BrandShield®
AI-Powered Digital Risk Protection

2025 CyberScam Report

BrandShield®
AI-Powered Digital Risk Protection

Table of Contents

Introduction and Key Findings

Introduction & Methodology

As cyber threats escalate in scope and sophistication, **Chief Information Security Officers (CISOs)** face a rapidly shifting security landscape. BrandShield's 2025 CyberScam Report delivers forward-looking insights to help CISOs understand emerging threats, new scams, and strategies for proactive defense.

Based on Brandshield's continuous collaboration with cybersecurity experts, this report highlights the key concerns shared by CISOs today. With generative AI increasingly weaponized to create and scale sophisticated scams and infringements, the urgency to stay ahead has never been greater. This report aims to provide CISOs with actionable intelligence to anticipate, rather than simply respond to, evolving threats.

Methodology

This report is based on insights gathered from survey responses from 200 CISOs across the finance, retail, and software sectors, with equal representation from each industry. All respondents were full-time employees, contributing a diverse view from companies of various sizes, evenly split between organizations with 100 - 1,000 employees and those with over 1,000 employees.

Responses were collected from CISOs based in:

 United States  United Kingdom  European Union

The survey was conducted by Global Surveyz Research, an independent survey organization, over a two-month period from September to October 2024.

This sample reflects the insights of security leaders actively managing today's evolving threat landscape, offering a comprehensive look into the specific concerns and priorities shaping their cybersecurity strategies.

Key Findings

98%

of organizations experienced some form of cyberattack in 2024.

This finding highlights the prevalent threat landscape, with nearly all organizations having faced at least one attack in 2024. Key threats included supply chain attacks (33%) and brand impersonation (31%), underscoring the variety and frequency of cyber incidents that require constant vigilance and holistic defense mechanisms.

94%

of CISOs reported losses of at least half a million dollars due to cyber scams, with an average financial damage of $1.7 million. Interestingly, the more damage incurred, the more CISOs express concern about Artificial Intelligence.

These staggering numbers reveal the significant financial impact of cybersecurity incidents. More than half of the CISOs surveyed reported losses exceeding $1 million, pointing to the critical need for organizations to strengthen their cybersecurity to mitigate these costly disruptions.

76%

of CISOs anticipate an increase in their 2025 threat monitoring budgets. Once again, those that suffered more losses plan to spend more to prevent them.

Reflecting the urgent need to address escalating cyber threats, a large majority of CISOs expect to increase their budget allocation for threat monitoring. This trend indicates a heightened focus on preventive measures, with 39% expecting a budget increase of up to 10% and 29% anticipating a more significant boost of 11 to 25%.

77%

of CISOs are considering switching cybersecurity providers, primarily in pursuit of holistic, comprehensive risk coverage.

CISOs are prioritizing integrated, end-to-end solutions that provide robust and scalable security across multiple threat vectors, with 22% identifying holistic coverage as a primary motivator for switching cybersecurity providers. Interestingly, cost-effectiveness ranked low among reasons for switching at only 13%, indicating that CISOs are more focused on effectiveness than on simply reducing costs.

Threats affecting brand reputation—such as brand impersonation, executive impersonation, and phishing and scam sites—are a prominent concern.

Brand-focused cyber threats have become a critical issue for CISOs, with brand impersonation (31%), executive impersonation (28%), and phishing and scam sites (27%) ranking among the top security concerns. These attacks not only target organizations directly but also exploit their reputation to deceive customers and partners, highlighting the growing overlap between cybersecurity and brand protection.

CISOs cite rogue mobile apps, social media impersonations, and compromised credentials as the top external threats.

When asked about the biggest external threats for the next 12 months, CISOs pointed to rogue mobile apps (27%), social media impersonations (27%), and compromised credentials (27%) as their top concerns. These threats emphasize the evolving nature of cyber risks, where digital deception and credential exploitation pose serious challenges to organizational security.

Security Attacks and Trends

Security Attacks Impacting Organizations Over the Last 2 to 3 Years

In 2024, nearly every organization surveyed (98%) faced one or more cybersecurity attacks. Supply chain attacks emerged as the most common type of attack, impacting 33% of CISOs.

