seemplicity

2026 Exposure Action Report

Real-World Insights on Tool Sprawl, AI Adoption, and the State of Remediation

Executive Summary

Exposure management has entered a new phase. For most organizations, the challenge is no longer discovering vulnerabilities, it is managing remediation activities that continues to scale year over year. As security programs mature and detection coverage expands, the gap between what tools surface and what teams can realistically fix has become one of the primary constraints on reducing risk.

This report looks at what exposure management looks like in practice. The insights are based on aggregated remediation and operational data observed across modern security environments throughout 2025. During this period, organizations processed an average of 67.3 million findings per year and relied on an average of seven security scanning tools across infrastructure, cloud, and application environments. Coverage is broad, but the nature of the risk is familiar. The most common issues are not novel or sophisticated attacks, they are repeatable and well understood problems that appear again and again, particularly in cloud-native and containerized environments. These issues persist not because teams are unaware of them, but because execution does not scale as easily as detection.

The data also presents a more realistic picture of efficiency. Organizations continue to reduce remediation backlogs and reclaim meaningful time and cost, but progress is no longer automatic. Gains depend on focus and discipline, not just tooling. At this level of scale, success is not defined by finding more issues, but by executing remediation efficiently through consolidation, prioritization, and scalable remediation practices. When security meets reality, exposure management success is measured by outcomes, not activity output. This report provides a view into what it takes to actually reduce risk under those conditions.

About the Data

The findings in this report are derived from aggregated and anonymized exposure management data collected from Seemplicity's SaaS Platform during 2025. The analysis focuses on remediation activity and how findings are prioritized, coordinated, and addressed by teams. This reveals operational patterns that are not visible in tool-specific or alert-level data. All data has been anonymized, and the insights presented reflect trends in exposure management rather than individual organizational performance.

Who the Data Represents

Exposure management is no longer a problem limited to a small set of technology-first organizations. The data reflected in this report represents organizations operating across a wide range of industries, each with its own mix of risk, regulatory pressure, and operational complexity. While the environments differ, the underlying challenge is the same. All of them are trying to manage exposure at a scale that keeps growing.

The industry mix observed in 2025 reflects this shift. Financial services represent the largest portion of the data, accounting for roughly 24 percent of observed environments, a sign of how closely exposure management has become tied to operational resilience and regulatory accountability. Manufacturing and healthcare also make up a meaningful share, representing about 10 percent and 9 percent respectively. In these environments, uptime, safety, and reliability matter just as much as traditional security concerns. Exposure management is no longer a background function, it is part of keeping the organization running.

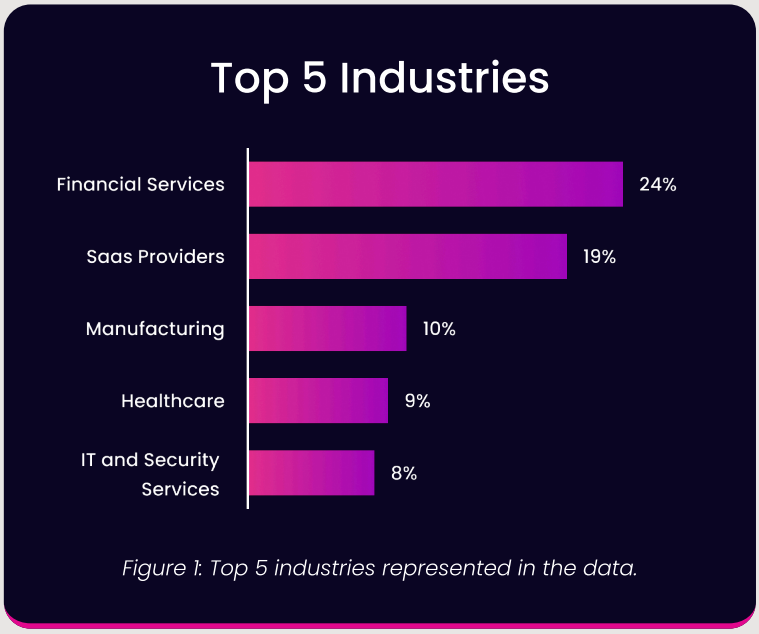

Figure 1: Top 5 industries represented in the data.

The data also spans organizations of very different sizes. The relatively even distribution across the three groups shows that size alone doesn't determine exposure management complexity. As infrastructure becomes more interconnected and tooling becomes more accessible, even smaller organizations are managing volumes of findings that require structured prioritization and coordinated remediation.

