PICUS

BLUE REPORT™ 2025

The State of Threat Exposure Management

Table of Contents

Introduction

from 69% to
62% ↓

Prevention Score

from 54% to
54% –

Log Score

from 12% to
14% ↑

Alert Score

At a Glance

Currently in its third year, the **2025 edition of the Blue Report** continues to deliver data-driven insights and actionable recommendations for cybersecurity professionals by evaluating the real-world effectiveness of prevention and detection capabilities. Developed by Picus Labs, this annual study is based on over **160 million attack simulations** performed on the Picus Security Validation Platform, providing a comprehensive view of how security products and configurations perform across modern enterprise environments.

The Blue Report 2025 is designed to serve as a practical guide for security teams and decision-makers aiming to mature their security posture through **Continuous Threat Exposure Management** (CTEM). By identifying blind spots, validating assumptions, and fine-tuning defenses based on adversary behavior, organizations can reduce uncertainty, better prioritize resources, and build a more resilient cybersecurity foundation.

What's New This Year

- This year, we've deepened the report's focus on prevention and detection effectiveness across attack vectors, regions, and industries. For the 2025 report, we've expanded our analysis to assess prevention performance against MITRE ATT&CK techniques, revealing alarmingly low prevention effectiveness across industries against frequently used adversary behaviors.
- The vulnerability section now focuses exclusively on CVEs disclosed in 2024 and 2025, offering a clearer view of how well organizations are addressing new and emerging threats. Findings from Attack Path Validation (APV) and Detection Rule Validation (DRV) highlight persistent gaps in lateral movement prevention, privilege escalation defense, and overall detection effectiveness.

Executive Summary

Data Theft
3%
Prevention Effectiveness

Password Cracking
46%
Success Rate

Valid Accounts
98%
Prevention Failure Rate

The Blue Report 2025 highlights the essential role of **Continuous Threat Exposure Management (CTEM)** and emphasizes the critical importance of **Adversarial Exposure Validation (AEV)** in confronting increasingly sophisticated cyber threats and operational blind spots. While the Red Report 2025 highlighted the rise of credential-targeting malware and infostealers, the Blue Report identifies surprising defensive gaps, particularly in data exfiltration and password-based attacks.

Of particular concern, password cracking attempts succeeded in 46% of tested environments, nearly doubling the previous year's rate. Compounding this risk, attacks using Valid Accounts (T1078) achieved a 98% success rate, highlighting persistent challenges in maintaining effective password policies and detection.

Data exfiltration defenses suffered a severe decline, dropping to an alarming prevention rate of just 3%. This decrease is particularly concerning given the rise of double-extortion ransomware attacks designed specifically to evade traditional encryption-focused defenses.

Despite these critical gaps, **Picus Attack Path Validation (APV)** assessments reveal significant improvements. **Domain administrator compromise rates notably fell from 24%** in 2024 to 19% in 2025, with domain admin access also decreasing significantly from 40% to 22%. These advances demonstrate strengthened lateral movement defenses, improved network segmentation, and better operationalization of security validation insights.

Average prevention effectiveness declined from 69% to 62%, indicating that security controls lose efficacy without continuous validation and tuning. While detection effectiveness improved slightly, with **alert scores rising from 12% to 14%**, a significant gap remains between logging and detection alerts, with log failures found in 54% of **Picus Detection Rule Validation (DRV)** assessments.

The Blue Report 2025 reinforces that **static defenses are no match for adaptive threats**. To stay ahead, organizations must adopt AEV into their CTEM programs to move beyond assumptions, prioritize with confidence, and respond faster to the threats that matters most.

Key Findings

The Blue Report 2025 reveals a shifting cybersecurity landscape, where progress in some areas is tempered by persistent and in some cases, deepening challenges and failures in others. This year's analysis shows the growing complexity of defending against real-world threats and the importance of continuous validation to reduce exposure. Below are some of the most significant findings from the report:

Data Exfiltration Defense Is Getting Worse Despite Rising Risk

For the third year in a row, data exfiltration remains the least prevented attack vector, but this year the prevention score has deteriorated even further, **dropping from 9% in 2024 to just 3% in 2025.**

This decline comes at a critical moment: the **Red Report 2025 revealed a 3x surge in infostealers**, while ransomware groups are increasingly use double extortion tactics to steal and leak sensitive data. Despite these escalating threats, most organizations remain woefully unprepared to detect or block data theft, highlighting a widening and urgent blind spot.

Password Cracking Threat Intensifies

In 46% of environments, at least one password hash was successfully cracked and converted into cleartext, nearly doubling last year's rate of 25%. This points to an ongoing reliance on weak password policies, particularly in internal domains.

The Red Report 2025 also found credential theft techniques like **Credentials from Password Stores (T1555) were used in 25% of malware samples**, with attackers leveraging stored logins and password managers to accomplish lateral movement and escalate privileges. These trends show how quickly a single compromised credential can open the door to broader access.

Significant Improvements in macOS Endpoint Security

In a notable reversal from last year (23%), **macOS endpoints** achieved a **76% prevention rate**, outpacing both **Windows (79%) and Linux (69%) endpoints.**

The dramatic gain in macOS protection reflects growing investment and maturity in securing Apple environments, which have been historically underprotected.

Key Findings

Prevention Effectiveness Declines

After a strong improvement in 2024, the **average prevention score fell slightly from 69% to 62%** in 2025. This drop suggests that many organizations are struggling to keep up with increasingly sophisticated attack techniques and that their previously effective controls may be losing their edge without continuous validation and tuning.

Detection Shows Modest Recovery

The log score remained stable at 54%, indicating consistent data capture and monitoring capabilities. However, **alert score improved ever so slightly from 12% to 14%**, signaling slow but positive momentum in converting logs into actionable intelligence. Still, the wide delta between logs and alerts points to persistent gaps in detection engineering and threat correlation.

SIEM Rule Failures Still Mainly Due to Logging Issues

Analysis on detection rules revealed that **log collection issues caused 50% of failures**. Other core problems included **performance issues (24%)** and **configuration errors (13%)**, highlighting weaknesses in the detection engineering pipeline. Additional gaps, such as improper log coalescing (17%), unavailable sources (7%), and broken sources (4%), reflect ongoing integration blind spots and monitoring lapses that continue to leave threats undetected.

BlackByte Continues to Challenge Ransomware Defense

Ransomware remains a top concern, and **BlackByte continues to be the hardest strain to prevent**, with a prevention effectiveness of just 26%, even after its prominence in last year's findings. BabLock and Maori followed at 34% and 41%, respectively.

Key Findings

Infrastructure Hardening Shows Measurable Progress with APV

This year's **Attack Path Validation (APV)** findings indicate meaningful gains in internal security posture. In 2025, only 19% of simulations led to full domain administrator compromise, down from 24% in 2024. Similarly, **domain admin access occurred in just 22% of environments, a significant drop from 40% the previous year.**

These improvements reflect stronger lateral movement defense, segmentation, and better use of validation insights. Still, with nearly a quarter of environments vulnerable to privilege escalation, **regular testing and targeted remediation both remain essential** to closing critical gaps.

Cybersecurity Product Effectiveness Still Varies in Practice

Despite strong lab performance, cybersecurity products often show **significant variability in real-world environments**. Solutions that score 100% in MITRE ATT&CK evaluations frequently fall short in production due to **infrastructure differences, misconfigurations, and integration gaps**.

These results help make the case for **continuous, context-aware validation and fine-tuning** to ensure controls perform reliably where they matter most.

Core Adversary Techniques Remain Effective

Despite growing awareness of adversary behavior, many common ATT&CK techniques remain under-prevented. In 2025, **Valid Accounts (T1078) had the lowest prevention rate at just 2%,** showing how easily attackers blend in using stolen credentials. Discovery techniques like **System Network Configuration Discovery and Process Discovery also scored below 12%**, exposing blind spots in early-stage detection.

Low prevention rates for Defense Evasion and Command and Control techniques, such as **Execution Guardrails (8%) and Data Encoding (3%)** further highlight the limitations of static detection. These trends point to a need for stronger behavioral detection to identify subtle, context-driven attacker techniques.

Key Recommendations

The findings of the Blue Report 2025 highlight the growing need for organizations to revisit their security strategies with a sharper focus on validation, visibility, and control hardening. Based on our analysis, we recommend the following actions to reduce exposure and improve threat readiness:

☑ Validate Exposure, Not Just Inventory

Shift from simply knowing where exposures exist to proving which ones matter. **Adopt the adversarial exposure validation approach** that goes beyond asset and vulnerability discovery to confirm exploitability. This enables faster, more informed prioritization and reduces the noise and wasted effort created by theoretical risks.

☑ Strengthen Data Exfiltration Defenses

With data exfiltration prevention falling to just 3%, it's essential to enhance controls that monitor and restrict outbound data flows. **Implement and validate data loss prevention (DLP) rules, outbound traffic filters, and behavioral detection** to reduce the risk of silent data theft, especially as infostealers and ransomware continue to rise.

☑ Enforce Stronger Password Hygiene

In 46% of environments tested, at least one password hash was successfully cracked, often due to weak password complexity, outdated hashing algorithms, or the reuse of credentials across systems. Organizations should **enforce strong password policies and regularly validate credential defenses** through simulated password cracking attacks.

☑ Continuously Validate and Tune Preventive Controls

The drop in prevention effectiveness signals the need to regularly test and refine your existing defenses. Security controls, no matter how advanced, can deteriorate over time. **Use real-world attack simulations to continuously validate** IPS, NGFW, and endpoint security tools, ensuring they remain effective against constantly changing adversary behaviors.

Key Recommendations

☑ Improve the End-to-End Detection Pipeline

A 54% log score means that nearly half of attacker behaviors go unlogged, leaving organizations with significant blind spots. Even more concerning, the alert score is also critically low at just 14%, far below the levels needed for effective detection and response. Organizations must **strengthen the full detection pipeline** from ensuring comprehensive log coverage to fine-tuning correlation rules and alert logic.

☑ Strengthen Ransomware Defenses in the Era of Encryptionless Extortion

As more organizations adopt modern backup and recovery solutions, ransomware groups are shifting tactics toward encryptionless extortion, threatening to leak stolen data without deploying encryption. Ensure endpoints have up-to-date security controls, and **regularly simulate full ransomware scenarios**, including data exfiltration and extortion techniques, to test your ability to detect, contain, and respond before any actual damage is done.

☑ Improve Detection of Common Techniques with Behavioral Analysis

To address persistent gaps in preventing common ATT&CK techniques, **organizations must strengthen their behavioral detection capabilities**. Static rules and signature-based controls often miss subtle attacker actions, especially those that mimic legitimate user behavior. Techniques like Valid Accounts (T1078) and early-stage Discovery techniques require context-aware monitoring and identity-aware detection logic to be effectively surfaced. Regularly validate your controls against common techniques such as credential abuse, discovery, and command and control to ensure your defenses can detect and respond to the tactics adversaries rely on the most.

Methodology

The findings in this year's report are based on the results of simulated attack scenarios executed by Picus Security customers from January to June 2025. **The data has been anonymized and aggregated from over 160 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 cyber attacks 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 current security measures, suggesting the need for security teams to conduct a thorough review and enhance their existing controls.

Detection Effectiveness assesses an organization's capability to identify potential cyber threats through the security controls they already have in place. 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 identifying areas for improvement.