Almost as detrimental were those threats affecting brand reputation—such as brand impersonation, executive impersonation, and phishing and scam sites.

The relatively balanced distribution of attack types underscores the fact that companies are confronting multiple threats at similar frequencies. The high prevalence of brand-focused attacks demonstrates the increasing overlap between cybersecurity and brand protection, emphasizing the need for CISOs to adopt strategies that safeguard not only organizational data but also brand reputation and executive identity.

**Question allowed more than one answer and as a result, percentages will add up to more than 100%*

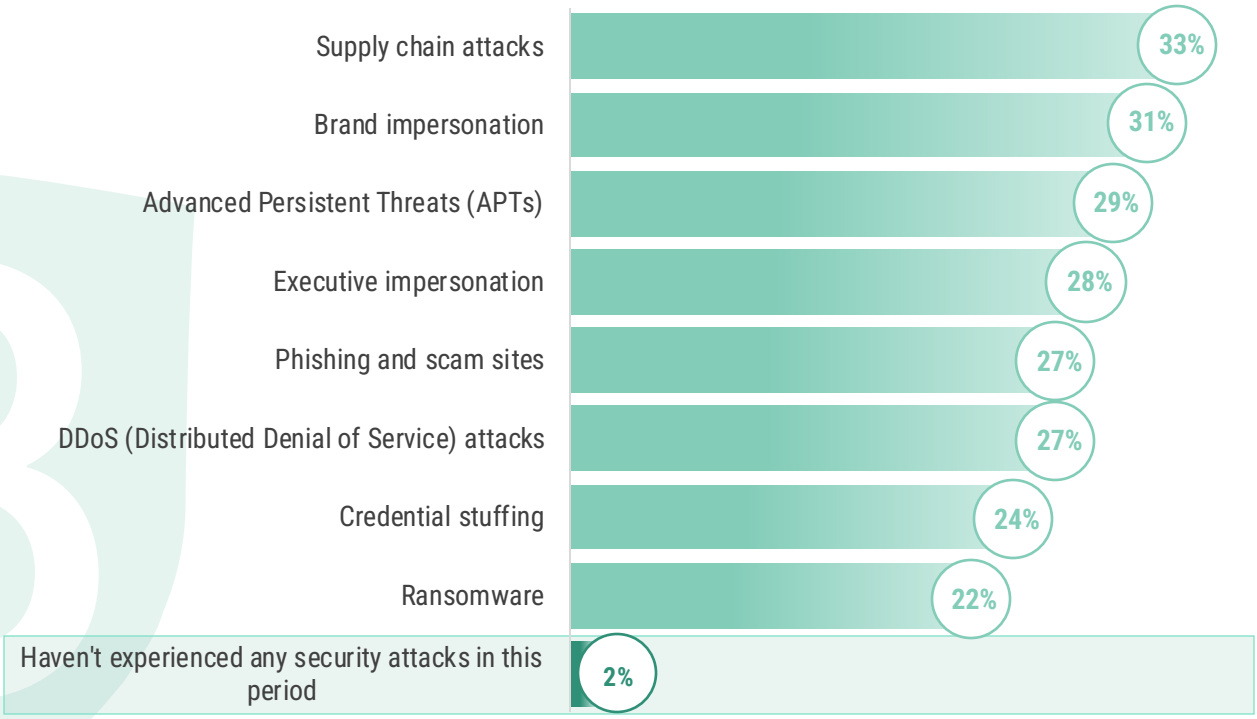

Figure 1: Security Attacks Impacting Organizations

Financial Damage from Online Scams in the Past 12 Months

The financial toll of online scams over the past year has been staggering. 94% of CISOs reported losses exceeding $500,000. Notably, 66% of CISOs reported losses surpassing $1 million, underscoring the significant cost of online scams, especially to mid-sized companies where such sums can represent a substantial portion of annual revenue.

The average financial damage across all regions reached $1.7 million per organization, with notable regional differences. The UK reported the highest average losses, 30% higher than the US and EU. This disparity may, in part, reflect the challenges the UK faces as it reestablishes cybersecurity protocols post-Brexit, creating opportunities for threat actors to exploit potential gaps during this transitional period.

