seemplicity

The Year of Scalable Risk Reduction

Insights from Seemplicity's 2024 Platform Data

REPORT

Vulnerability and exposure management is no longer about addressing individual flaws but about conquering systemic challenges. Data shared in this report reflects that security leaders face heightened urgency to scale up their remediation operations so that they can prioritize findings effectively, streamline workflows, and reduce risk. But how are organizations tackling these challenges? And what lessons can be drawn from their successes and struggles?

This data-based report dives into insights derived from Seemplicity's SaaS platform to provide a comprehensive look at modern exposure management. By analyzing over a billions of findings across diverse organizations and industries, this report uncovers the trends, strategies, and operational shifts shaping how businesses are evolving their approach to remediation. From automating workflows to consolidating data and prioritizing what matters most, the report's findings reveal a clear path forward for teams striving to enhance their security posture at scale.

ABOUT THE DATA

The data presented in this report is derived from Seemplicity's SaaS platform and was aggregated and anonymized from a diverse range of environments. It encompasses dozens of organizations across industries such as retail, financial services, healthcare, and manufacturing and is based on an analysis of over a billion vulnerability findings processed by the Seemplicity platform throughout 2024. By examining this extensive dataset, this report uncovers key trends, operational bottlenecks, and emerging best practices that are helping organizations navigate the complexities of modern exposure management.

The Vulnerability Landscape in Numbers

The challenges of managing vulnerabilities and exposures have never been more pressing for organizations across all industries, and the year 2024 was no exception. The National Vulnerability Database (NVD) demonstrates that the volume of vulnerabilities continues to grow year over year. In 2022, there were 25,043 vulnerabilities recorded. This number rose to 28,818 in 2023, representing a 15% increase. Near the end of 2024, the NVD documented over 35,000 vulnerabilities for the year, indicating a 22% rise compared to 2023. This upward trend highlights the growing challenges organizations face in managing and mitigating security risks. As the volume of vulnerabilities and cyber threats grow, the need for structured, automated, and scalable vulnerability and exposure management has become essential.

Modern Exposure Management

These dynamics mean organizations are under mounting pressure to improve their exposure management strategies. Specifically, organizations need smarter processes, enhanced prioritization, and scalable remediation workflows.

Through this report, we highlight the intricacies of modern exposure management and what organizations are doing to navigate these complexities, from balancing automation and human oversight to integrating the many tools and solutions needed in today's security ecosystems. These insights serve as a benchmark for security leaders seeking to streamline operations, improve prioritization, and ultimately reduce risk at scale.

Top Industries Represented in Data Analysis

Figure 1 highlights the top industries represented in our dataset. These industries face diverse challenges, from securing sensitive data to managing complex infrastructure and high volumes of vulnerabilities. The common thread across this broad representation is that managing vulnerabilities is a critical priority across diverse sectors, regardless of their specific business focus or organizational size.