Figure 2: Organization sizes, measured by number of employees, represented in the data.

Taking Figures 1 and 2 together, this diversity reinforces an important point. The challenges described in this report are not unique to any single industry or company profile. They reflect a shared operational reality. Regardless of size or sector, organizations are facing the same fundamental question: How do you reduce exposure effectively when environments scale faster than remediation capacity?

The Scale of the Problem

Looking back at the findings from last year's analysis, this year's report shows that the scale at which organizations are managing exposure continues to grow. In 2025, organizations processed an average of 67.3 million findings, up from 48.6 million the year before. This increase is not simply a result of expanding attack surfaces. It can be explained, in part, by the industry's shift toward more continuous scanning, monitoring, and reassessment of environments.

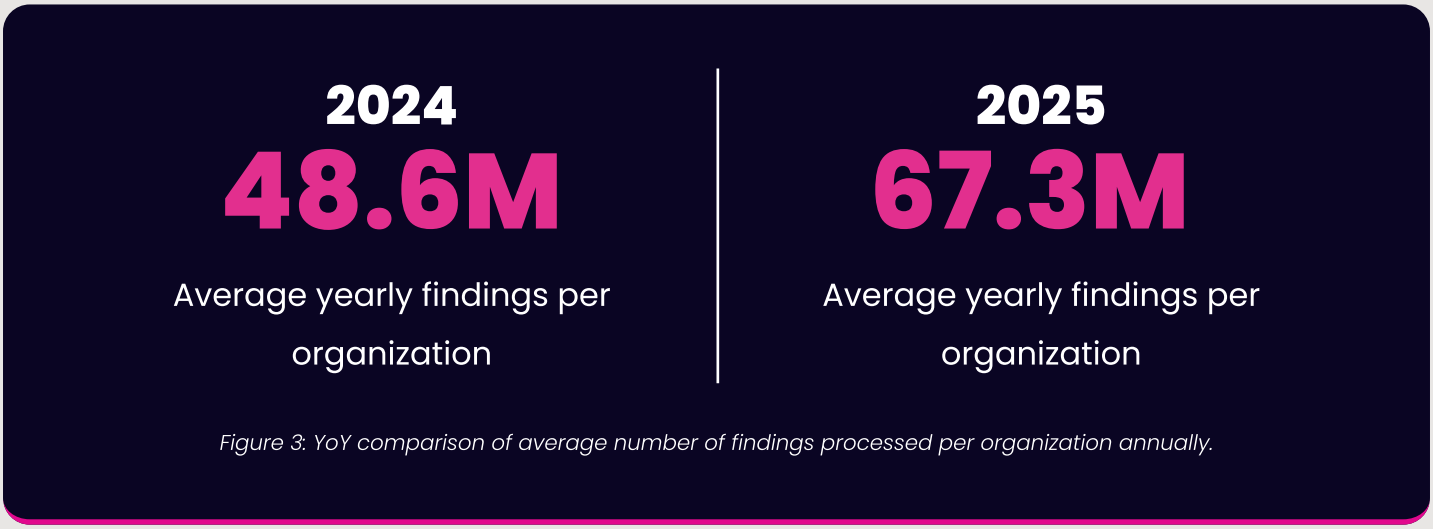

Figure 3: YoY comparison of average number of findings processed per organization annually.

At this volume, many of the assumptions that shaped traditional vulnerability management start to break down. Manual triage does not scale. Ticket-by-ticket remediation becomes unsustainable. Tool-by-tool prioritization makes it harder, not easier, to understand what actually needs attention. Even well-resourced teams are forced to make tradeoffs, not only about what to fix first, but about what may not get addressed at all.

What makes the problem more complex is that exposure does not grow in a smooth or predictable way. Volumes often spike alongside cloud adoption, infrastructure expansion, or the addition of new scanning tools. When that happens, remediation workflows feel the impact immediately. The constraint is no longer detection capacity, it is the ability to turn large volumes of findings into coordinated action across teams, processes, and tools.

At this scale, success is not defined by finding more issues, but by executing remediation efficiently through consolidation, prioritization, and scalable remediation practices.

Organizations that continue to rely on manual processes or fragmented workflows will struggle to keep pace. The following sections look at how teams are dealing with this reality, and what exposure management looks like when security meets peak execution.