**Question allowed more than one answer and as a result, percentages will add up to more than 100%*

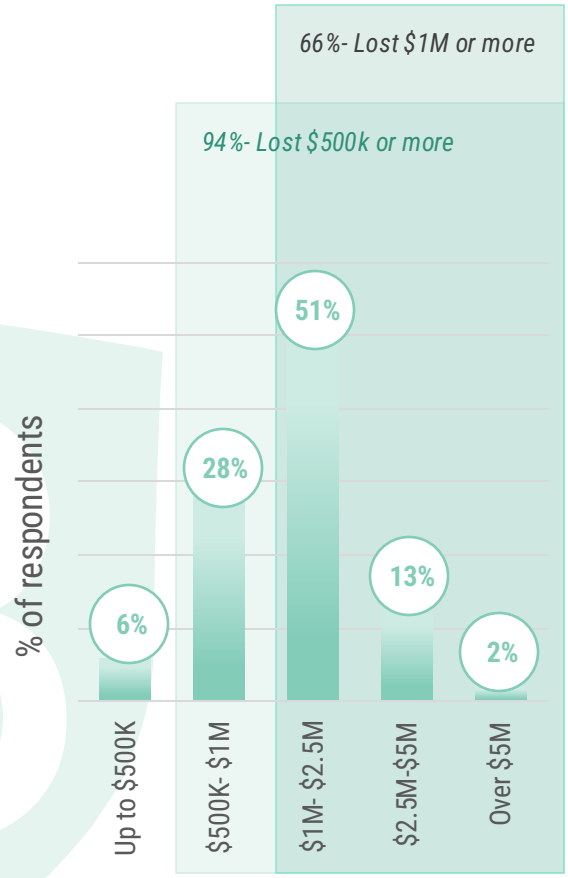

Figure 2: Financial Damage from Online Scams in the Past 12 Months

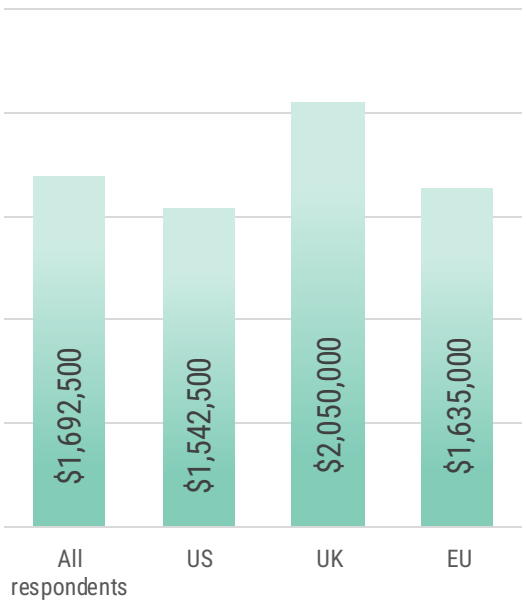

Figure 3: Average Financial Damage from Online Scams in the Past 12 Months, by Country

Top External Threats for the Next 12 Months

CISOs have identified a range of external threats that they anticipate as major cybersecurity challenges for the coming year. Rogue mobile apps, social media impersonations, and compromised credentials top the list. Phishing and scam sites and account takeover threats are also top threats. Interestingly, the dark web has emerged for the first time as a critical focal point.

This diverse set of anticipated threats, with similar levels of concern across categories, underscores the complex, multi-faceted landscape that organizations face entering 2025.