90-100% Optimized	**Organizations with optimized security controls continuously monitor, refine, and update them to keep up with the an ever-evolving threat landscape and maintain their edge in exposure management.**
70-89% Managed	**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 their exposure management.**
40-69% Moderate	**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.**
20-39% Basic	**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 keep building a more effective threat exposure management program.**
0-19% Inadequate	**Inadequate security controls provide almost no protection to a very minimal level of 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.**

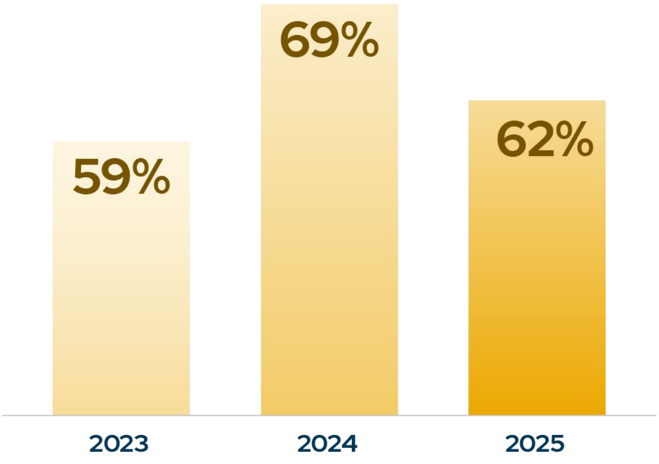
Overall Prevention and Detection Effectiveness Performance

This year's report reflects a mixed landscape for organizations attempting to prevent and detect cyber attacks. While certain metrics held steady or showed incremental improvement, others signaled areas of real regression. The drop in prevention effectiveness, combined with stagnant detection performance, suggests that many organizations are struggling to maintain hardened defenses in the face of a growing volume of sophisticated threats. It's a reminder that security controls are not set-and-forget tools. They degrade over time and require continuous validation to remain effective.

Prevention Effectiveness

In 2025, **the prevention effectiveness score declined to 62%**, down from 69% in 2024. This marks a reversal of last year's significant 10-point gain, where scores had improved from 59% in 2023. This year's slip backward suggests that many organizations are now falling behind on maintaining and fine-tuning their security controls. While 62% still represents the ability to block nearly two-thirds of simulated attacks, the decline highlights how quickly and easily defenses can degrade without continuous oversight.

These findings reinforce the importance of continuous exposure validation and real-world attack simulation to remain operationally effective against evolving threats.

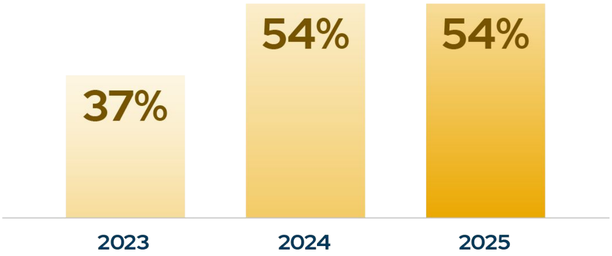


Prevention Scores Over Time

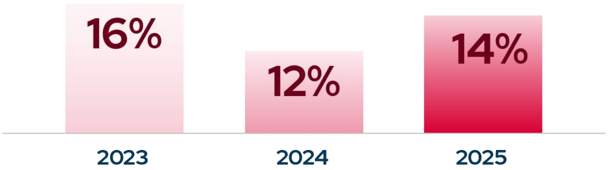
Detection Effectiveness

In 2025, the detection effectiveness scores showed only modest recovery and remain a critical area of concern. **The log score held steady at 54%**, meaning nearly half of attacker behaviors are still not logged in most environments. **While the alert score increased slightly from 12% to 14%, this still indicates that less than 1 in 7 attacks generate a meaningful alert.** For most organizations, this level of performance is far below what's needed for timely detection and effective response.

The stagnation in logging coverage is concerning, as it reflects persistent weaknesses in the foundational layer of the detection pipeline. Without full visibility into attacker activity, no amount of analytics or correlation can compensate. At the same time, the low alert rate reinforces that even when logs are captured, they are often not correlated, prioritized, or escalated effectively, leaving threats undetected and security teams uninformed.



Logging Scores Over Time



Alerting Scores Over Time

This growing gap between what is logged and what is alerted highlights systemic issues in detection engineering. Many organizations are still operating with ineffective detection pipelines that are prone to silent failure, either because telemetry never reaches the SIEM or because detection logic fails to trigger relevant behaviors.

To address these issues, organizations need to move beyond basic telemetry collection and invest in validating the entire detection lifecycle. This includes not only verifying log availability and quality but also testing whether detection rules are functioning as intended and whether they generate high-fidelity alerts in response to real-world attacker behaviors. Without these validations, organizations risk overestimating their detection capabilities and underestimating their exposure.

Addressing the Gaps

Once again, our findings reveal a troubling pattern: many organizations believe their controls are working until they're tested. This false sense of security stems from an overreliance on dashboards, static metrics, and assumptions that logging equates to visibility or that prevention implies protection. In reality, security controls degrade over time due to configuration drift, tool misalignment, software updates, new adversary techniques, and evolving infrastructure. Without continuous validation, these failures stay hidden until it's too late.

Log collection is essential,
but not enough for effective detection.

The flatlining log score and persistently low alert score expose this illusion. Collecting telemetry is not the same as understanding it, and logging alone does not guarantee that threats will be detected, prioritized, or acted upon. Likewise, even high-performing prevention controls can degrade if not regularly tested against modern threats. In many cases, what appears to be protection is merely a lack of visibility into successful bypasses.

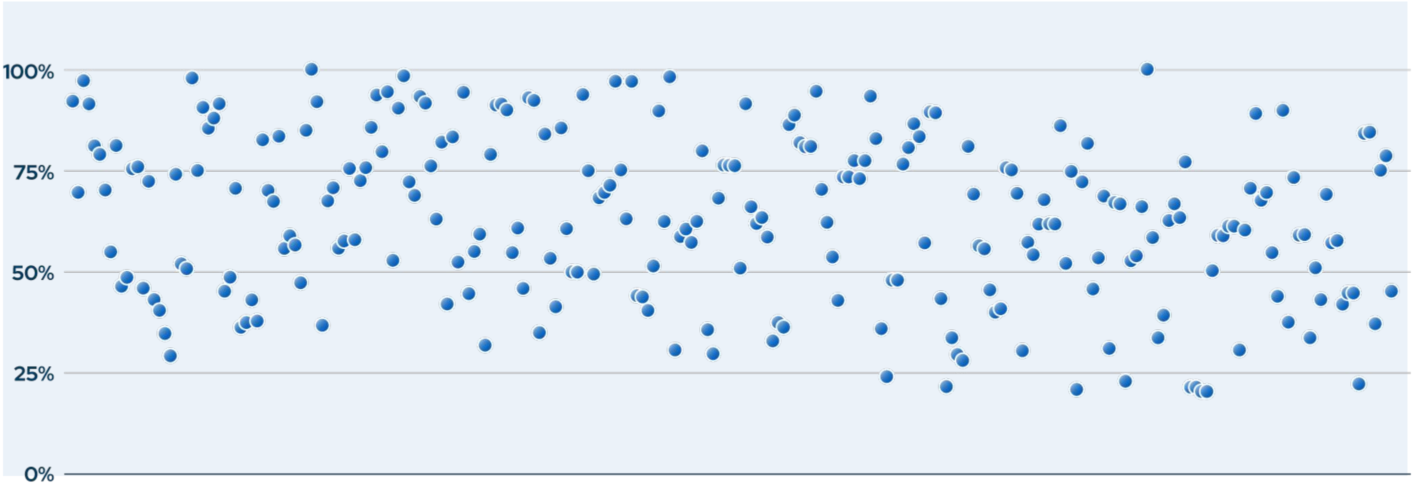
To close these gaps, organizations must adopt an "assume breach" mindset that assumes failure is possible at every layer of defense and seeks to find it before adversaries do. This means regularly testing whether logs are complete, detection rules are firing, alerts are being generated, and controls are blocking attacks in real-world conditions. It also means challenging assumptions, removing reliance on static assessments, and integrating exposure validation into daily security workflows.

Real-World Performance of Cybersecurity Products

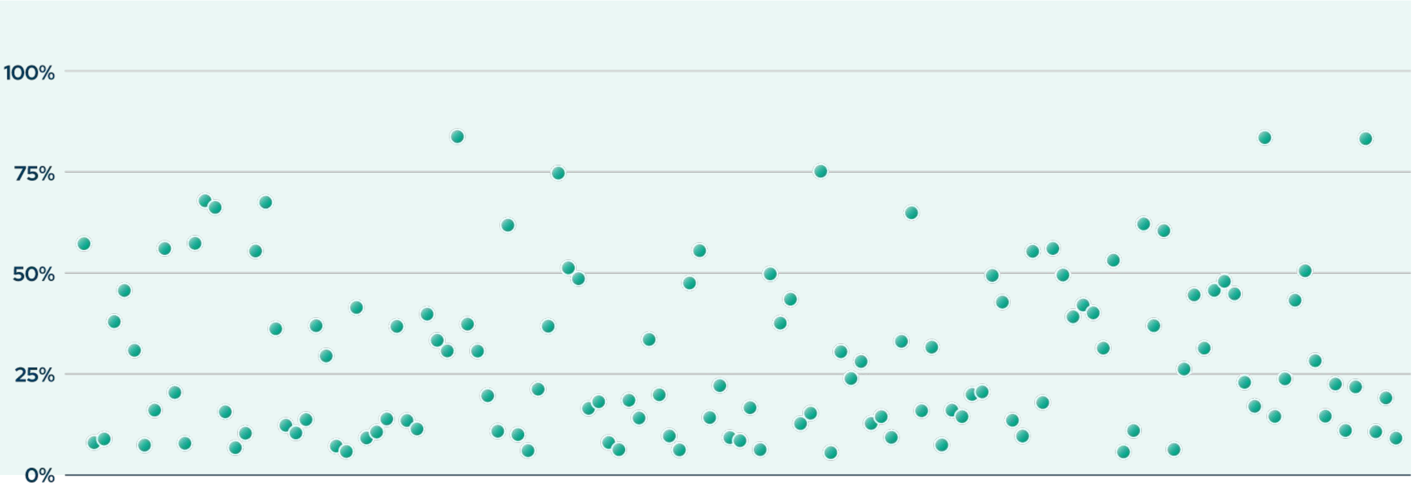
Cybersecurity products are often evaluated in controlled test environments using curated attack scenarios, tightly defined metrics, and ideal configurations. **Benchmarks like ATT&CK® Evaluations offer valuable insight into a product's potential, but they do not reflect the full complexity of production environments**, where configuration drift, integration friction, and operational constraints can significantly impact outcomes. This year's findings reinforce this persistent reality: strong performance in a lab does not guarantee effectiveness in production.

Even security solutions that achieve 100% prevention and detection scores in lab tests often exhibit inconsistent effectiveness once deployed. This isn't because the products lack potential. It's because they are rarely deployed or maintained under ideal conditions.

Prevention Score



Detection Score



Our analysis shows that control degradation is more common than most teams realize. Security tools that were properly installed and configured at deployment may fail over time due to:

- **Configuration drift:** Policy changes, software updates, and integration rollouts gradually alter how tools behave.
- **Broken integrations:** A misconfigured log source or disabled alerting rule may render a detection pipeline ineffective without anyone noticing.
- **Operational complexity:** Each organization has a unique mix of systems, staffing levels, compliance requirements, and network architecture. These variables can significantly impact product effectiveness.
- **Dynamic threats:** The threat landscape evolves constantly. Products must be regularly tested and updated to keep up with new TTPs. Static signatures and stale configurations quickly become obsolete.

It's not uncommon for security teams to assume that a product is working simply because it exists in the stack. But **presence is not proof of performance**. Without validation, there's no way to confirm whether a detection rule triggers, whether a prevention control actually blocks a live threat, or whether an alert is ever escalated.

This disconnect between expected and actual performance results in unseen exposure, even within well-resourced security programs. To ensure cybersecurity investments deliver their intended value, **organizations must recognize that security products require continuous maintenance, not one-time deployment.**

We recommend:

1. **Treat evaluations as guidance, not guarantees.**
MITRE ATT&CK® Evaluations and other independent tests offer valuable starting points. But they must be validated in your own environment, with your configurations, controls, and constraints.
2. **Expect degradation and plan for it.**
Even the best tools lose effectiveness without maintenance. Routine validation is the only way to detect control drift and silent failures before attackers do.
3. **Make continuous validation part of your workflow.**
Use simulated attack scenarios to test both prevention and detection capabilities in context. Confirm that controls behave as expected, that alerts are generated, and that response processes activate when they should.

