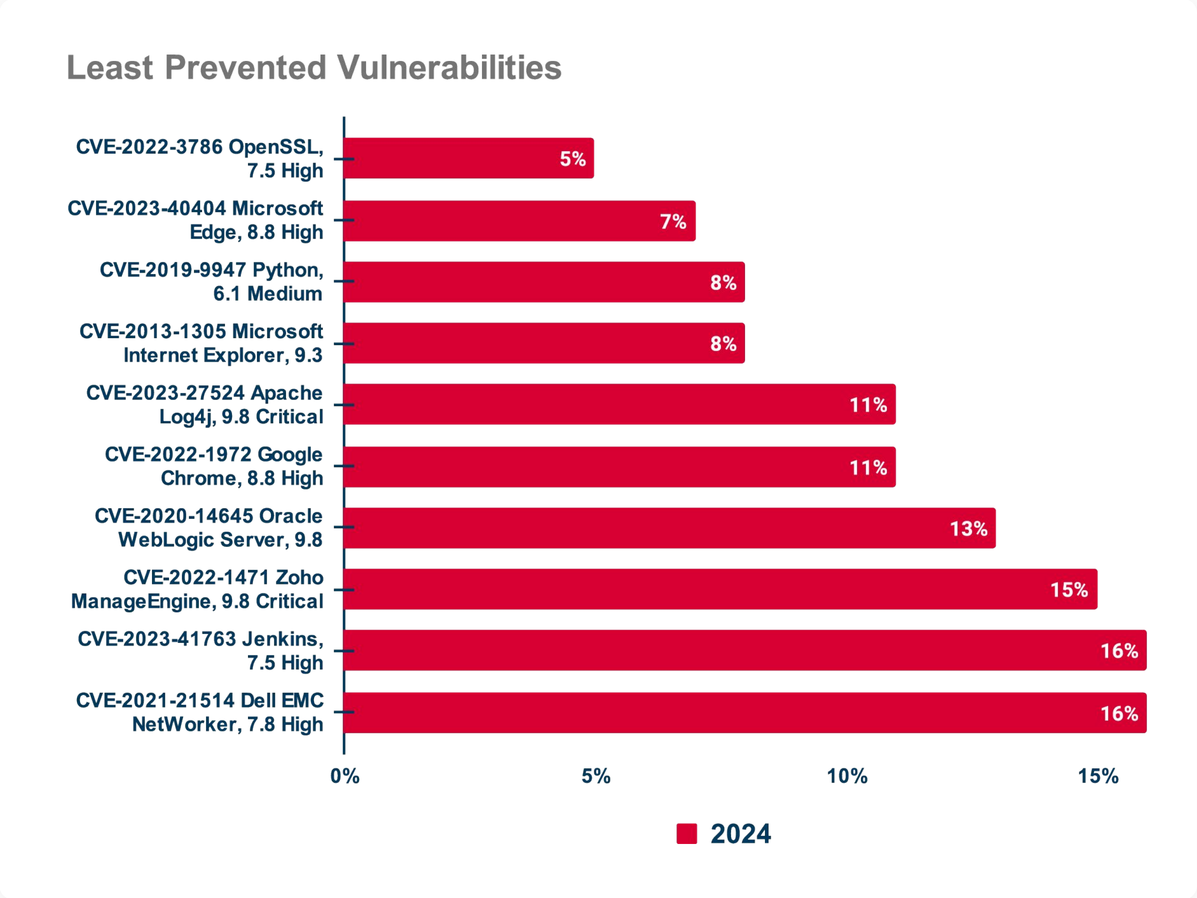
MarioLocker and **FAUST**, with prevention scores of 31% and 35% respectively, reflect the complexity of their attack chains, which often include data exfiltration before encryption, increasing the pressure on organizations to pay the ransom.

Mountlocker (38%) and **BlackKingdom** (39%) also continue to pose significant threats due to their advanced network infiltration and lateral movement capabilities, often using stolen credentials to escalate privileges and deploy ransomware across multiple systems.