**Question allowed more than one answer and as a result, percentages will add up to more than 100%*

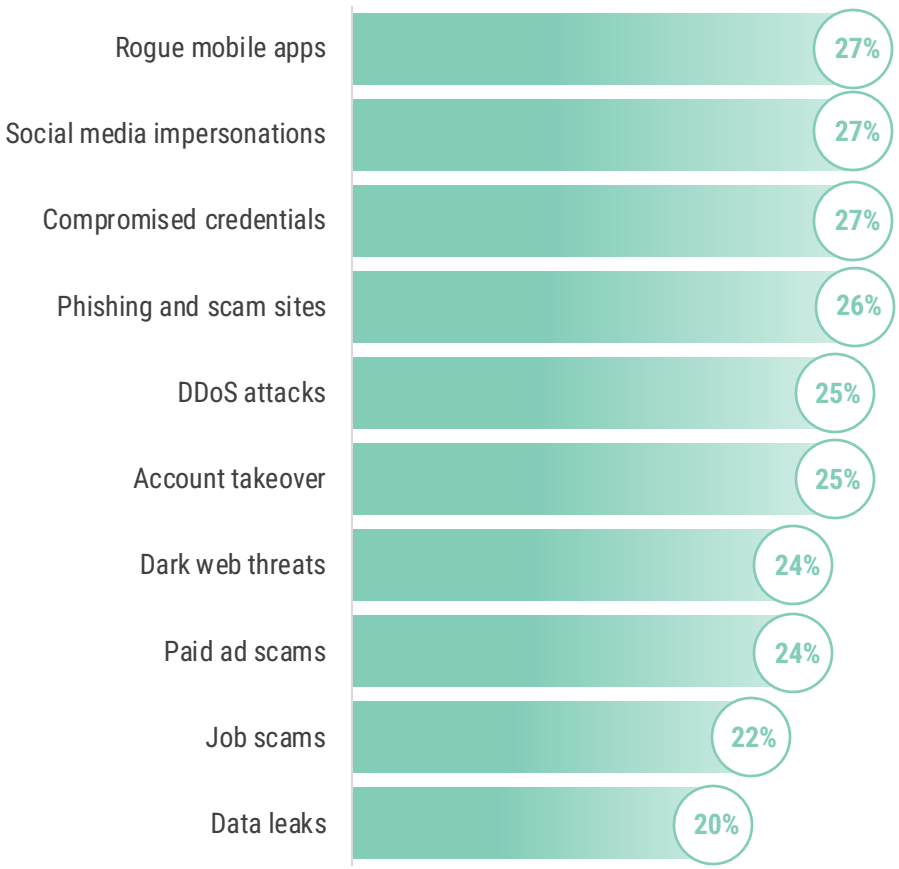

Figure 4: Top 3 External Threats for the Next 12 Months

Priorities and Challenges

Top Cybersecurity Priority for the Next 12 Months

Incident response has emerged as the top priority for CISOs in 2025. When asked to select their single top priority for the year, CISOs emphasized the need to not only identify threats but also to take swift action to remediate them. Incident response often involves taking down rogue websites, fake social media accounts, and malicious apps. CISOs are prioritizing partnerships with cybersecurity vendors that go beyond threat detection to provide fast, effective solutions.

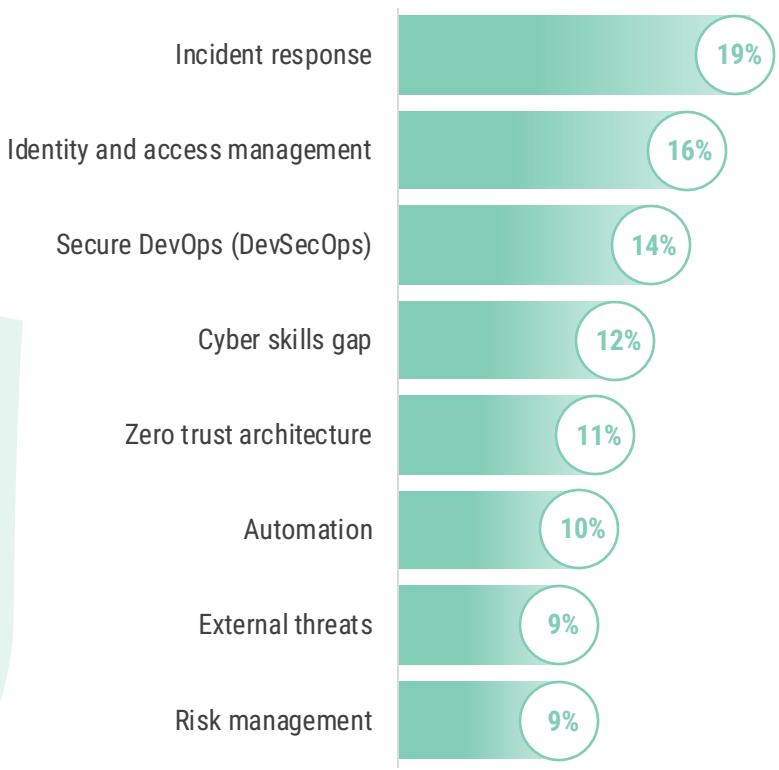

Figure 5: Top Cybersecurity Priority for the Next 12 Months

Biggest Cybersecurity Challenge in 2025

CISOs are navigating an era of rapid change. Their challenges reflect a broad range of concerns, with one common thread—adapting to an evolving threat landscape.