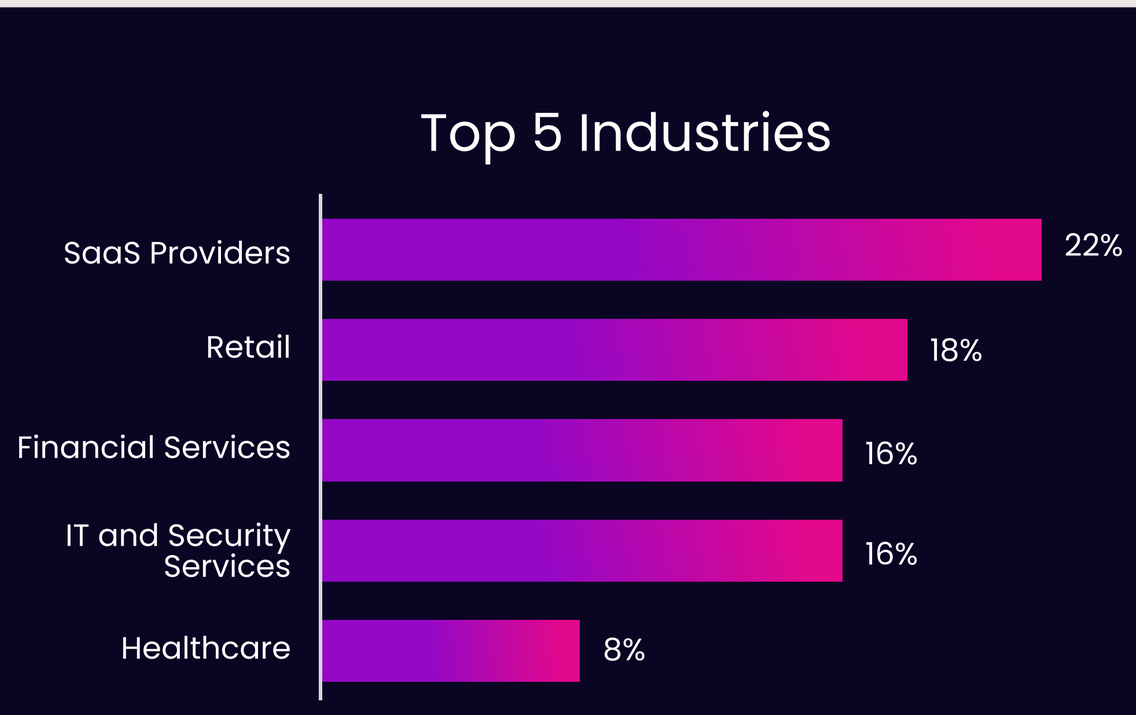

Figure 1: Top 5 Industries Represented in the Report Data

SAAS PROVIDERS | 22%

Vulnerability and exposure management is vital for companies developing software to secure their diverse and dynamic environments, protect code integrity, and address risks in cloud, development, and DevOps pipelines. With fast-paced development cycles and third-party dependencies, efficient exposure management helps remediate vulnerabilities without slowing releases.

RETAIL | 18%

Retailers manage large-scale, typically highly distributed digital operations involving vast resources and high volumes of personal customer data, often with the added challenge of working within tight profit margins. Security in this industry is critical, as breaches can damage customer trust and have significant financial repercussions.

FINANCIAL SERVICES | 16%

The financial services sector is entrusted with handling sensitive customer and financial information and must comply with stringent regulatory requirements. Financial institutions are constantly under pressure to prioritize cybersecurity to protect customer assets and data, and to avoid costly regulatory penalties.

IT AND SECURITY SERVICES | 16%

Security and risk reduction are inherent concerns for providers of cybersecurity and IT services and solutions. Companies in this category bear a significant responsibility for managing and reducing risks across multiple client environments. These companies monitor, manage, and respond to vulnerabilities not only in their own systems but also in those of their clients, which adds a layer of complexity to their operations.

HEALTHCARE | 8%

The healthcare industry represents a highly regulated sector with unique security challenges. Healthcare organizations handle massive amounts of personal and medical data, which, if compromised, can have serious repercussions for patient privacy and safety. Given the prevalence of health information and data privacy laws globally, including Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) in the US and other privacy laws, the healthcare sector needs a robust approach to vulnerability and exposure management.

Remediation Operations No Matter the Size

The dataset in **Figure 2** reflects that the report represents a balanced perspective of organizations of all sizes, from small teams managing robust digital infrastructures to large enterprises with complex, distributed operations. The relatively equal distribution of business sizes underscores that managing vulnerabilities is a shared challenge, regardless of an organization's size or resources, requiring scalable strategies to address diverse needs effectively.