Making Sense of Scale with AI

As findings volumes continue to grow, the challenge for security teams is no longer access to data. It is making sense of it quickly enough to act. At this scale, practitioners need help interpreting exposure, understanding context, and deciding what to do next.

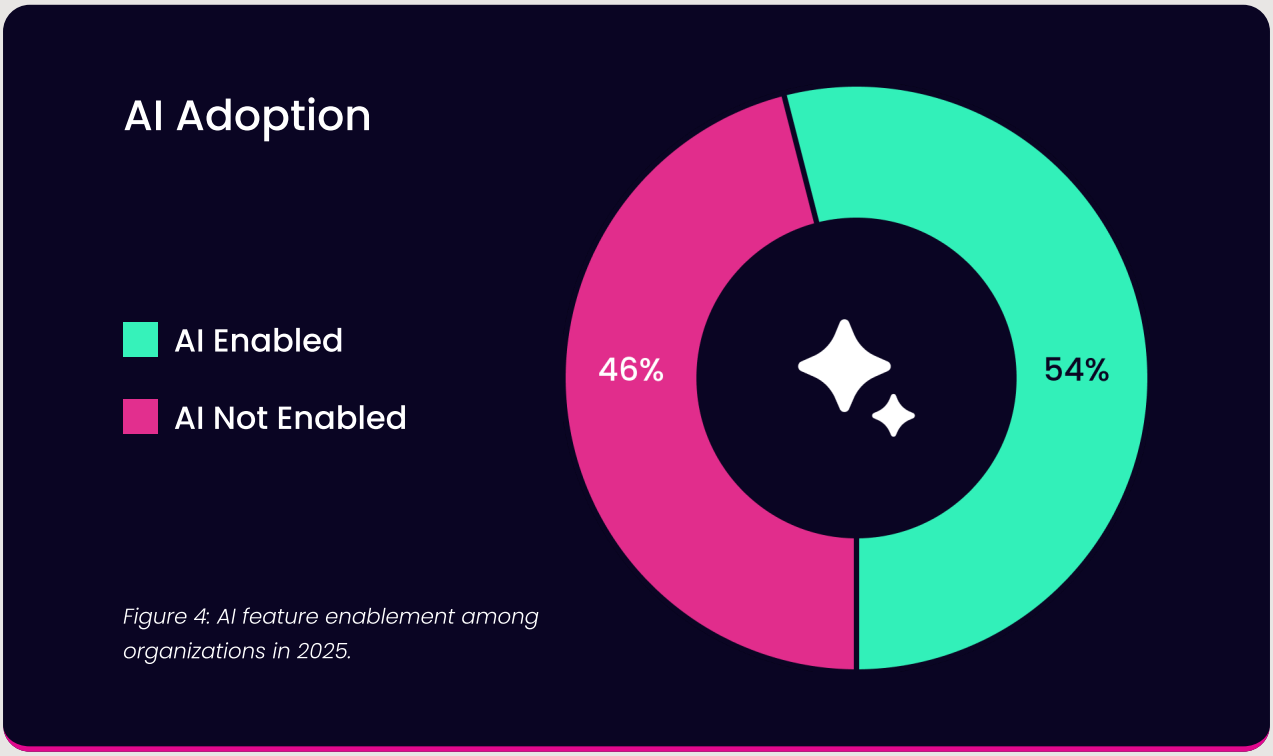

Figure 4: AI feature enablement among organizations in 2025.

In 2025, more than half of organizations using the Seemplicity platform enabled AI features. Adoption increased as AI capabilities matured and became embedded directly into exposure management workflows. This reflects growing comfort with using AI to support analysis and decision-making, rather than treating it as a standalone feature.

It is important to note that AI agents in the Seemplicity platform operate in a few distinct ways. The Clarity AI Agent provides always-on context inside findings, including AI-generated summaries, aggregated exposure details, and remediation context whenever users review their backlogs. In addition, teams interact directly with agents such as the Insights and Remediation agents when they need deeper analysis or guidance.

Usage patterns show that AI is being incorporated more and more into day-to-day work. On average, organizations used AI features more than two times per week as part of remediation workflows. These interactions represent deliberate use of AI to interpret data and accelerate remediation decisions, not one-time experimentation.