Economic pressures, such as supplier instability and rising costs, create opportunities for scammers to exploit vendor delays through fake invoices and fraudulent payment apps.

AI is reshaping cyber scams, making phishing emails and executive impersonation more convincing and effective than ever before. The rise of 5G expands attack surfaces, giving threat actors more entry points to exploit, steal credentials, and sell them on the dark web.

The bottom line: new technology and global instability are redefining cybersecurity risks, making adaptability more critical than ever.

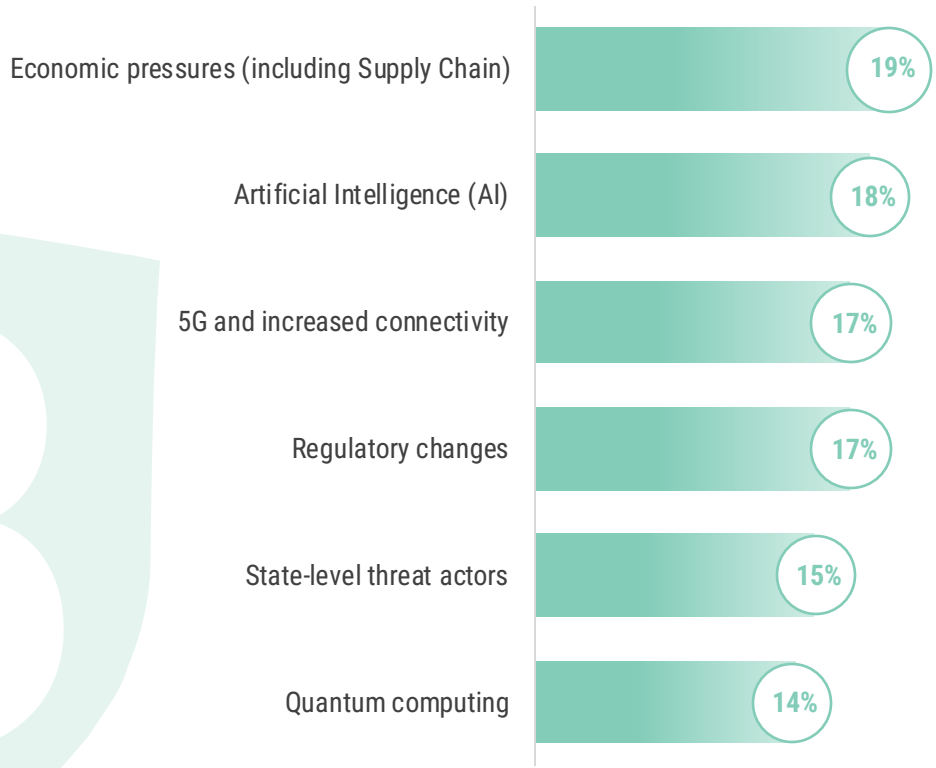

Figure 6: Security Attacks Impacting Organizations

Expected Changes in 2025 Budget for Threat Monitoring

76% of CISOs anticipate an increase in their threat monitoring budgets in 2025.

This commitment to higher budgets reflects the urgent need for CISOs to secure funding to address a rapidly evolving threat landscape.

Meanwhile, 16% of CISOs are planning for budget reductions, likely looking for technologies that can "do more with less." In light of economic pressures, many of these organizations may be considering a shift toward holistic cybersecurity solutions that integrate multiple functions within a single framework, reducing the need for disparate tools.