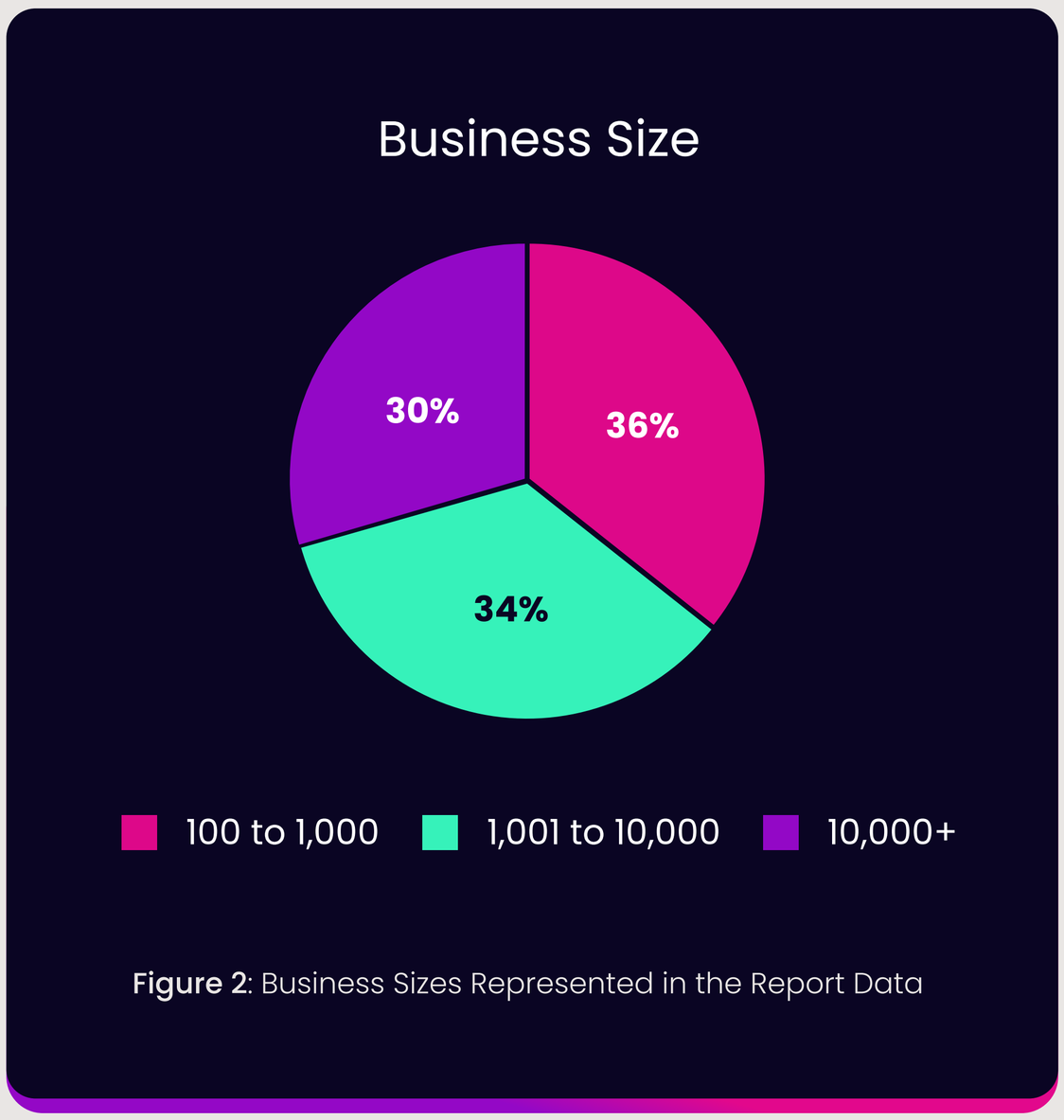

Figure 2: Business Sizes Represented in the Report Data

Who's Responsible for Remediation Operations?

The data in **Figure 3** highlights the range of roles involved in remediation operations, reflecting the need for collaboration and effective communication to execute exposure management well.

Developers make up the majority of those contributing to remediation, indicating their critical role in addressing vulnerabilities alongside their primary responsibilities. This emphasizes the need for solutions that enable developers to address remediation tasks quickly and efficiently, minimizing disruption to their core work.

IT and Cloud Operations teams play a significant part in ensuring the stability and security of infrastructure, while dedicated security teams, though smaller in number, often bear the heaviest burden of triaging and prioritizing findings.

This distribution illustrates the diverse skill sets required to maintain a robust security posture and the importance of cross-functional coordination in modern remediation efforts.