Uncovering Critical Defensive Gaps with Automated Penetration Testing

Automated penetration testing remains a vital capability for uncovering real-world weaknesses across enterprise environments. Leveraging the Picus Attack Path Validation (APV) module, organizations can emulate full-chain adversarial behavior starting from initial access and credential compromise to lateral movement and privilege escalation without requiring red team resources or intrusive manual efforts.

This year's findings from Picus APV assessments show clear progress in infrastructure hardening. In 2025, only 19 percent of simulations resulted in full domain administrator compromise, down from 24 percent in 2024, indicating more effective lateral movement defense, tighter network segmentation, and broader adoption of exposure validation practices.

Additionally, domain administrator access was achieved in 22 percent of tested environments, a significant improvement from 40 percent the previous year. In other words, fewer than one in four organizations had a viable attack path to full domain compromise. While this marks meaningful progress, the fact that nearly a quarter of environments still contain exploitable privilege escalation paths highlights the ongoing need for continuous validation and targeted remediation.

Despite improvements in overall infrastructure resilience, password cracking success rates increased dramatically. **In 46% of APV simulations, attackers were able to crack at least one dumped password hash and obtain valid credentials, up from 25% in 2024.**
This rise points to persistently weak password policies and outdated hashing algorithms, especially in internal domains where complexity requirements, rotation policies, or multi-factor protections may be inconsistently applied. In many scenarios, a single cracked credential triggered a chain of lateral movement events that led to broader exposure. These findings emphasize that even with better segmentation and endpoint visibility, compromised credentials remain a fast track to privilege escalation.

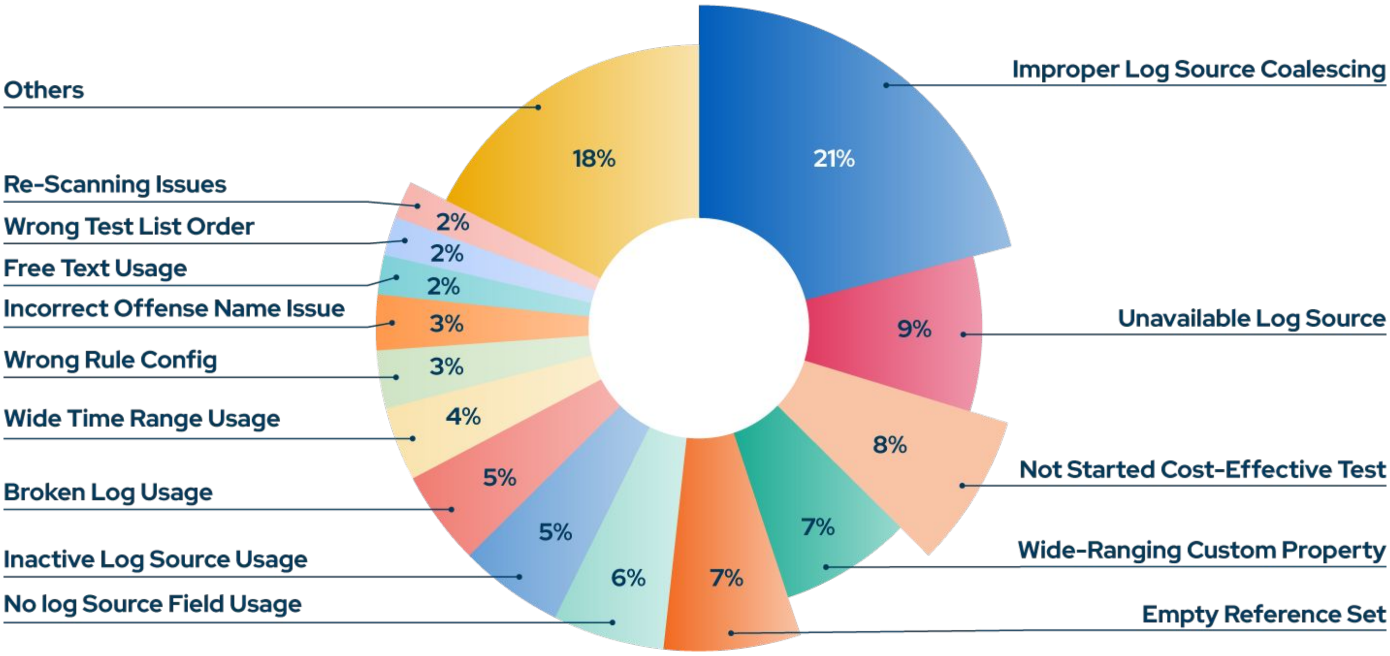
Organizations must complement hardening efforts with:

- Stronger password complexity and rotation policies
- Elimination of legacy or deprecated hashing methods
- Regular validation of credential exposure through simulated attacks

Detection Rule Effectiveness

Detection rules serve as the core logic layer of threat detection. When properly written, validated, and maintained, they allow SIEM and EDR platforms to raise meaningful alerts from massive volumes of telemetry. However, our analysis of detection rules reveals that many organizations still struggle with rule reliability, precision, and operational readiness.
This year's findings highlight a familiar pattern: log source issues remain the dominant root cause of rule failure, but configuration and performance issues also continue to silently undermine detection capabilities across the board.

Common Issues Affecting Detection Rule Effectiveness



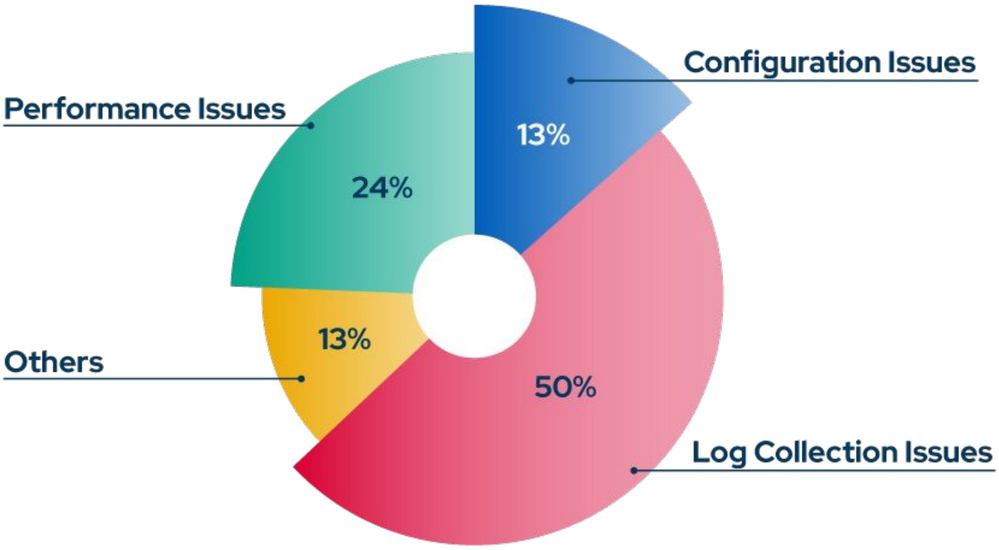
The most common and high-impact failure point in 2025 was Improper Log Source Coalescing, affecting 21% of assessed rules. This problem occurs when event coalescing is enabled for specific log sources such as DNS systems, proxy servers, Windows servers, and endpoints, leading to data loss. When critical threat behaviors are compressed or dropped, detection logic becomes partial, delayed, or entirely ineffective.

Unavailable Log Sources accounted for 9% of issues, often resulting from telemetry pipeline disruptions, misconfigured forwarding agents, or network segmentation. **Together with Inactive Log Source Usage (5%) and Broken Log Source connections (5%),** these issues collectively account for **nearly 20% of failures** and represent a persistent visibility gap that detection teams must address urgently.

Beyond logging gaps, configuration-related issues such as **Empty Reference Sets (7%), No Log Source Field Usage (6%), and Wrong Rule Configuration (3%)** continued to impact rule integrity. These failures often stem from a drift between detection content and infrastructure changes, resulting in rules that exist but silently fail to trigger in production.

In 2025, performance-focused issues were also evident. For instance, **Not Starting Cost-Effective Test Filters (8%) and Wide-Ranging Custom Property Definitions (8%)** were among the top issues affecting rule performance and scalability. These overly broad configurations consume excessive processing power, slow down query response times, and often lead to alert fatigue due to imprecise matches.

Common Issues Types in Detection Rules



The dataset for these statistics is sourced from Picus Detection Rule Validation (DRV), which leverages a continuously updated checklist to identify and categorize over 50 recurring issues in detection rules. This year's findings once again highlight the operational fragility of SIEM detection pipelines.

Log collection issues accounted for 50% of all detection rule failures, reinforcing that visibility gaps remain the single largest barrier to effective detection. In addition, **performance-related problems (24%) and configuration errors (13%)** continue to impact detection quality, precision, and scalability.

Together, these categories represent the majority of rule failures observed this year. The findings emphasize the need for continuous validation, fine-tuning, and regular updates to maintain detection rule effectiveness. By addressing these systemic weaknesses, security teams can dramatically improve the reliability and responsiveness of their detection infrastructure.

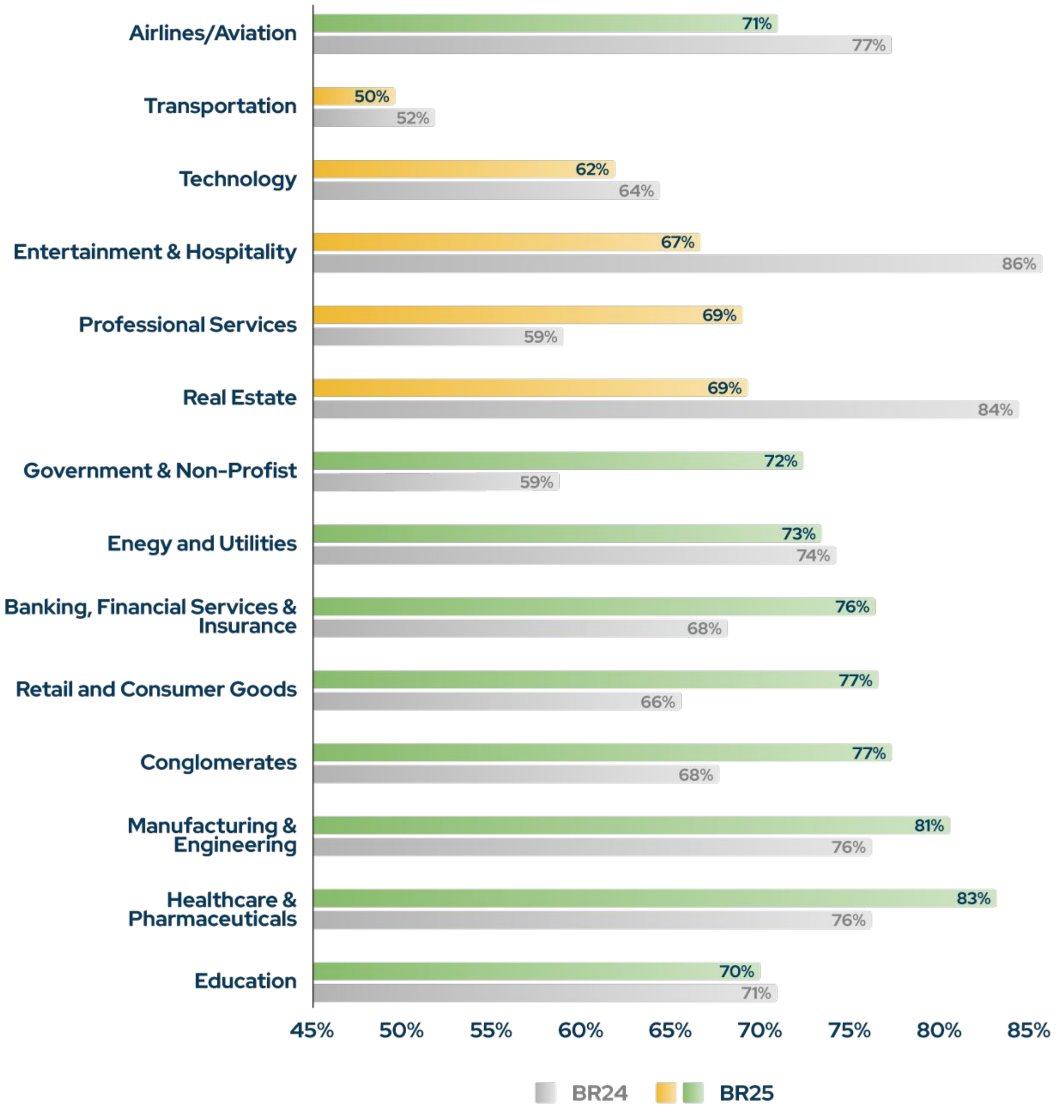
Performance by Industry

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 cyber attacks.