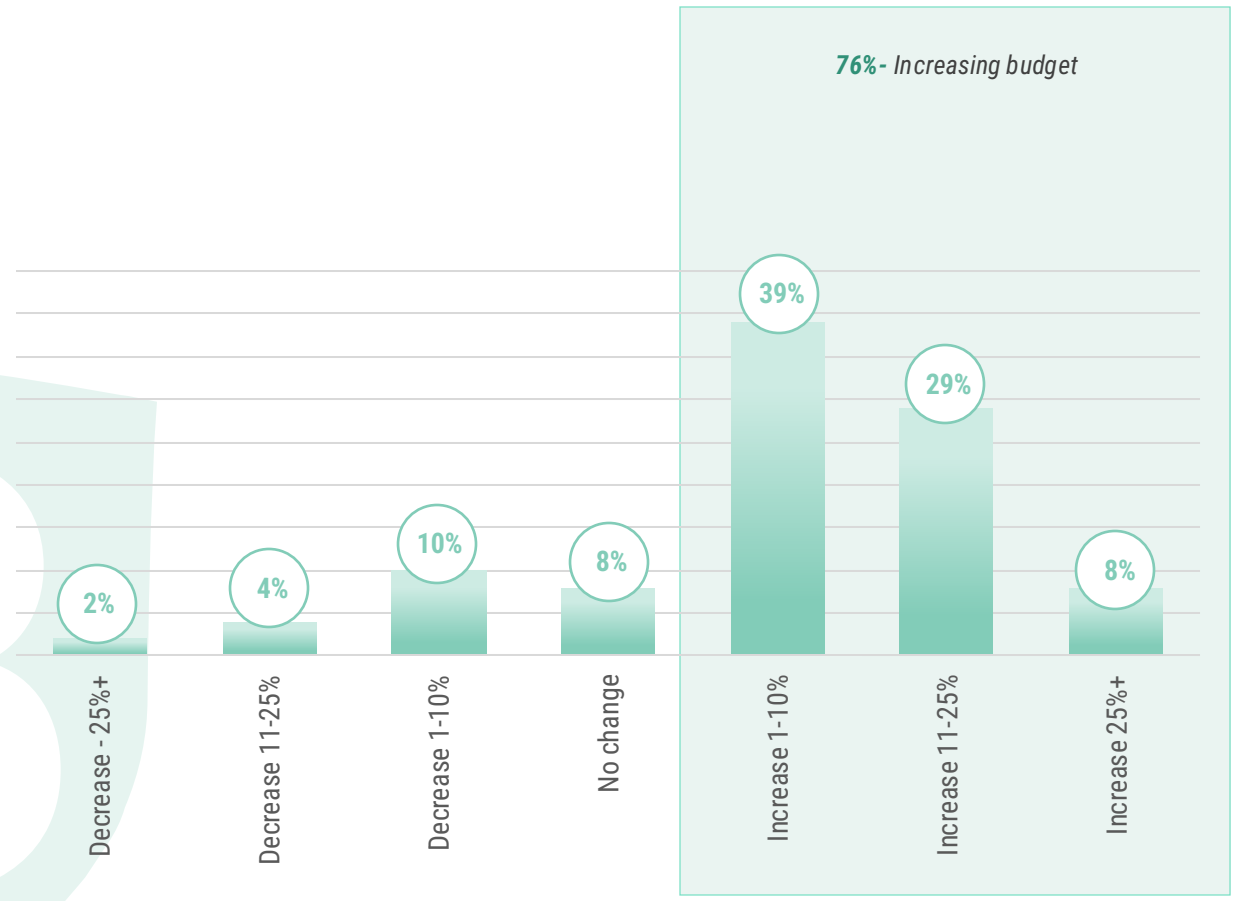

Figure 7: Expected Changes in 2025 Budget for Threat Monitoring

Biggest In-House Challenges in Digital Threat Protection

Intra-organizational challenges remain a major concern for CISOs.

Among the various challenges organizations face in digital risk protection, uncovering cross-platform hidden networks stands out as the top concern, cited by 40% of CISOs. This marks a notable increase from last year's survey, where only 31% highlighted it as a primary concern—an increase of approximately 33%.

This emphasis reflects the need for comprehensive visibility across all online environments, including websites, digital ads, mobile apps, marketplaces, social media, and in particular, the dark web.