As exposure volumes continue to increase, AI is becoming a practical tool for sense-making. It helps teams cut through noise, focus on what matters, and move from findings to action more efficiently. In environments defined by scale, AI supports execution by augmenting human judgment, not replacing it.

Tooling Reality: Coverage vs. Complexity

Over the past several years, organizations have expanded their security tooling to improve visibility across infrastructure, cloud, and application environments. In 2025, organizations relied on an average of seven security scanning tools to identify and assess exposure, down from eight tools the year before. Tool sprawl has slowed, but simplicity has not followed.

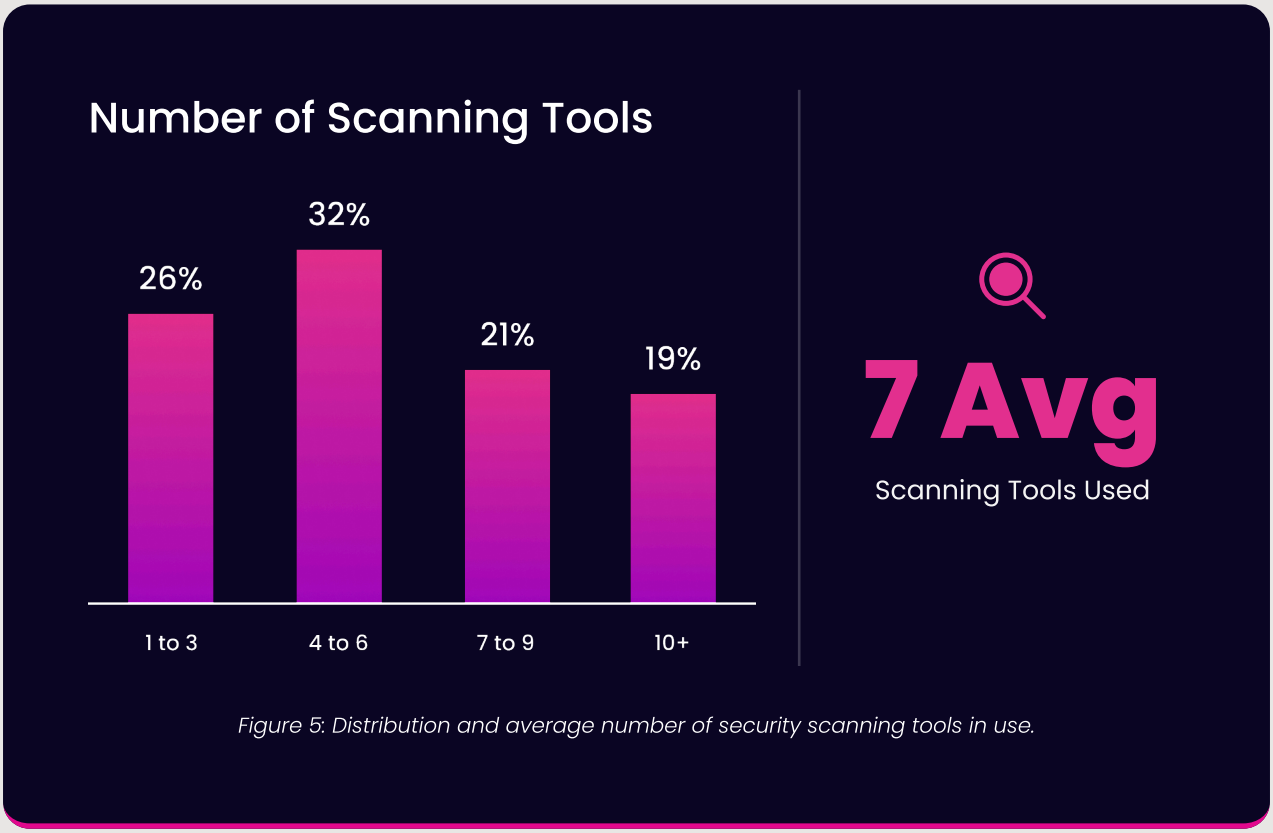

Figure 5: Distribution and average number of security scanning tools in use.

In some cases, this visibility has allowed organizations to simplify their tooling directly. In 2025, one organization identified a scanning tool that consistently produced redundant findings across the same assets and chose to retire it, without reducing overall coverage. This reflects a broader shift from accumulating tools toward understanding where they add distinct value.