LockBit and **AvosLocker**, both currently at 40%, also displayed a high degree of sophistication with features designed to evade detection and ensure persistence. **LockBit**'s automated attack capabilities make it particularly dangerous, as it can quickly spread within a compromised network. **KeRanger**, with a prevention effectiveness score of 41%, is notable for being one of the first ransomware targeting macOS systems, exploiting users who may feel a false sense of security on non-Windows platforms.

Spotlight on Vulnerabilities

Software vulnerabilities, often labeled with common vulnerabilities and exposures (CVEs), are another avenue frequently used by attackers. The recent data highlights a concerning trend in prevention effectiveness against these vulnerabilities, indicating there are still significant gaps in organizations' security measures. We identified the **ten least prevented vulnerability exploits** as part of our analysis of attack simulations. Organizations were able to prevent them only 5-16% of the time. Moreover, the data reveals that organizations are not particularly good at prioritizing timely vulnerability patching, with many high-severity vulnerabilities remaining exposed despite being known for years.



Several of these vulnerabilities have drawn substantial media attention due to their high severity and widespread impact. For example:

- **Log4Shell (CVE-2023-27524, Apache Log4j)**: With a prevention effectiveness of just 11%, this critical vulnerability allows remote code execution, posing a severe risk to systems utilizing the Apache Log4j library.
- **Zoho ManageEngine (CVE-2022-1471)**: This vulnerability, also with an 11% prevention effectiveness, enables remote code execution, highlighting the urgent need for improved security measures in managing engine software.

- **Oracle WebLogic Server (CVE-2020-14645)**: Known for its remote code execution (RCE) exploits, this vulnerability has a prevention effectiveness of 13%, underscoring the necessity for better patch management and network segmentation.

The presence of older vulnerabilities such as **CVE-2019-9947 (Python)** and **CVE-2013-1305 (Microsoft Internet Explorer)**, with prevention effectiveness scores of 8%, emphasizes the long-term security risks posed by unpatched systems. These vulnerabilities remain critical points of exploitation due to their extensive use of their exploited applications and the complexities involved in updating legacy systems.

Other noteworthy vulnerabilities include:

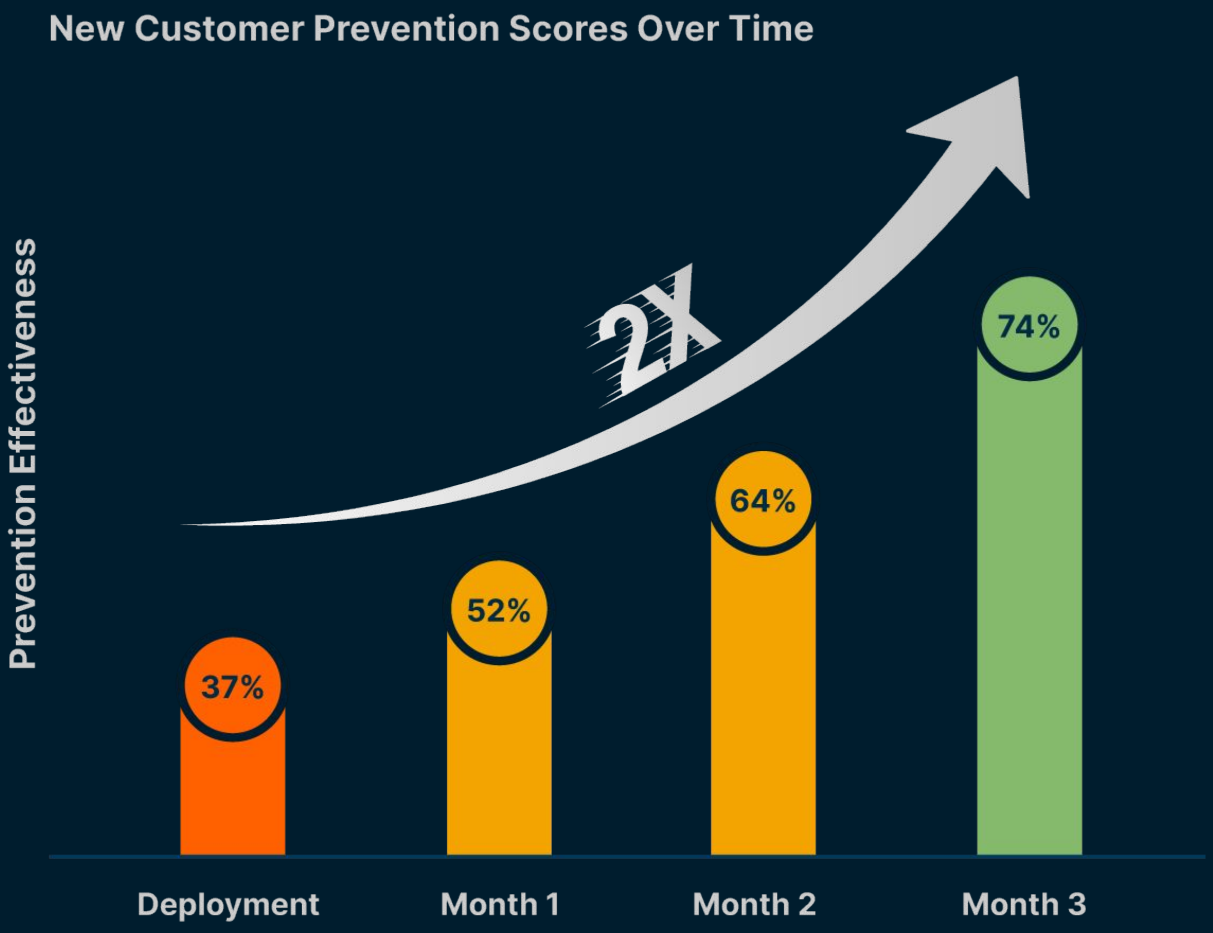
- **CVE-2023-40404 (Microsoft Edge)** and **CVE-2022-1972 (Google Chrome)**: Both have prevention effectiveness scores of 7% and 11%, respectively. The low scores reflect the ongoing challenges in securing widely-used web browsers against sophisticated attacks.