**Question allowed more than one answer and as a result, percentages will add up to more than 100%*

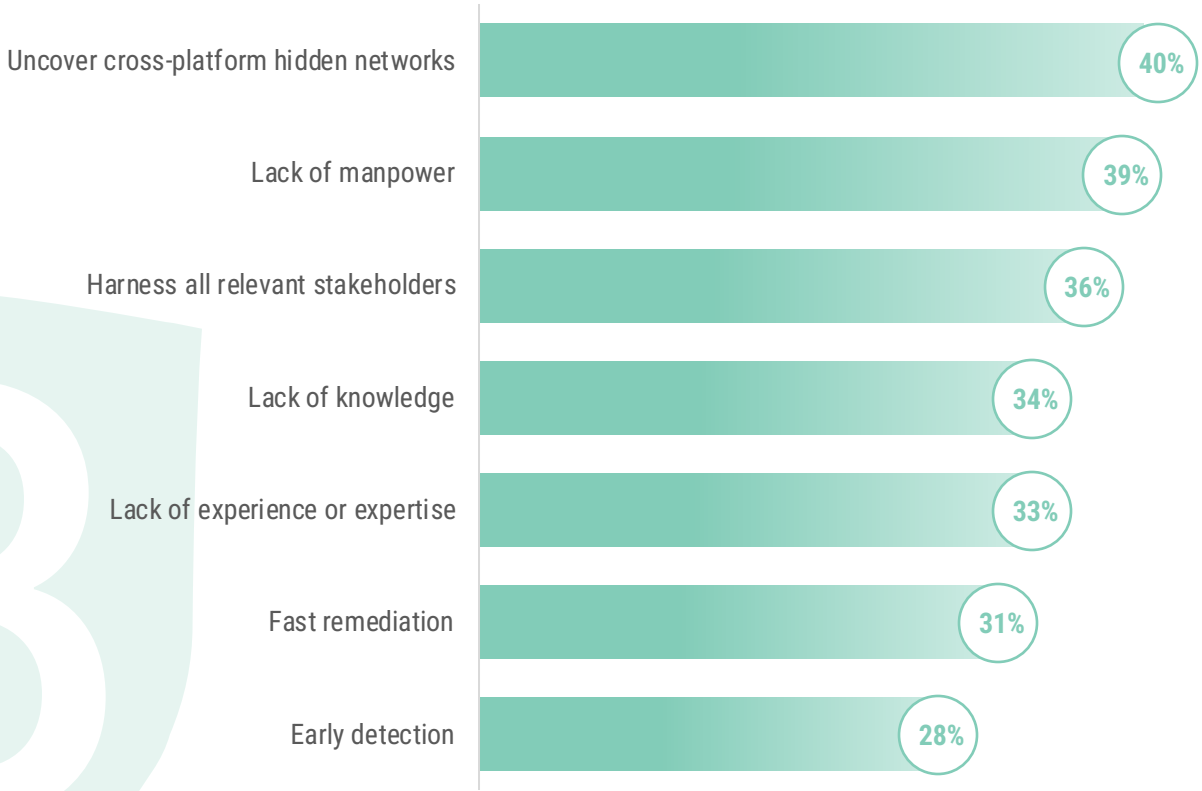

Figure 8: Biggest In-House Challenges in Digital Threat Protection

Key Metrics for Measuring Cybersecurity Solution Success

CISOs prioritize long-term value in cybersecurity investments.

When evaluating the success of cybersecurity initiatives, CISOs focus on metrics that balance financial impact with operational efficiency.

Total cost of ownership extends beyond upfront expenses, encompassing the overall financial footprint, which CISOs increasingly link to ROI as they align cybersecurity spending with broader business objectives.

In contrast, response and remediation time and incident reduction rank lower, indicating that while speed and incident frequency remain important, CISOs are shifting their focus toward broader, long-term value when defining cybersecurity success.