Each tool still produces its own findings, severity models, and remediation guidance. In practice, this means multiple tools often assess the same underlying assets from different perspectives. While each tool provides useful context, the resulting findings tend to accumulate around shared resources. Findings volume continues to increase, but the picture does not necessarily become clearer.

This overlap creates real operational friction. Findings arrive through different systems, follow different workflows, and compete for attention across teams. Without consolidation, teams are left managing parallel queues that describe similar problems in slightly different ways. Over time, this fragmentation makes prioritization harder and remediation slower, even when coverage is strong.

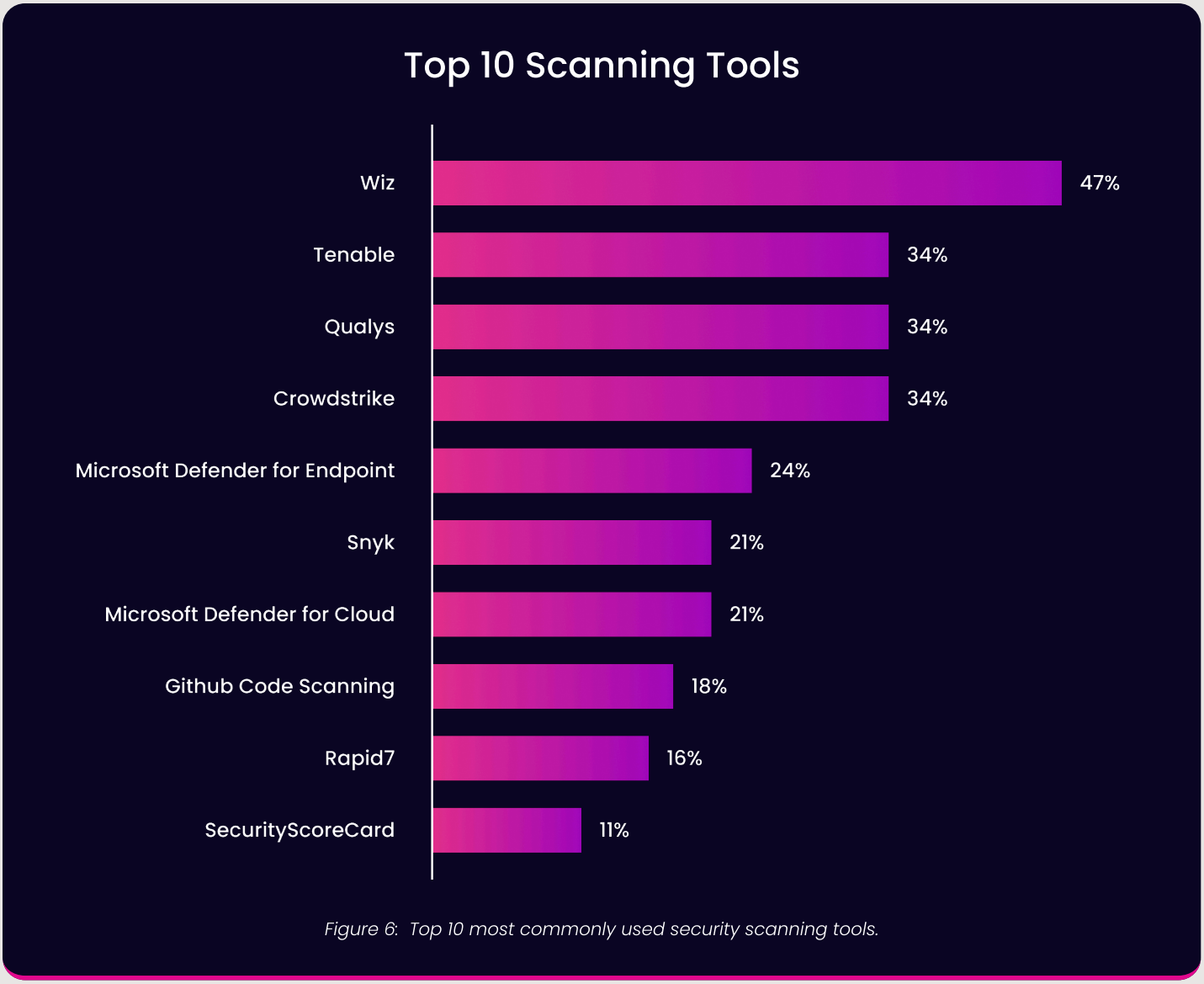

Figure 6: Top 10 most commonly used security scanning tools.