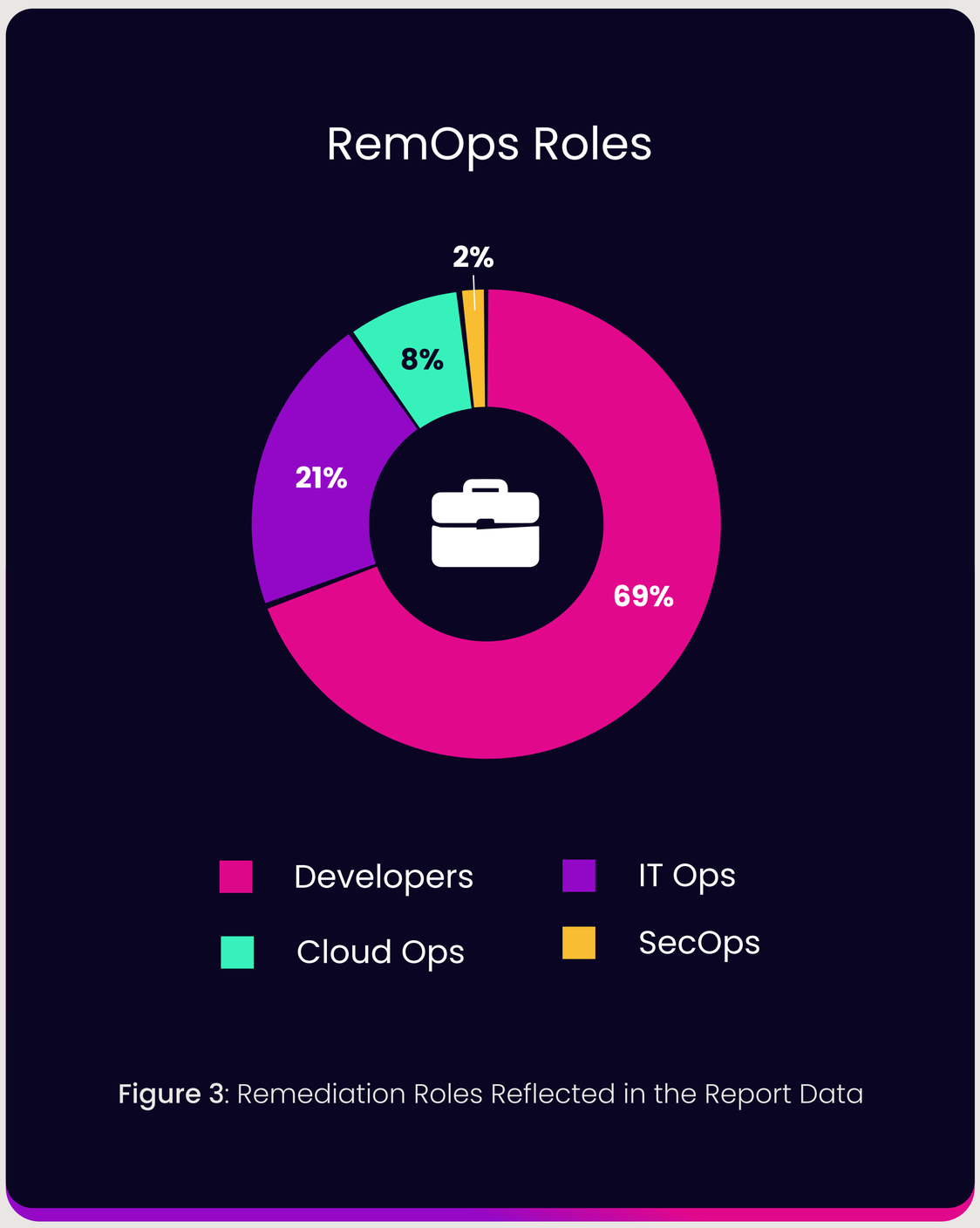

Figure 3: Remediation Roles Reflected in the Report Data

Security Scanning Tool Adoption

Figure 4 illustrates the number of security scanning tools organizations are using to assess and manage security across their digital environments. The data highlights a continued reliance on multiple scanning sources across code, cloud and infrastructure, as organizations seek comprehensive visibility into potential vulnerabilities. Modern organizations are no longer able to rely on just a few scanners and, instead, integrate data from an average of eight different tools, reflecting the need for broad and comprehensive security coverage.