Prevention Effectiveness

In 2025, prevention effectiveness scores varied widely across industries. **The Healthcare and Pharmaceuticals industry** led all sectors with an **83% prevention effectiveness score,** marking a continued upward trend after major gains in 2024. This strong performance likely reflects increased investment in security validation, given the sector's exposure to ransomware and regulatory scrutiny around patient data.

Prevention Effectiveness Score by Industry



Close behind, **Manufacturing and Engineering scored 81%,** followed by **Retail and Consumer Goods and Conglomerates, both at 77%.** These industries often operate with complex, distributed environments and high-value digital assets, making validation and control tuning critical to their resilience.

Banking, Financial Services, and Insurance (BFSI) also performed strongly at **76%,** continuing its consistent trajectory of improvement. The sector's steady performance reflects the impact of maturing CTEM programs and increasing regulatory requirements.

On the other end of the spectrum, **Transportation** registered **the lowest prevention score at 50%,** indicating ongoing exposure to attacks in environments that may lack centralized visibility or consistent control enforcement. **The Technology sector** also underperformed at **62%,** a surprising result given the industry's overall sophistication, suggesting shifting priorities like innovation and growth over improving security practices.

Professional Services (69%), Real Estate (69%), and Entertainment & Hospitality (67%) all hovered near the industry average, with modest but measurable improvements. **Government and Non-Profit organizations achieved a 72% score,** reflecting stable but unremarkable gains.

Airlines/Aviation and Education, both at or near 70%, remain in the moderate-to-managed range, with significant room to grow. These sectors often face unique operational constraints, making control tuning and validation at scale more difficult to implement consistently.

Detection Effectiveness

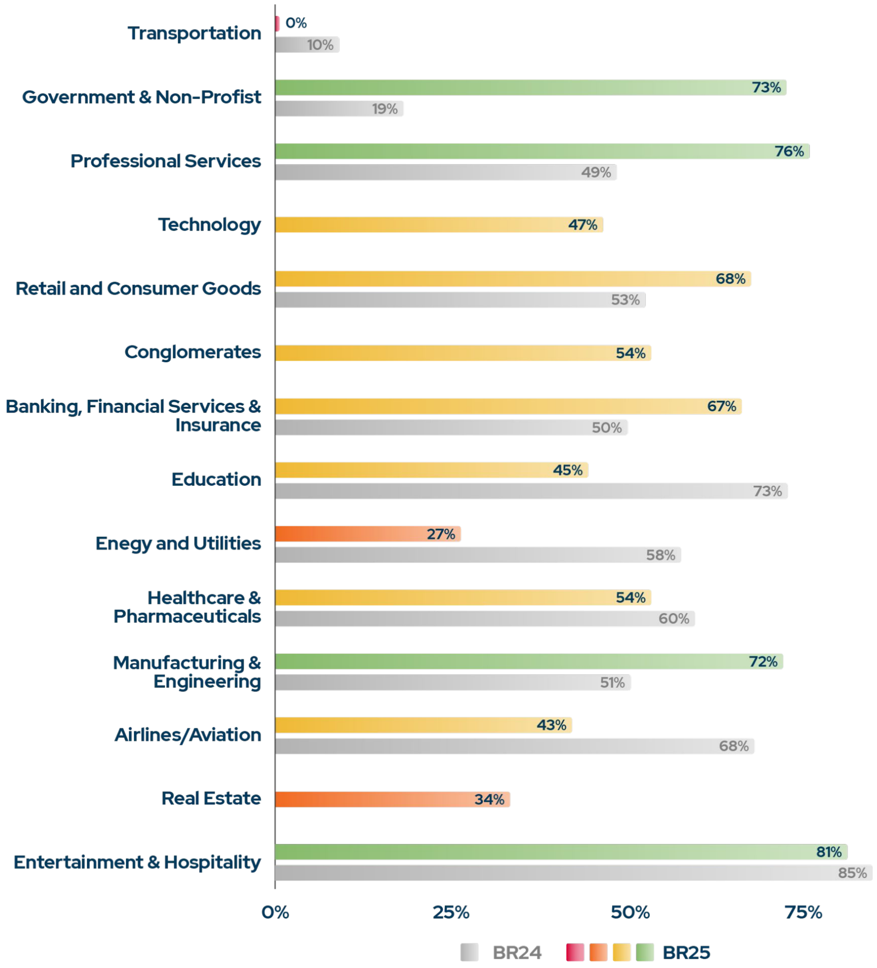
This year's findings reveal a continued disparity between logging and alerting performance across industries, highlighting the persistent challenge of transforming raw telemetry into actionable detection. While several sectors have improved log collection coverage, most are still struggling to generate timely and meaningful alerts.

Entertainment & Hospitality led all industries in log score with an **impressive 81%,** reflecting major improvements in visibility and telemetry coverage.

However, **its alert score remained relatively modest at 20%,** illustrating the broader industry trend: good visibility does not always translate into effective detection.

Professional Services, by contrast, showed a significant gap between log and alert performance. **Despite a strong log score of 76%, it reported a concerningly low alert score of just 5%,** indicating severe inefficiencies in correlation, rule logic, or alert thresholds.

Log Score by Industry



Government and Non-Profits demonstrated the most balanced detection performance in 2025, achieving **a log score of 73%** and **a leading alert score of 50%.** This improvement suggests a strategic focus on both telemetry coverage and actionable detection content.

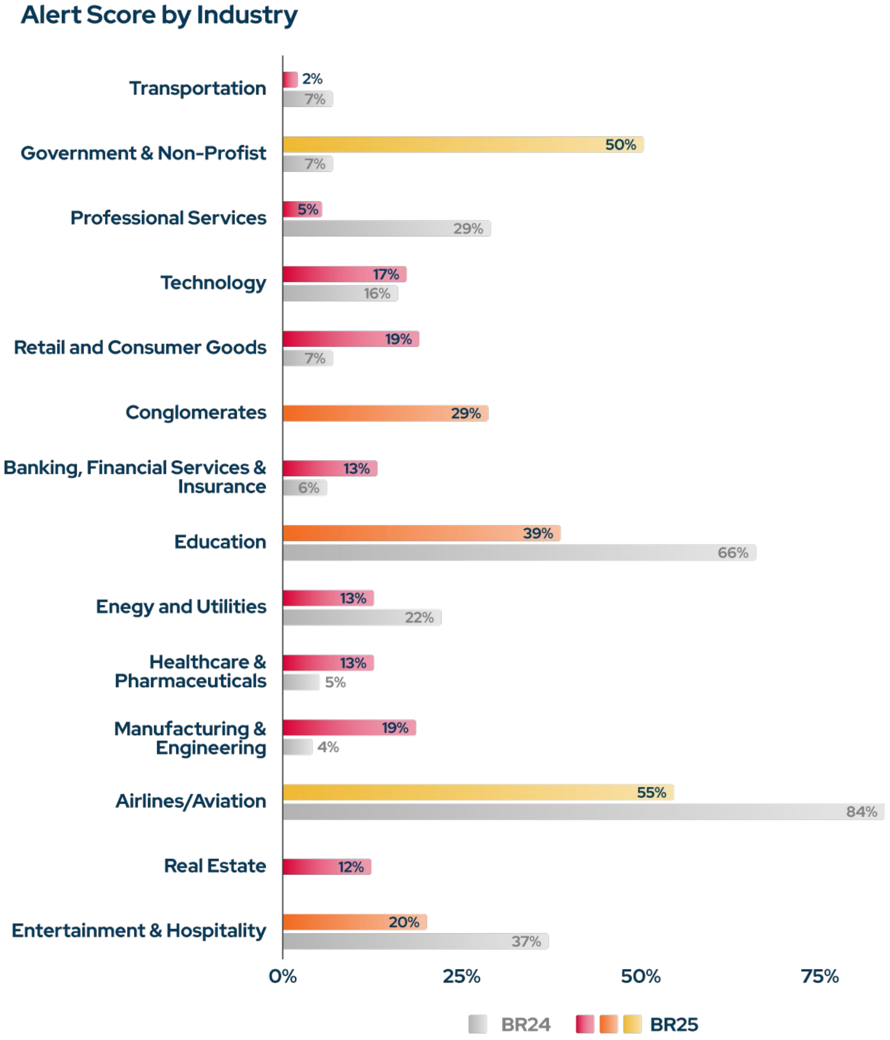
The Airlines/Aviation sector, often constrained by legacy systems and real-time operations, recorded **a low log score of 43%** but **a surprisingly high alert score of 55%.** This unusual inversion suggests tight filtering and highly tuned rule sets, though it also raises concerns about blind spots where threats may go unlogged and undetected.

Banking, Financial Services, and Insurance (BFSI) continued to perform within a managed range, **with a log score of 67% and an alert score of 13%.** The low alerting rate highlights the sector's need to better correlate threat behaviors and reduce latency between event ingestion and incident escalation.

Several other sectors, including **Healthcare and Pharmaceuticals, Energy and Utilities, and Manufacturing and Engineering,** clustered around **50–70% log scores but only 13–19% alert scores,** reinforcing that the log-to-alert conversion gap remains a systemic issue.

Notably, **Technology and Education** underperformed on both fronts. **The Technology sector's log score was just 47%, with a 17% alert score, while Education logged 45% of threats and generated alerts only 39% of the time.**

These scores suggest visibility and detection maturity remain uneven across digital-native and resource-constrained environments alike.

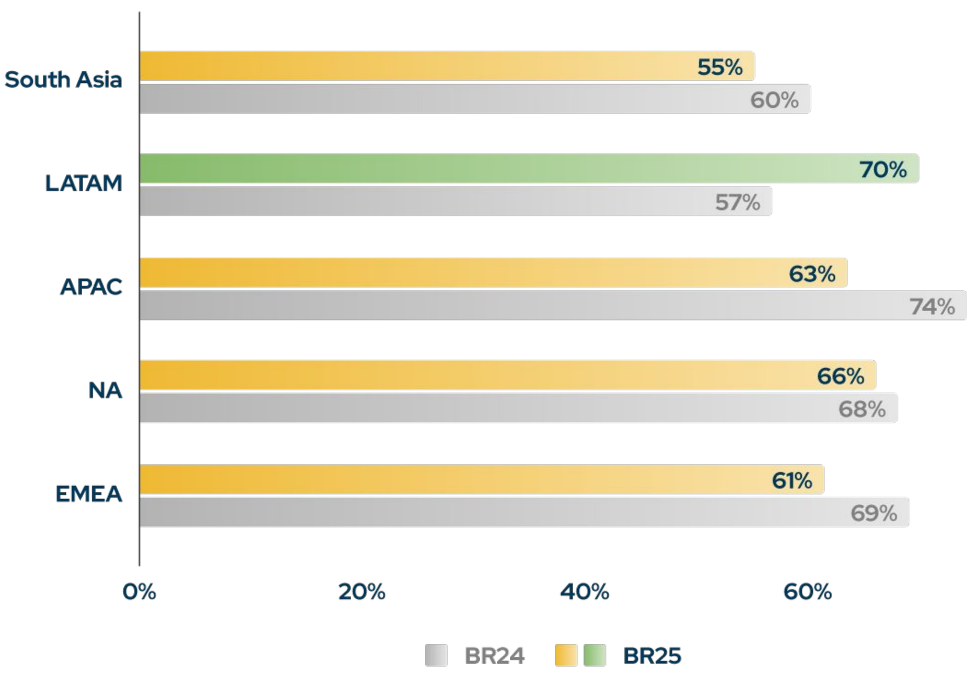


Performance by Region

Prevention Effectiveness

In 2025, prevention effectiveness scores ranged from moderate to managed levels across most regions, with notable shifts from the previous year.