The most commonly used tools represented in the data span vulnerability management, cloud security, application security, and endpoint protection. This reflects the reality of modern environments. Comprehensive coverage requires multiple perspectives. The challenge is not tool selection. It is how effectively organizations translate coverage into coordinated action.

At this level of complexity, detection is no longer the differentiator, execution is. Organizations that succeed are able to reduce duplication, align findings across tools, and focus teams on fixes that address root causes rather than individual alerts. When security meets reality, the value of tooling is measured by how well it supports remediation, not by how much data it produces.

Where Risk Converges

When exposure management data is viewed at scale, risk doesn't appear evenly distributed across assets or categories. As shown in Figure 7 it converges around a small number of shared operational surfaces. Machines, more than anything else, stand out as a magnet for findings.

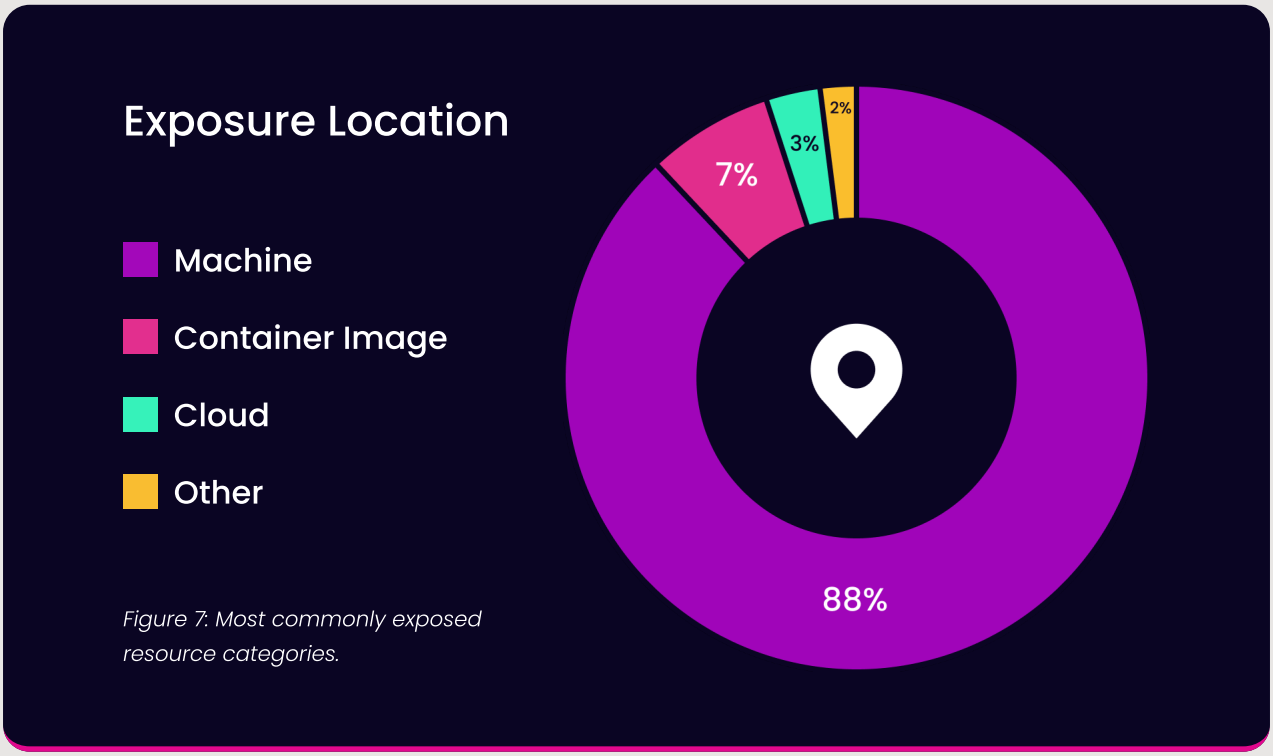

Figure 7: Most commonly exposed resource categories.

In 2025, a large portion of findings were associated with machine-level resources. This does not mean that all risk originates from infrastructure alone. It reflects how modern security tooling operates in practice. Many scanners, including cloud, container, endpoint, and vulnerability management tools, assess the same underlying machine assets. As noted earlier, each tool looks at those assets through a different lens, which means findings can point back to the same systems from multiple perspectives.