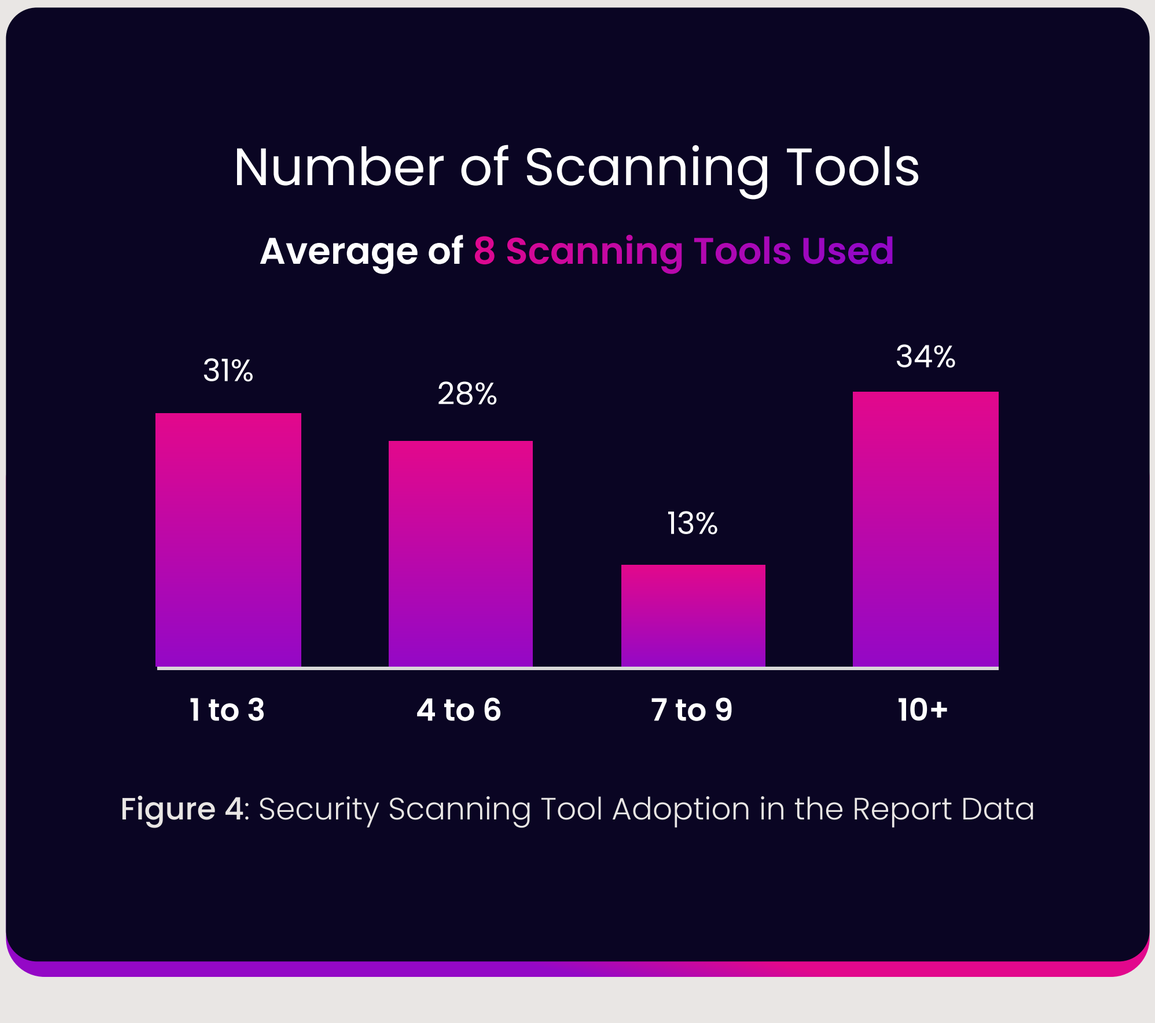

Figure 4: Security Scanning Tool Adoption in the Report Data

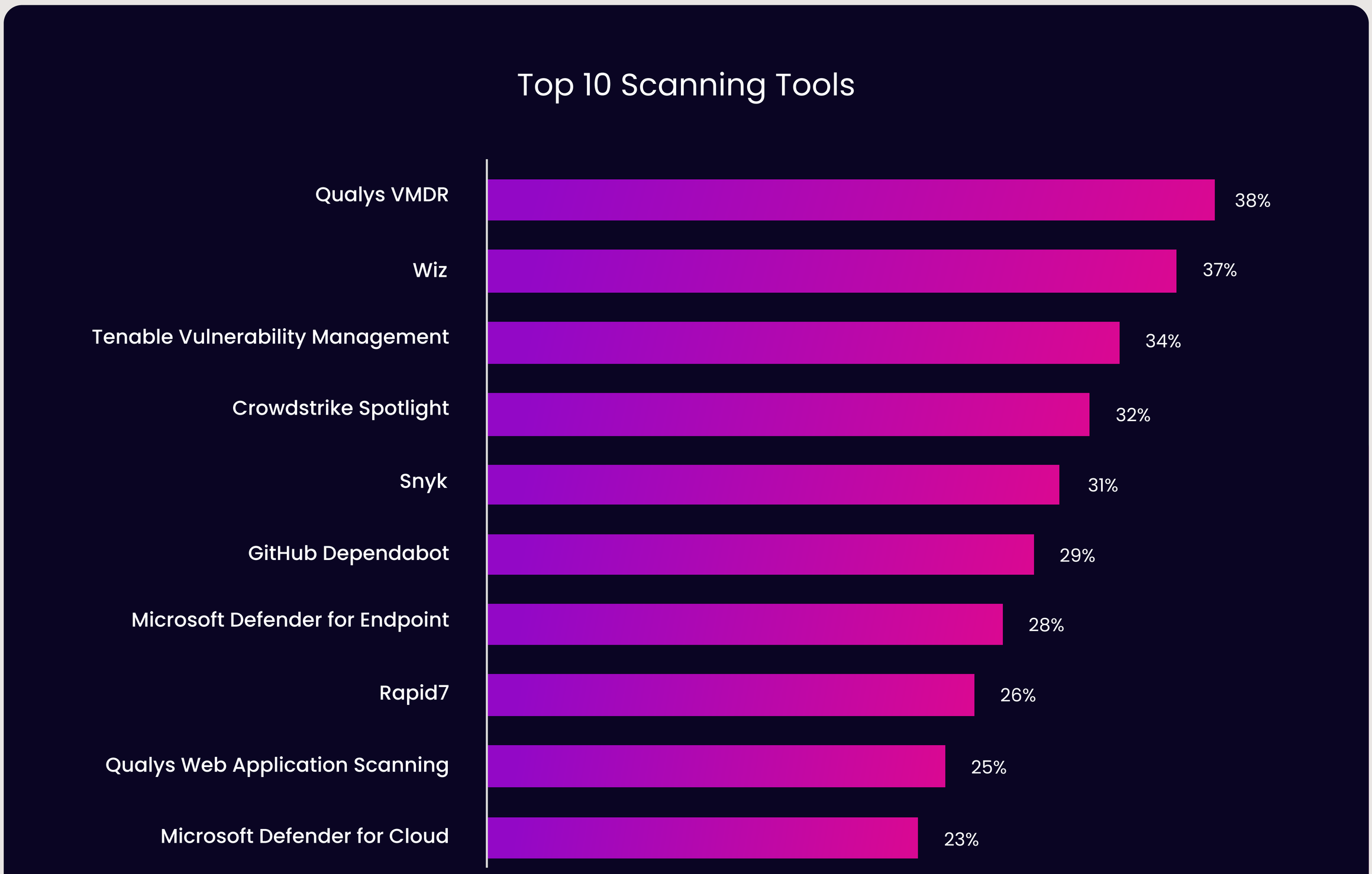

Figure 5: Top 10 Security Scanning Tools in the Report Data

The most commonly used scanning tools represented in the data provide further evidence that organizations are implementing a multi-layered approach to securing their attack surface across code, cloud and infrastructure. The high representation rates of Tenable, Wiz, and Qualys products demonstrate that organizations value comprehensive vulnerability and exposure assessment platforms capable of handling multiple aspects of security, from on-premises infrastructure to cloud-native assets.

Microsoft Defender for Cloud and Microsoft Defender for Endpoint adoption shows that protecting cloud environments and endpoints is a priority as organizations manage large-scale, distributed IT ecosystems, while also securing applications, especially in development-heavy environments. Managing the security of open source software components has become essential as organizations increasingly rely on third-party libraries to accelerate time-to-production, as evidenced by Snyk in position 5.

This broad scanning tool usage underscores the need to consolidate and centralize RemOps, as organizations work to secure multiple domains within their digital ecosystems—from cloud environments and endpoints to web applications and code dependencies.

The Scale of Findings Processed

48.6 Million

Findings Processed Per Customer

Figure 6: Average Number of Findings Processed Annually per Customer by Seemplicity

The data reveals the immense scale of vulnerability findings organizations must address, with the average company managing tens of millions of findings annually. This massive volume of findings is too large to be managed manually and cannot be done without efficient processes. Remediation processes need to be automated, intelligently managed, and tailored to the needs of each team. Without scalable, efficient workflows, organizations struggle to address even a fraction of these vulnerabilities, leaving critical gaps in their security posture. Effective vulnerability and exposure management requires consolidating data from diverse sources, identifying high-priority issues, and streamlining remediation workflows so that security teams can focus on what matters most.