Prevention Score - Region



Latin America (LATAM) emerged as the strongest performer in prevention, achieving a **70% prevention effectiveness rate,** reflecting gains likely driven by increased investment in control testing and modernization initiatives. Close behind, **North America (66%) and Asia-Pacific (63%)** continued to demonstrate solid but plateauing performance, suggesting a need to revalidate existing controls and address signs of stagnation.

EMEA, once a leader in **prevention, dropped to 61%,** likely due to widening resource gaps between large and mid-sized enterprises and the increasing complexity of hybrid environments. Meanwhile, **South Asia** remains **the most exposed region in 2025** with a **prevention score of 55%**, a figure that reflects systemic challenges in maintaining security controls.

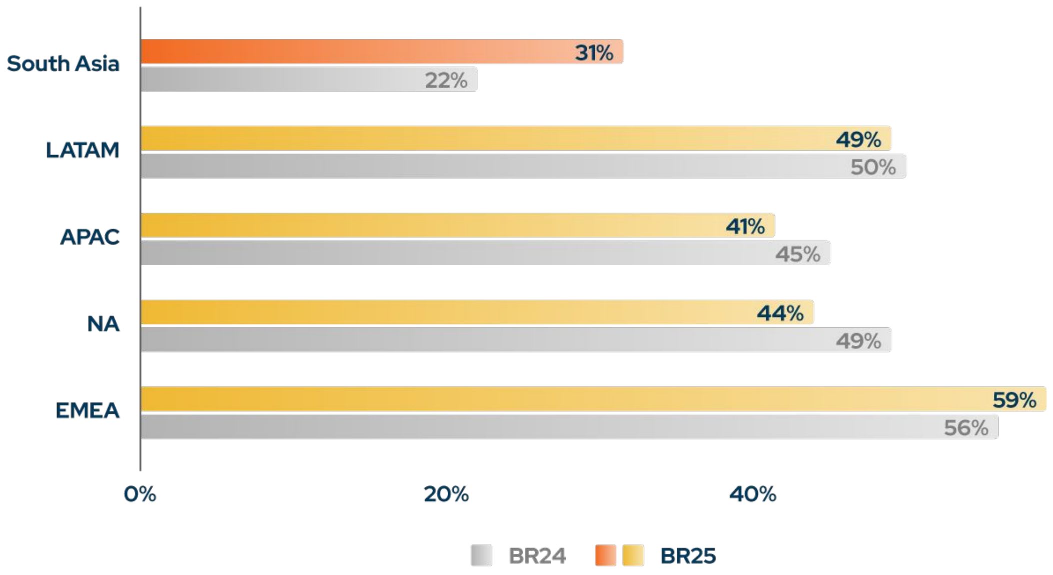
Across all regions, these results indicate that control effectiveness is not static. Without frequent validation and tuning, even high-performing regions risk regression over time.

Detection Effectiveness

Detection performance in 2025 remains markedly uneven across regions, with wide gaps between telemetry coverage and actionable alerting.

EMEA led all regions in **log score (59%),** suggesting significant improvement in telemetry collection and visibility across SIEM environments. However, the region's **alert score (20%),** while higher than previous years, still indicates inefficiencies in correlating and escalating threat signals.

Log Score - Region

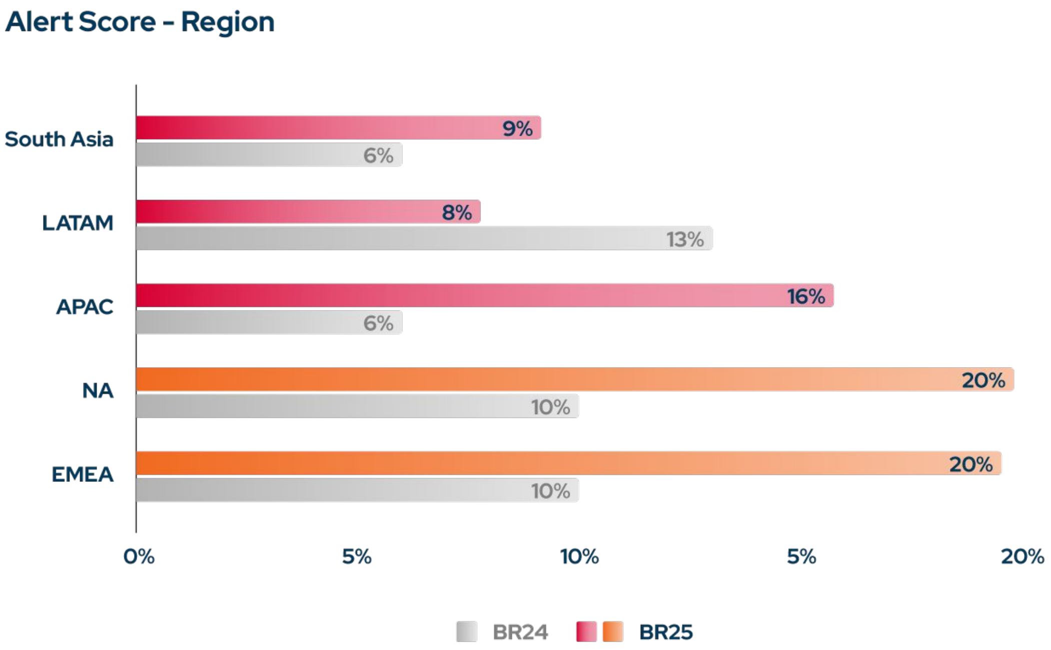


North America, while maintaining a l**og score of 44%**, achieved **the highest alert score of 20%.** This shows a relatively tuned detection pipeline, where fewer but better-targeted logs are successfully triggering alerts. Still, the region's logging coverage remains below optimal levels and could hinder long-term detection scalability.

Asia-Pacific (APAC) reported **a log score of 41% and an alert score of 16%,** reflecting a small rebound after last year's drop. However, continued issues with fragmented infrastructure and inconsistent log forwarding suggest that many APAC organizations still lack the telemetry depth required for high-confidence detection.

Latin America (49%) and South Asia (31%) trailed in detection visibility. **Alarmingly, South Asia's alert score was just 9%, the lowest across all regions.** Combined with its low prevention effectiveness, this indicates a critical detection readiness gap in the region.

LATAM also struggled to convert logs into alerts, with a detection **alert rate of just 8%,** suggesting that while visibility is improving, rule tuning and alert generation remain underdeveloped.

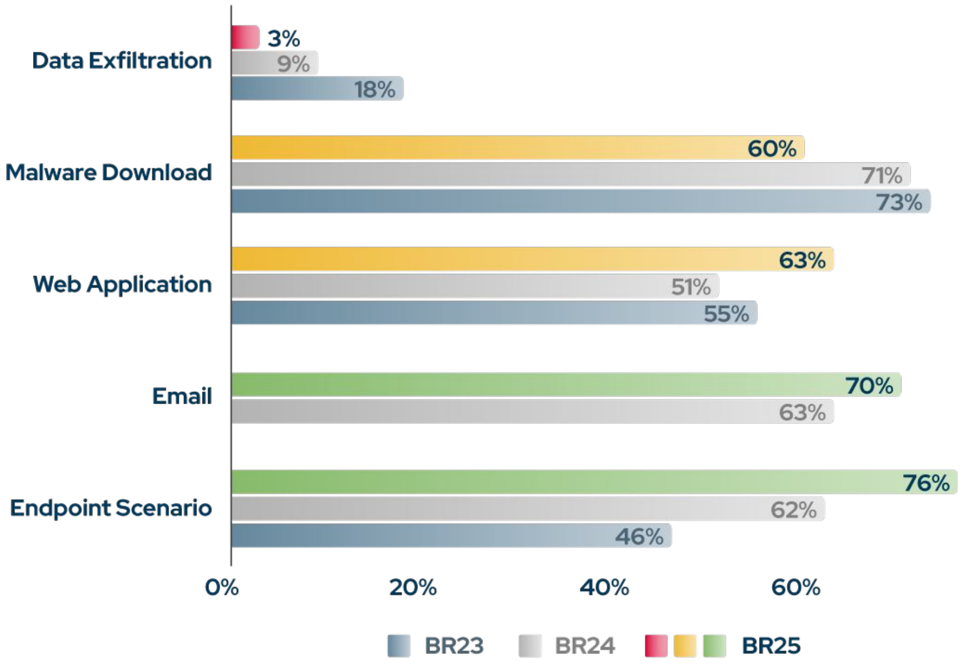


While some regions are progressing in detection maturity, telemetry coverage, and detection engineering remain significant weak points globally. Bridging the gap between log ingestion and actionable alerting requires not only better tools but continuous validation of rule logic, alert thresholds, and log source health tailored to each region's operational context.

Performance by Attack Vector

This year's findings continued to vary widely depending on the type of attack vector, highlighting the importance of validating controls across the entire kill chain. While many organizations have improved defenses against common attack paths, others remain critically underprepared to stop tactics that lead to sensitive data loss.

Prevention Effectiveness Score by Attack Vector



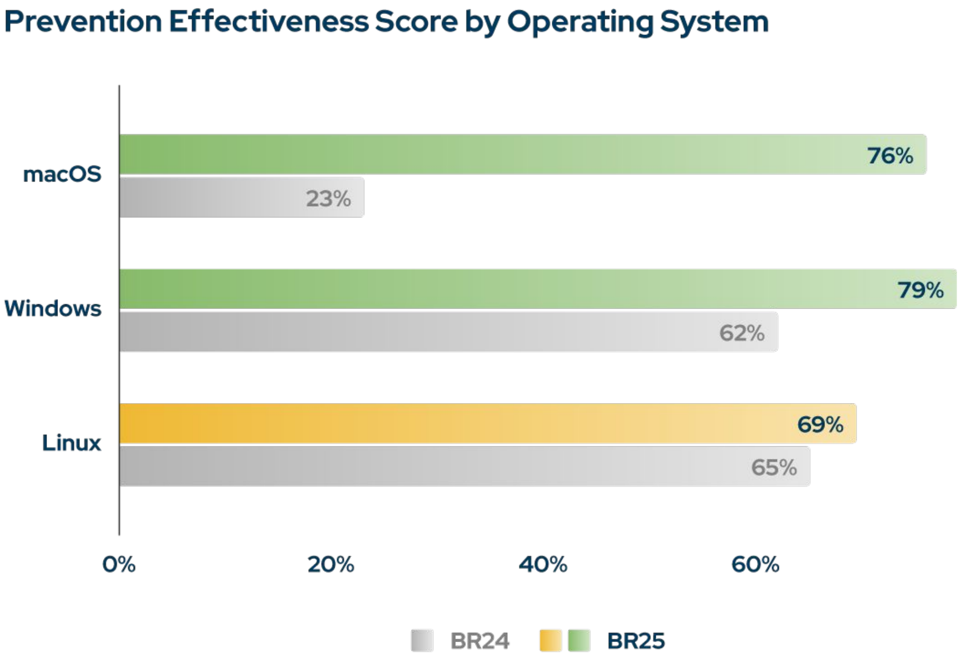
Once again, **data exfiltration** emerged as **the least prevented attack vector,** with effectiveness plummeting to just **3%, down from 9% in 2024.** This steep drop comes at a time when infostealer activity has surged threefold (as reported in the Red Report 2025), and ransomware operators increasingly rely on double extortion techniques to pressure victims. Despite these growing threats, most organizations lack the granular outbound monitoring and detection logic needed to block covert data theft.