This convergence is not a detection problem. It is a structural reality of modern environments. Machines serve as the foundation for cloud workloads, container platforms, and application runtime environments. When multiple tools continuously assess those foundations, exposure accumulates in predictable places. For remediation teams, this means that a large share of their effort is driven by issues tied to the same underlying assets, even when the findings come from different tools.

For security leaders, the implication is practical. Effective exposure management at scale depends on recognizing where risk converges and responding accordingly. Progress comes from consolidating related findings, addressing root causes, and prioritizing fixes that reduce exposure across multiple tools and environments. Treating each finding or category in isolation makes convergence harder to manage, not easier.

The Reality of Modern Exposure

When exposure management data is viewed at scale, a consistent pattern emerges. The most common issues organizations deal with are not limited to a single domain or technology. Instead, exposure shows up across containers, cloud infrastructure, and widely used software components, often at the same time.

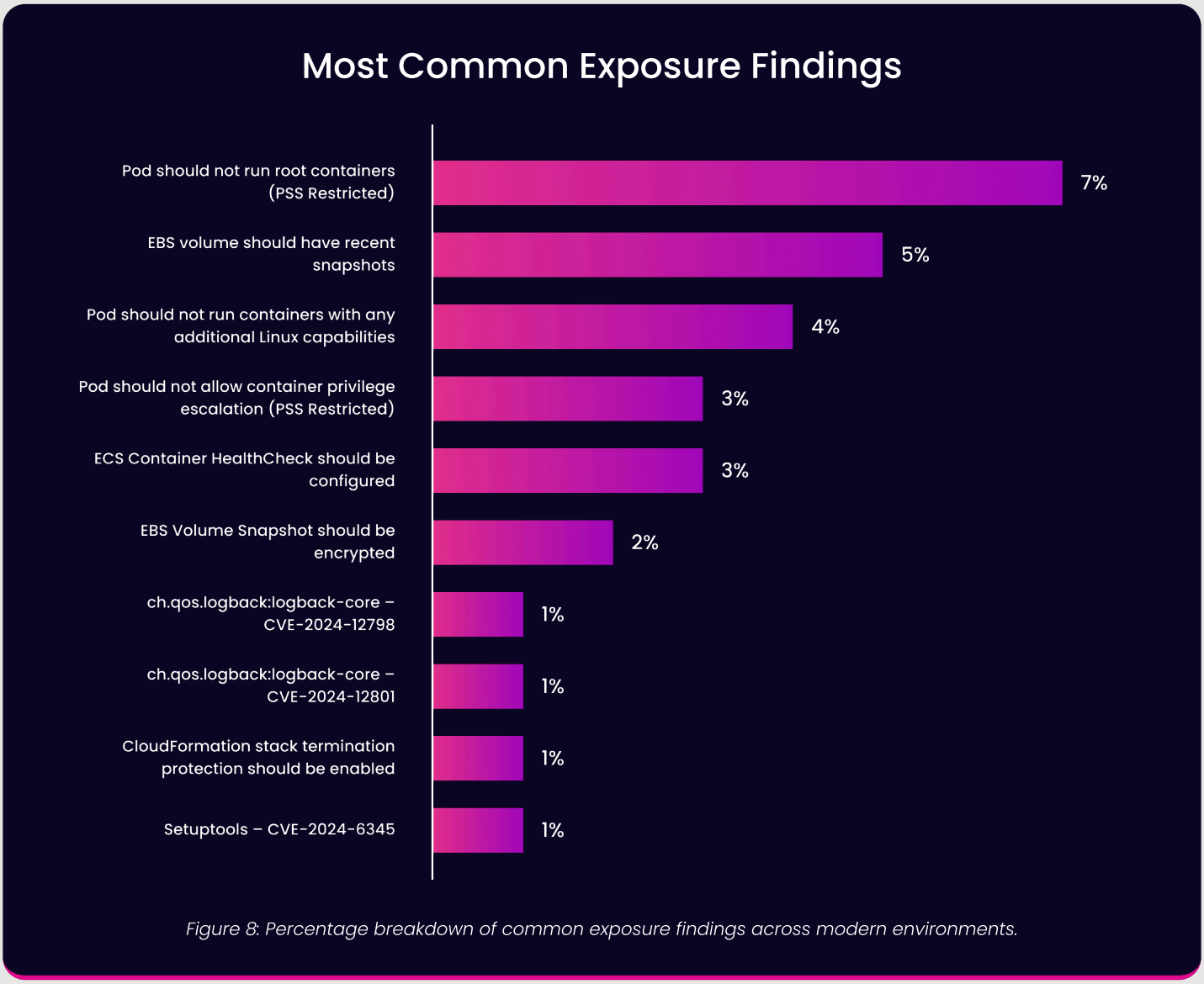

Figure 8: Percentage breakdown of common exposure findings across modern environments.