- **CVE-2023-41763 (Jenkins)**: With a prevention effectiveness of 16%, this vulnerability highlights the risks in Continuous Integration/Continuous Deployment (CI/CD) environments.

Overall, the data paints a clear picture: despite the high severity of these vulnerabilities, many organizations continue to struggle with effectively prioritizing and preventing them.

In summary, while notable progress has been made in prevention effectiveness, significant challenges remain, especially in detection capabilities and endpoint security. The report underscores the importance of adopting a proactive security mindset and implementing Continuous Threat Exposure Management (CTEM) to stay ahead of evolving threats. By enhancing detection and prevention mechanisms, fortifying ransomware defenses, improving endpoint security configurations, and prioritizing effective log management and password security, organizations can significantly improve their resilience against cyberattacks. Through continuous validation and fine-tuning of security controls, organizations can achieve a robust and adaptive security posture that aligns with the dynamic threat landscape.

Picus Security Customers Prevent Twice As Many Attacks



Picus Security provides a threat exposure management solution - the Picus Security Validation Platform, powered by our Exposure Data Fabric and Numi Ai™ . The platform includes Security Control Validation (SCV), Cloud Security Validation (CSV), Attack Path Validation (APV), Detection Rule Validation (DRV), and Attack Surface Validation (ASV) allowing organizations of all sizes to continuously correlate, prioritize and validate exposures to reduce their cyber risk.

On average, our customers prevent twice as many attacks, within just three months. With Picus Security, security leaders can quickly mature their security posture and move beyond the complexity of siloed threat data and basic vulnerability management. Instead of spending their days making impossible trade-offs that may leave gaps in their defenses, they can prioritize critical gaps and high-impact fixes that allow teams to stop more threats with less effort.

About Picus Security

Picus Security, the leading security validation company, provides organizations a clear picture of their cyber risk based on business context. The Picus Security Validation Platform transforms security practices by correlating, prioritizing, and validating exposures across siloed findings so teams can focus on critical gaps and high-impact fixes. Picus strives to empower security teams to understand their cyber risk and prioritize issues worth pursuing with one-click mitigations, stopping more threats with less effort.

For more information, visit **picussecurity.com**

BLUE REPORT
2024

picussecurity

picussecurity.com

PICUS