Prevention against endpoint scenarios improved further in 2025, reaching 76%, as organizations continued to invest in EDR solutions and policy hardening. The increase suggests that security teams are more effectively identifying and stopping post-compromise activity, particularly lateral movement and privilege escalation.

Email-borne threats remained one of the most targeted vectors in 2025, but prevention effectiveness rose to 70%, reflecting improved phishing detection, attachment sandboxing, and URL analysis capabilities across email security gateways. Still, consistent testing of email modules and coverage of business email compromise (BEC) tactics remains essential.

Web application attacks were prevented 63% of the time, up slightly from **last year's 51%.** This improvement may be attributed to better WAF tuning and more frequent testing of authentication and input validation controls. However, given the widespread reliance on web platforms for customer-facing operations, even a modest prevention gap can result in substantial risk.

Prevention effectiveness for malware download scenarios declined to 60%, down from 71% in 2024. This drop is especially concerning given that malware delivery is one of the oldest and most well-understood attack vectors. Despite its familiarity, many organizations are dropping the ball on detection and blocking of malicious payloads, particularly those delivered through legitimate-looking or compromised infrastructure. As loaders and droppers continue to evolve and evade traditional defenses, frequent validation of download scenarios remains critical to prevent initial access and downstream compromise.

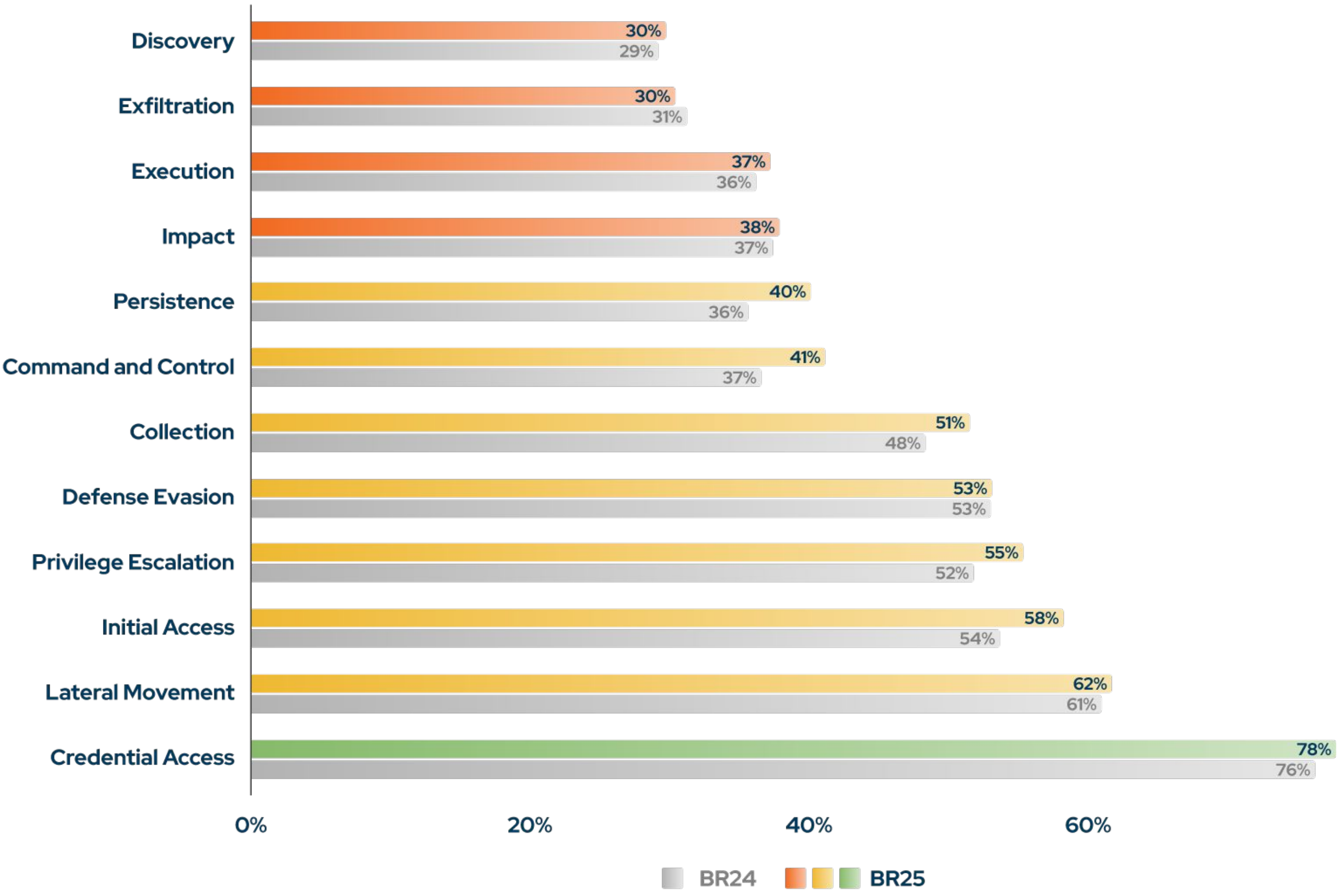


A breakdown by operating system shows that **Windows endpoints led at 79%, followed by macOS at 76%, which marks a significant leap from last year's 23%.** This reversal shows the growing maturity in securing macOS environments, which had long lagged behind.

Linux systems maintained solid defensive performance at 69%, though tuning coverage for hybrid environments remains a challenge.

Performance by MITRE ATT&CK® Tactics

The MITRE ATT&CK® framework continues to serve as a strategic lens for assessing security readiness across the entire adversary kill chain. **In 2025, Picus simulations once again measured prevention effectiveness across the 14 tactics defined in the ATT&CK Enterprise matrix.** The results reveal a clear divide between early-stage and post-compromise defenses, with several persistent blind spots that adversaries continue to exploit.



As in previous years, **Discovery** was **the least prevented tactic, with a prevention effectiveness score of 29.75%.** This reflects the continued difficulty organizations face in detecting low-noise reconnaissance behaviors such as account enumeration, host discovery, and network scanning activities that frequently go unnoticed until later stages of an attack.

Exfiltration closely followed **at 30.37%**, reinforcing a troubling trend. Despite the growing prevalence of infostealers and the rise of double extortion ransomware tactics, most organizations still lack detection mechanisms to prevent the transfer of sensitive data. These low scores highlight a critical blind spot in coverage.

Execution (37.21%), Impact (37.84%), and Persistence (40.10%) tactics also ranked among the least prevented. These stages involve actions such as script execution, payload deployment, service abuse, and sabotage, all of which remain difficult to catch without tightly configured endpoint controls and host-level monitoring. The persistently low scores suggest that many organizations continue to struggle with visibility and control inside the endpoint layer, especially post-initial access.

Tactics such as Command and Control (41.15%), Collection (51.48%), and Defense Evasion (53.05%) showed moderate prevention scores, but still leave ample room for improvement. The variability in these scores points to inconsistent network telemetry coverage, lack of deep packet inspection, and limited visibility into living-off-the-land techniques, which attackers frequently use to bypass legacy defenses.

Encouragingly, organizations performed better against early and privilege-oriented tactics. **Initial Access (58.19%), Lateral Movement (61.68%), and Privilege Escalation (55.32%)** all showed improvement, reflecting gains made through email security, identity-based segmentation, and endpoint control validation.

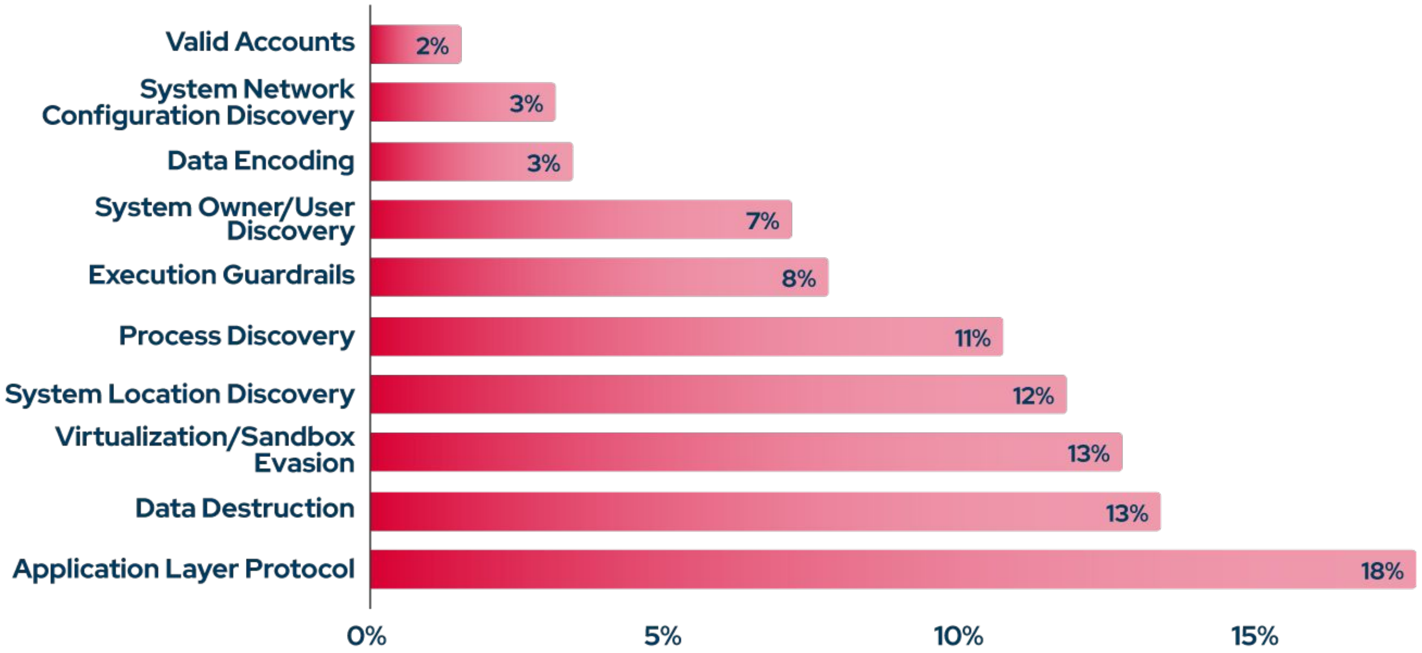
The standout performer in 2025 was Credential Access, with a prevention effectiveness of 77.71%. This suggests that password policy enforcement, credential hardening, and memory protection mechanisms are becoming more effective at limiting access to authentication material, though the rise in hash cracking success (reported separately in this report) indicates that downstream use of credentials remains a concern.

In conclusion, while progress has been made in initial access and privilege defense, critical gaps remain in lateral awareness, outbound data detection, and stealthy attacker behaviors. To truly align with the ATT&CK framework, organizations must continuously validate not only control presence but also control performance at every phase of the attack lifecycle.