The most frequently observed findings in 2025 reflect this mix. Container security issues such as running workloads as root or allowing unnecessary privileges appear alongside cloud hygiene gaps like missing snapshots or unencrypted backups. Traditional vulnerabilities also remain present, including known CVEs in commonly used libraries. None of these findings are unusual on their own, but what stands out is how consistently they appear across environments.

This combination is a natural result of how modern systems are built and operated. Cloud environments rely on shared infrastructure. Containers run on machines that are continuously scanned by multiple tools, and common libraries are embedded across applications and services. As a result, exposure does not appear as isolated problems. It clusters around shared assets and repeatable configurations, creating familiar patterns that remediation teams encounter over and over again.

Most exposure is not driven by rare or sophisticated attacks. It comes from baseline configuration gaps and well-known vulnerabilities that persist because they are hard to address consistently at scale. Teams are not struggling to understand what these issues are, they are struggling to keep up with the volume and repetition.

What It Takes to Reduce Risk at Scale

Reducing exposure at scale is not about eliminating every finding. At the volumes organizations are dealing with today, that goal is neither realistic nor necessary. The data shows that meaningful progress comes from how remediation is organized and executed, not from trying to address everything at once.

In 2025, organizations continued to make measurable progress by focusing remediation efforts where they mattered most. On average, teams reduced remediation backlogs by 40 percent and reclaimed roughly 33,000 hours of time each year across the people involved in remediation work. These gains did not come from adding more tools, they came from prioritization, consolidation, and workflows designed around fixes rather than individual alerts.

40%

Average backlog reduction

Figure 9: Average remediation backlog reduction.

$1.7 Million

Average annual savings per organization

33,000 Hrs

Average annual time savings per organization

Figure 10: Average annual money and time savings across remediation teams.

At the same time, the data reflects a more mature reality. As exposure volumes grow, efficiency gains are no longer automatic. Improvement requires discipline. Low-impact issues need to be filtered out, and duplicate findings need to be consolidated. Remediation work needs to be coordinated across development, infrastructure, and security teams so effort is not wasted solving the same problem multiple times.

At this level of scale, remediation becomes an operational capability rather than a series of individual decisions. Teams that treat exposure management as an ongoing process, with clear ownership, repeatable workflows, and shared priorities, are better positioned to sustain progress over time. The difference is not effort, it is structure. When remediation is designed to scale, organizations are able to reduce exposure consistently, even as environments continue to grow.

What This Means for Security Leaders

Exposure management has reached a point where scale exposes reality. As environments grow and detection coverage expands, the limiting factor in reducing risk is no longer visibility. It is execution. The data in this report reflects a consistent pattern across modern environments: Organizations make progress when they focus on how remediation actually happens, not just on what tools report.

Several implications stand out from the data:

Findings do not equal risk reduction.

Identifying vulnerabilities is necessary, but it is only the starting point. When organizations are dealing with tens of millions of findings each year, progress depends on how effectively those findings are prioritized, consolidated, and acted on.

Scale rewards focus, not coverage.

Risk tends to converge in predictable places. Leaders who direct remediation effort toward high-impact areas see better results than those who try to address every category of exposure evenly.

Cloud-native risk is an execution problem.

Most cloud and container findings are well understood. They persist because environments change quickly and remediation does not always keep pace. Improving execution matters more than expanding detection.

Efficiency requires discipline.

Backlog reduction and time savings do not happen by accident. They require clear prioritization, consolidation across tools, and coordination across teams. At scale, efficiency has to be designed into remediation workflows.

Outcomes are the real measure of maturity.

Exposure management programs mature when success is measured by reduced risk, not by the number of findings processed. Leaders who align remediation with organizational impact and sustainability are better positioned to make steady progress over time.

Taken together, these points lead to a simple conclusion. When security meets reality, exposure management success is defined by outcomes, not activity. Leaders who recognize this shift are better equipped to manage risk in environments that continue to grow in complexity and scale.