Prioritizing Critical Vulnerabilities For Greater Efficiency

Distribution of Vulnerabilities by Severity

Figure 7: Distribution of Finding Severity Represented in the Report Data

The data reveals that, on average, less than 2% of vulnerability findings are deemed most business critical, underscoring the importance of effective prioritization in exposure management.

By applying tailored prioritization criteria that account for their unique needs and infrastructure, organizations can filter out lower-risk findings, and identify and concentrate on the vulnerabilities that pose the greatest business risk. This focus enables security teams to allocate their resources efficiently, directing immediate attention to vulnerabilities that would have the most significant impact on their organization.

Given that developers make up the majority of those contributing to remediation (see **Figure 3**), it's vital to minimize disruptions to their primary responsibilities by limiting the volume of vulnerabilities requiring their attention. Ensuring that the most business critical issues are flagged helps prevent teams from being overwhelmed and enables them to dedicate their time and expertise to tasks that truly matter, and quickly get back to creating software that generates revenue for their organizations. This approach is imperative for maintaining operational stability while effectively managing security risks.

The ROI of Effective Remediation Operations

Figure 8: Average Backlog Reduction for Seemplicity Customers | Average Annual Savings for Seemplicity Customers | Average Annual Time Savings for Seemplicity Customers

Organizations using the Seemplicity platform reduced their findings backlog by an average of 57%, enabling security teams and their counterparts to focus on remediation efforts that truly matter. This reduction is a testament to the power of efficient RemOps. By consolidating and deduplicating findings from across multiple scanning tools and aggregating findings based on their common solutions, the platform transforms what would otherwise be an overwhelming list of vulnerabilities into a streamlined and actionable set of fixes. The approach of focusing on fixes rather than raw findings allows remediation teams to address clusters of high-impact issues with a single action, significantly reducing the workload and improving efficiency.

Seemplicity customers enjoy an estimated average of $1.8 million in savings each year due to RemOps efficiency. Automation and business-oriented prioritization not only reduce the costs associated with manual processes but also minimize the risk of breaches, as well as any fines and expenses tied to unaddressed vulnerabilities. RemOps efficiency also maximizes the return on investment of existing scanning tools by making it possible for organizations to get the most out of them by effectively managing the steady stream of findings they receive from their tools. This conservative estimate of $1.8 million does not include additional savings such as reduced incident response costs or avoided security noncompliance fines, meaning that the actual financial benefits are likely substantially higher.

Streamlined workflows and automated processes significantly reduce the time spent on manual remediation tasks, enabling teams to process vulnerabilities and exposures faster and more efficiently. By alleviating the burden of manual, repetitive work, teams can redirect resources to other critical priorities, ensuring a more balanced and productive approach to security operations.