Performance by MITRE ATT&CK® Techniques

Beyond evaluating prevention at the tactic level, this year's findings also reveal that some of the most fundamental and frequently used techniques remain poorly prevented, particularly those related to **Discovery, Credential Access, Defense Evasion, and Command and Control.**

These findings highlight the need for organizations to strengthen their behavioral analysis and detection capabilities, **moving beyond static rule-based logic to identify subtle, context-driven attacker behaviors commonly used across both malware and APT campaigns.**



Valid Accounts (T1078), a technique used for initial access and persistence, was the least prevented technique in 2025, with a **prevention rate of just 2%.** This reflects the persistent difficulty organizations face in detecting attackers who reuse stolen or weak credentials to blend in with legitimate user activity. As more campaigns employ tactics like password spraying, MFA fatigue, and token hijacking, validating controls against credential-based access has become essential to defending against lateral movement and privilege escalation.

A cluster of discovery techniques also ranked among the least prevented. These methods are typically used early in an attack to map out the environment and locate valuable assets. **System Network Configuration Discovery (T1016)** was **prevented only 3% of the time,** while **System Owner/User Discovery (T1033), Process Discovery (T1057), and System Location Discovery (T1614.001) scored 7%, 11%, and 12%,** respectively. Despite their simplicity, these tactics are often overlooked by controls that prioritize high-severity threats. Their low prevention rates suggest a widespread lack of behavioral visibility into reconnaissance activities, especially when such actions are executed using native tools or administrative interfaces.

Defense evasion techniques also continue to evade traditional prevention mechanisms. **Execution Guardrails (T1480.001) had a prevention score of just 8%, and Virtualization/Sandbox Evasion (T1497) followed closely at 13%.** These methods allow adversaries to avoid detection by disabling or bypassing analysis environments, causing malware to remain inactive unless executed under real-world conditions. The low prevention rates indicate that many endpoint and sandbox solutions fail to fully emulate user or system behavior, providing adversaries with a clear advantage during staged deployments or delayed execution attacks.

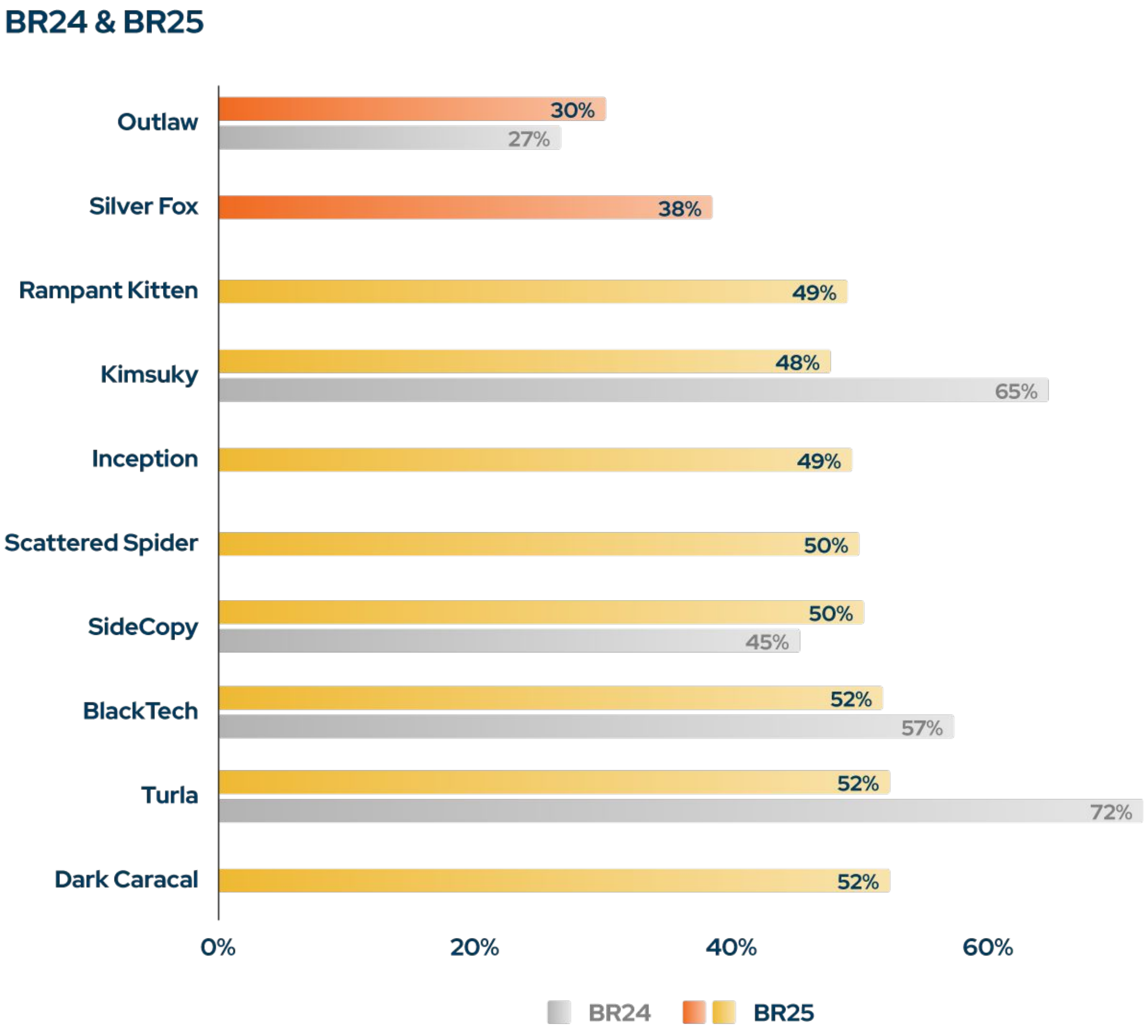
When it comes to command and control techniques, **Data Encoding (T1132),** which is used to obfuscate outbound communications, **had a prevention rate of just 3%,** highlighting weak detection of manipulated or encoded traffic leaving the network. Similarly, **Application Layer Protocol (T1071),** which enables adversaries to establish command and control over common protocols such as HTTPS, DNS, or SMTP, was **only prevented 18% of the time.** These low scores reflect the challenge of distinguishing malicious traffic from legitimate communication, particularly in environments that lack deep packet inspection, TLS decryption, or behavior-based anomaly detection.

In comparison, **Data Destruction (T1485),** an impact technique frequently observed in ransomware and wiper campaigns, had a **prevention effectiveness of just 13%.** This suggests that many organizations still lack the behavioral controls necessary to detect rapid file encryption or deletion, leaving them exposed to destructive actions once an attacker gains initial access.

Performance by Threat Group

Organizations' ability to prevent real-world adversaries continues to vary significantly by threat group. This year's findings reaffirm a familiar challenge: advanced actors, especially those combining espionage tradecraft with modern malware and evasive techniques, routinely bypass conventional defenses.

Notably, half of the least prevented threat groups in this year's analysis are newly prominent or previously unranked, appearing in the Blue Report for the first time. This shift highlights a growing gap between emerging threats and existing defensive coverage. As new campaigns surface and attacker behaviors evolve, many organizations struggle to adapt detection content and validation strategies fast enough, particularly when adversaries operate outside the bounds of known playbooks.



Outlaw, with a prevention score of just 30%, emerged as the most successful threat group in evading defenses this year. Known for its opportunistic attacks across sectors, Outlaw blends cryptojacking, botnet activity, and lateral movement often flying under the radar of conventional network controls.

Also among the least prevented were **Silver Fox (38%),** an emerging APT group leveraging loader frameworks and obfuscated malware, and **Dark Caracal (52%),** a persistent espionage group with ties to mobile surveillance and hybrid cyber operations. These new groups were not in last year's threat group analysis, yet now represent some of the most difficult to defend against.

Established espionage groups like **Kimsuky (48%), Rampant Kitten (49%), and Inception (49%) also ranked among the lowest in prevention.** These actors continue to exploit social engineering, macro-based payloads, and native system tools to avoid triggering traditional prevention logic. Their tactics emphasize quiet persistence and stealth, often bypassing controls focused only on known malware signatures.

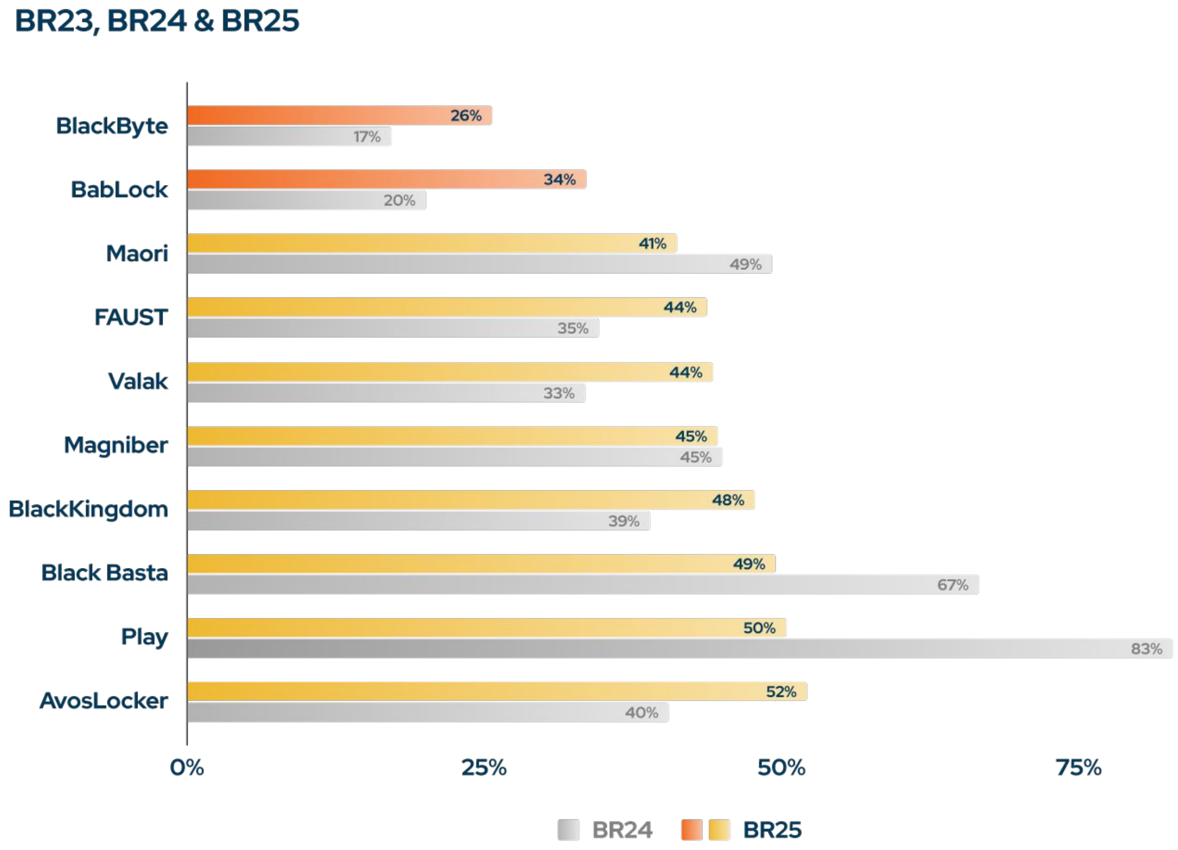
SideCopy (50%) and BlackTech (52%), known for targeting South Asian and East Asian government and defense sectors, respectively, further demonstrate that living-off-the-land and modular backdoor techniques remain effective when controls are not thoroughly validated.

Scattered Spider, a financially motivated group known for SIM swapping, identity abuse, and cloud account takeover, had a **prevention score of 50%.** Despite heightened awareness following their high-profile ransomware and extortion attacks, Scattered Spider's manipulation of identity systems and MFA fatigue tactics continues to bypass defenses in environments lacking strong identity and behavioral analytics.

Even longstanding APTs like **Turla (52%),** with decades of experience in stealthy operations, continue to evade defenses through sophisticated command-and-control channels, staged loaders, and custom implants. Their continued success highlights how legacy groups can maintain effectiveness simply by evolving quietly, taking advantage of control fatigue and assumption-based coverage.

Spotlight on Ransomware Attacks

Ransomware remains one of the most persistent and destructive threats facing organizations worldwide. In 2025, our research revealed that many ransomware strains continue to evade defenses with ease. Despite heightened awareness and investments in ransomware resilience, prevention effectiveness against leading ransomware families remains alarmingly low.



For the second consecutive year, **BlackByte** ranked as the least prevented ransomware variant, with a **prevention effectiveness score of just 26%.** Known for exploiting public-facing applications and moving quickly to exfiltrate and encrypt sensitive data, BlackByte continues to bypass traditional controls, particularly in environments lacking behavioral monitoring and outbound traffic filtering.

BabLock (34%) and Maori (41%) followed closely behind. Both ransomware families use modular payloads, anti-analysis techniques, and staged execution patterns that evade static detection and sandbox inspection. BabLock, in particular, has leveraged double extortion techniques to increase pressure on victims, while Maori has gained traction through regional campaigns and fileless delivery tactics.

FAUST (44%), Valak (44%), and Magniber (45%) showed similar prevention gaps, suggesting that many organizations still lack adequate coverage for file encryption behavior, registry modifications, and lateral movement within endpoint environments.

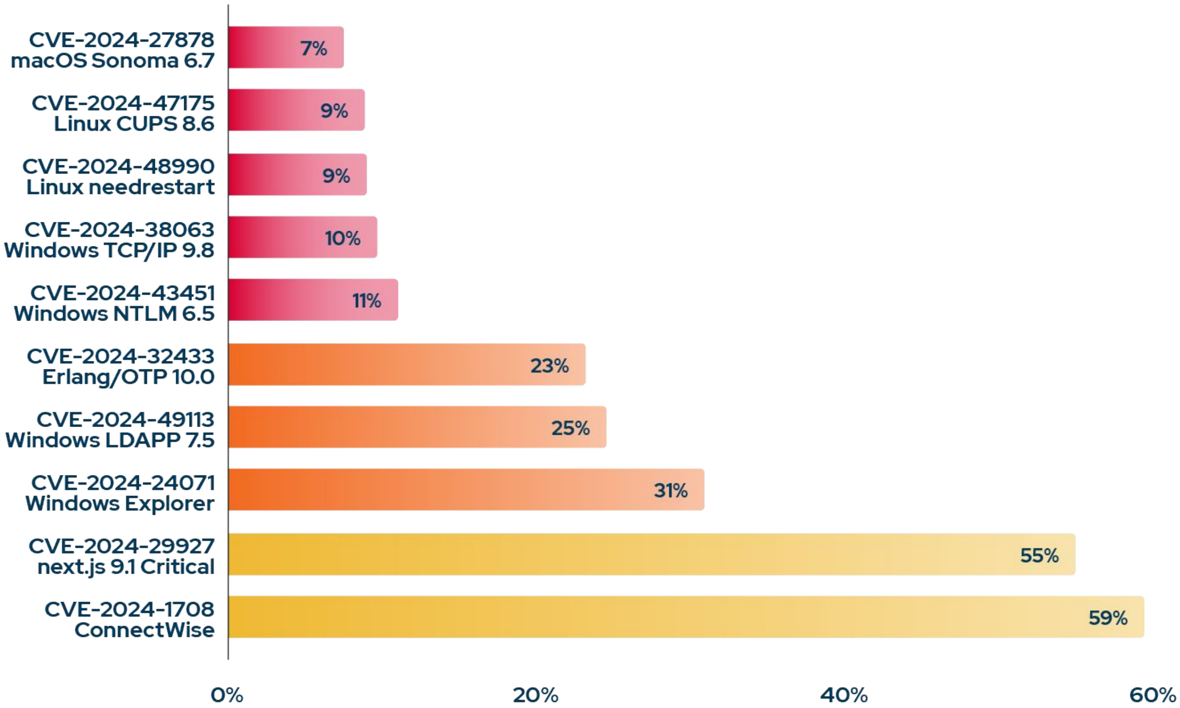
BlackKingdom (48%), Black Basta (49%), and Play ransomware (50%) continued to demonstrate evasiveness through stolen credential abuse, process hollowing, and remote service execution. Despite being well-documented, these strains remain difficult to prevent, highlighting how organizations are struggling to maintain effective prevention against ransomware.

Organizations achieved a 52% prevention rate against AvosLocker, meaning nearly half of simulated attacks were successful. Known for targeting critical sectors using privilege escalation and advanced obfuscation techniques, **AvosLocker remains a significant threat.**

Spotlight on Vulnerabilities

For the 2025 edition of the Blue Report, we narrowed our vulnerability analysis to CVEs disclosed in 2024 and 2025, offering a focused view into how well organizations are preventing exploitation of recently found vulnerabilities. This shift allows for a more accurate assessment of how quickly security controls adapt to newly emerging threats.

The findings reveal that many recent vulnerabilities remain underprotected, **with several CVEs exhibiting prevention effectiveness rates below 10%, despite widespread public disclosure and the availability of patches or signatures.** This highlights a continued lag in patch prioritization, virtual patching, and threat-informed validation.



At the bottom of the list, **the macOS Sonoma CVE-2024-27878 vulnerability was the least prevented vulnerability**, with just 7% of simulated exploit attempts successfully blocked. Close behind were **Linux CUPS CVE-2024-47175** vulnerability (9%), **Linux needrestart library CVE-2024-48990** vulnerability (9%), and **Windows TCP/IP CVE-2024-38063** vulnerability (10%). Other vulnerabilities like **Windows NTLM CVE-2024-43451** vulnerability (11%) and **Erlang/OTP CVE-2025-32433** vulnerability (23%) also remained underprotected, despite growing exploitation activity. These low scores suggest that many organizations are slow to patch known vulnerabilities in operating systems.

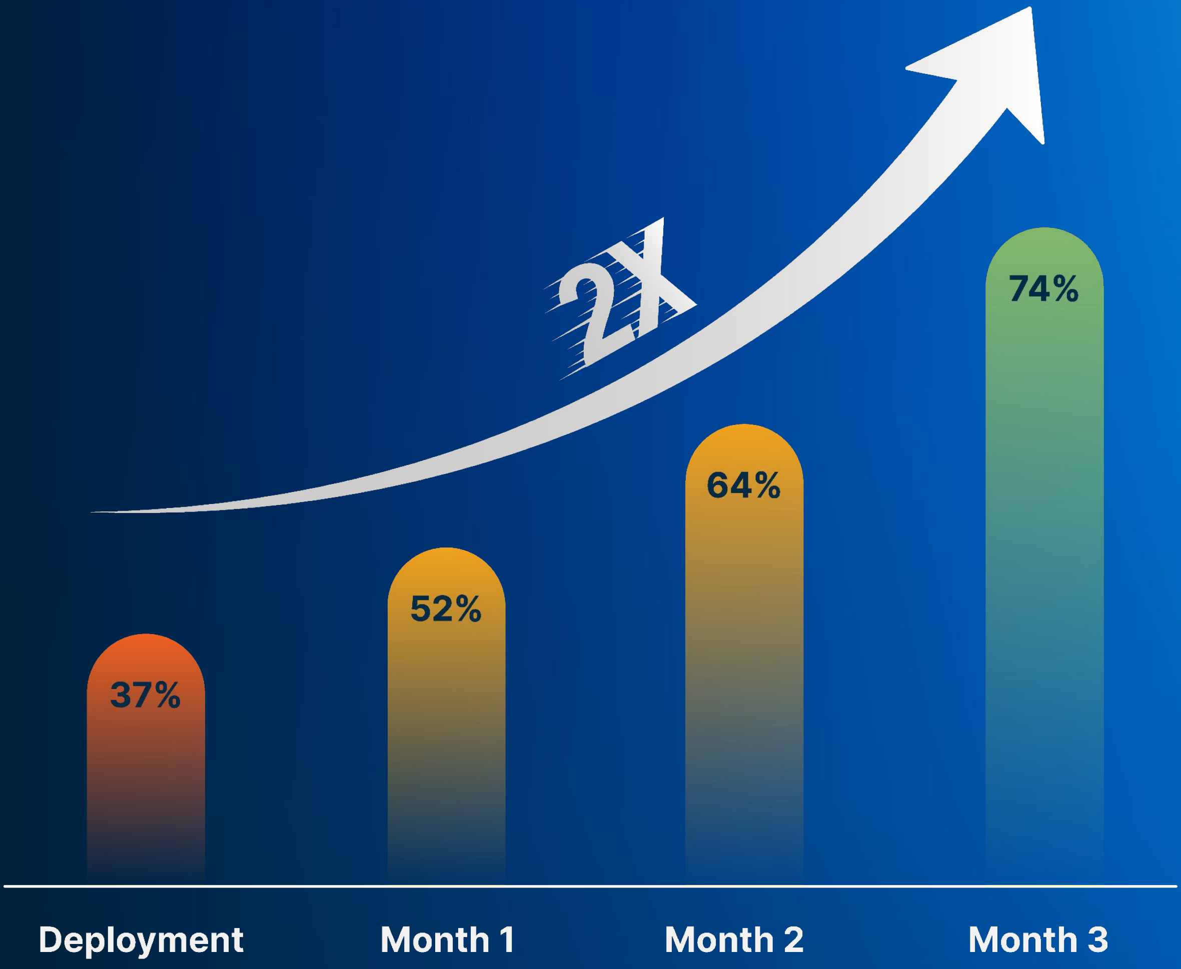
Encouragingly, some CVEs showed moderate levels of prevention. **Windows LDAP CVE-2024-49113 vulnerability and Windows Explorer CVE-2025-24071 vulnerability were blocked in 25% and 31% of simulations,** respectively, still below ideal thresholds, but a signal that certain threat intelligence and operating system updates are being operationalized more effectively.

Critical web application vulnerabilities such as **next.js CVE-2025-29927 vulnerability (55%) and ConnectWise ScreenConnect CVE-2024-1708 vulnerability (59%)** achieved moderate levels of prevention scores among recent vulnerabilities tested. While it's promising that some exploit attempts are being blocked more reliably, even these figures reflect that nearly half of attack attempts still succeed.

These results highlight that many organizations struggle to patch operating systems and critical web applications in a timely manner. In such cases, it becomes essential to have effective compensating controls, such as WAFs, endpoint protection, and intrusion prevention systems that can detect and block exploit attempts tied to recent CVEs.

Whether through patching or mitigation, organizations must ensure that vulnerabilities are addressed before they can be weaponized. This is particularly important for zero-day and n-day vulnerabilities, where the window between public disclosure and exploitation is often too short for traditional patch cycles to keep up.

Picus Security Customers *Prevent Twice As Many Attacks*



Picus Security provides an exposure management solution - the Picus Security Validation Platform, powered by our Security Control Validation (SCV), Cloud Security Validation (CSV), Attack Path Validation (APV), Detection Rule Validation (DRV), and Attack Surface Validation (ASV) to help organizations of all sizes continuously validate and reduce their cyber risk. Security teams can evaluate the effectiveness of their security controls, discover at-risk assets and identify high-risk attack paths that attackers could use to access critical systems and users.

On average, our customers prevent twice as many attacks, within just three months (see chart above). With Picus Security, security leaders can quickly mature their security posture and move beyond basic vulnerability management. Instead of spending their days making impossible trade-offs that may leave gaps in their defenses, they can consistently and successfully defend against sophisticated multi-pronged attacks.

About Picus Security

Picus Security is the pioneer of Adversarial Exposure Validation, enabling organizations to understand and reduce cyber risk with precision and speed. The Picus Security Validation Platform empowers security teams to continuously correlate, prioritize, and validate exposures across on-premises, cloud, and hybrid environments.

By simulating real-world attacker behaviors and validating control effectiveness, Picus helps teams focus on critical gaps and high-impact fixes, rather than managing siloed alerts or theoretical risks. With ready-to-deploy mitigations and actionable guidance, the Picus Platform makes it easier to stop more threats with less effort.

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

BLUE REPORT™ 2025