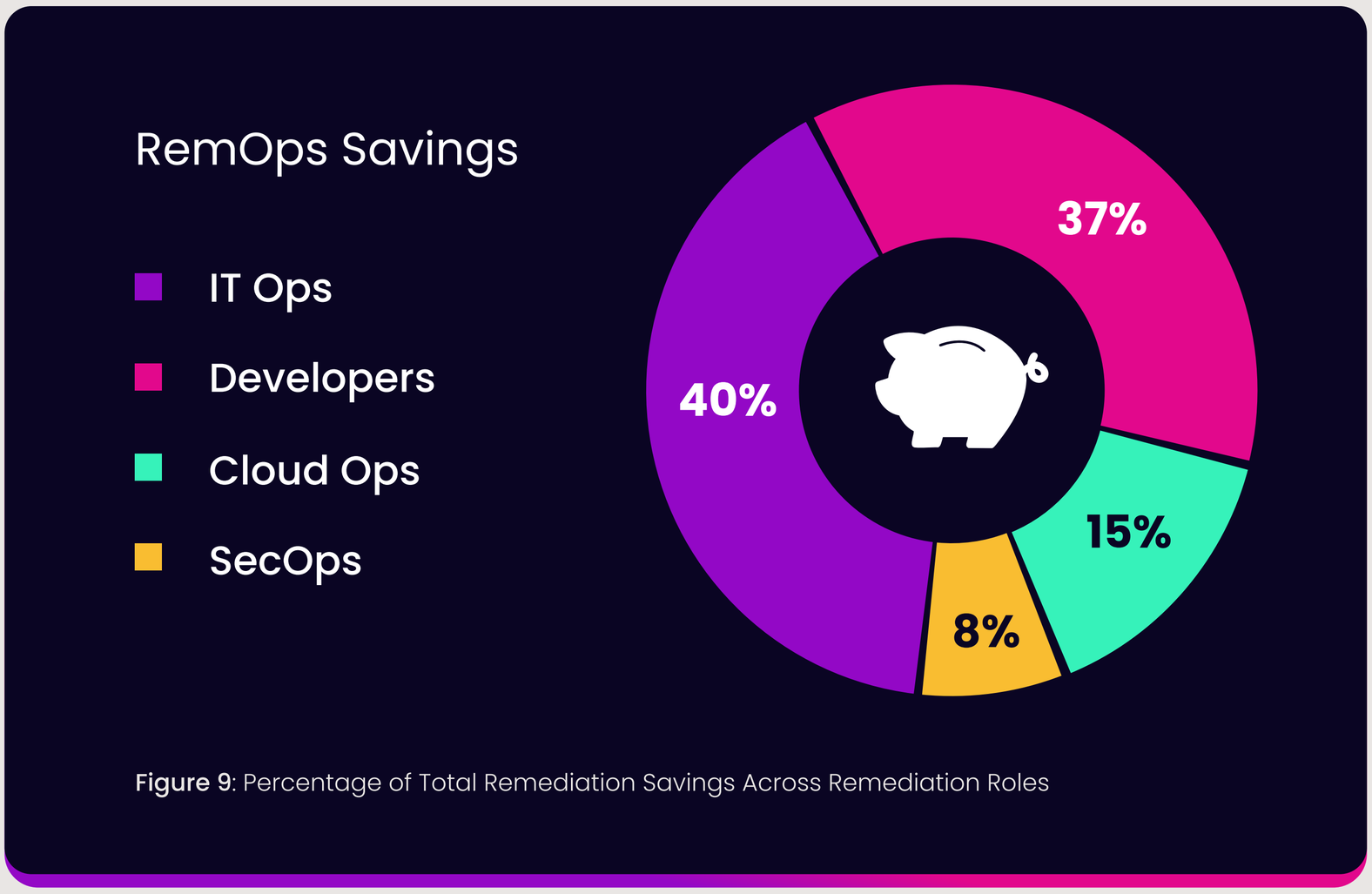

Figure 9: Percentage of Total Remediation Savings Across Remediation Roles

The distribution of savings across an organization reflects the intensity of each team's remediation workload. The data highlights that teams from IT Operations and development see the greatest savings from efficient remediation workflows. This is directly tied to their substantial involvement in the remediation process (see **Figure 3**). Developers, who make up the majority of those contributing to remediation, often work across high volumes of findings, which can divert time away from their core responsibility of creating and maintaining secure software. When workflows are optimized to prioritize only the most business critical vulnerabilities, developers spend less time managing low-priority issues, resulting in significant time and cost savings.

IT Operations teams also benefit greatly from streamlined workflows. These teams are frequently at the center of operational bottlenecks caused by redundant or low priority findings. Efficient RemOps processes, such as deduplication and automation, help IT Operations teams focus on meaningful remediation efforts, further amplifying their savings.

Cloud Operations and security teams see relatively smaller shares of the total savings, reflecting their more specialized roles. However, these savings remain impactful as streamlined workflows reduce the strain on these teams, enabling them to address vulnerabilities with greater focus and efficiency.

The data illustrates a clear correlation: the more involved a team is in the remediation process, the more they stand to save from efficient RemOps practices. This highlights the manual and unscalable nature of existing approaches and the value of solutions that alleviate the remediation burden across all roles while ensuring resources are directed toward high-priority risks.

A Year of Progress and Transformation

The findings in this report affirm the importance of streamlining and scaling RemOps. It is clear that manual processes and fragmented tools can no longer keep pace with the increasing volumes of vulnerabilities and corresponding exposure management challenges. The insights presented in this report underscore the critical role that RemOps platforms play in empowering organizations across industries to address vulnerability and exposure management challenges efficiently and effectively.

Seemplicity is helping to transform the way businesses approach vulnerability and exposure management by providing a centralized, automated solution that helps teams focus on what matters most—reducing business risk and improving their overall security posture. By consolidating findings, deduplicating data, and aggregating issues based on common remedies, solutions like the Seemplicity platform provide the structure and scalability needed to tackle the challenges of modern exposure management. As organizations continue to scale their digital operations, the need for efficient remediation operations will remain essential for maintaining a strong security posture.