**Question allowed more than one answer and as a result, percentages will add up to more than 100%*

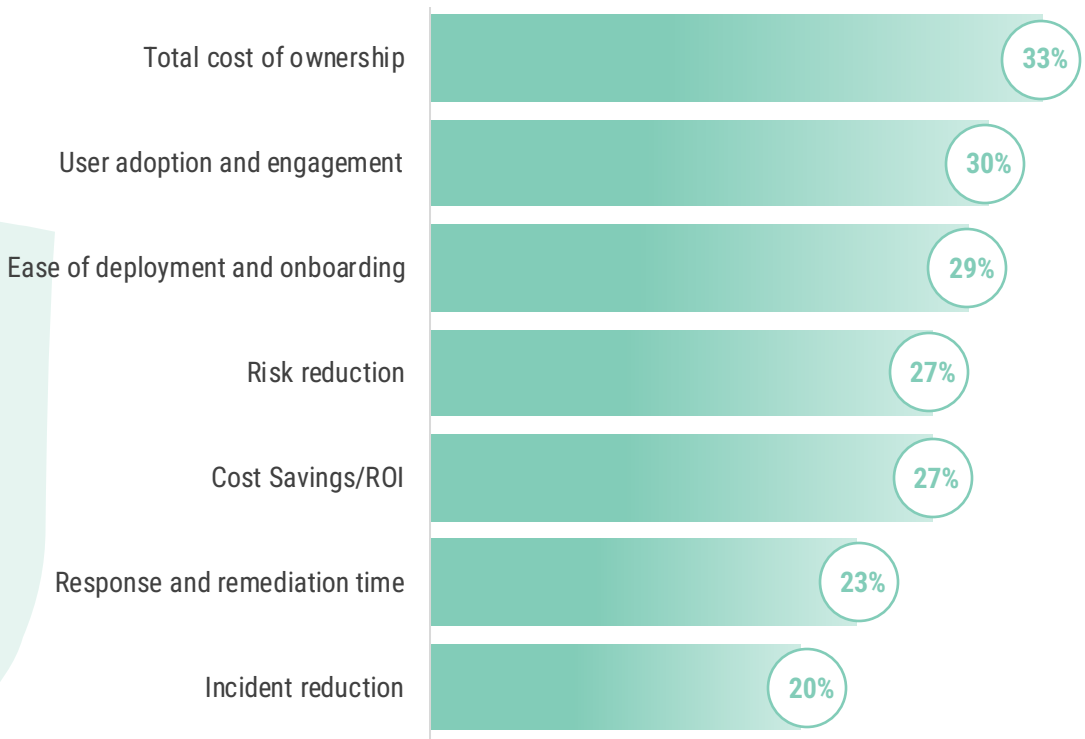

Figure 9: Key Metrics for Measuring Cybersecurity Solution Success

Factors Influencing the Decision to Switch Cyber Brand Protection Providers

77% of CISOs plan to switch cybersecurity providers in search of holistic, end-to-end solutions (22%).

CISOs are increasingly looking for providers that cover the full lifecycle of cyber incidents—from detection to analysis, incident response, takedowns, and continuous monitoring. This approach ensures seamless protection and allows organizations to avoid the complexities of patching together multiple systems.

Notably, cost-effectiveness ranks low among reasons to switch providers, despite being a key factor in cybersecurity investment decisions (as seen in Figure 9). This suggests that while CISOs prioritize value, they're not switching providers for lower prices. Instead, they're seeking comprehensive solutions that can reliably address the evolving ecosystem of online scams.

**Question allowed more than one answer and as a result, percentages will add up to more than 100%*

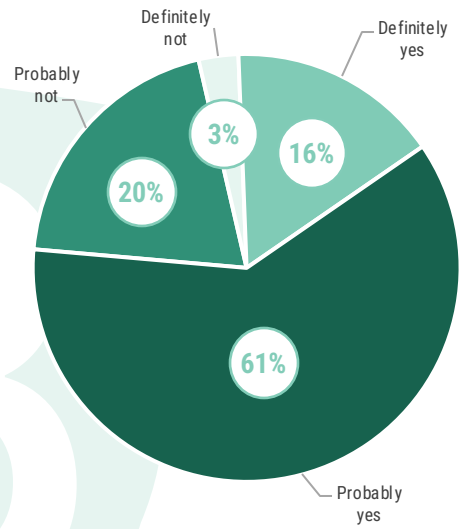

Figure 10: Likelihood of Switching Cybersecurity Providers by 2025

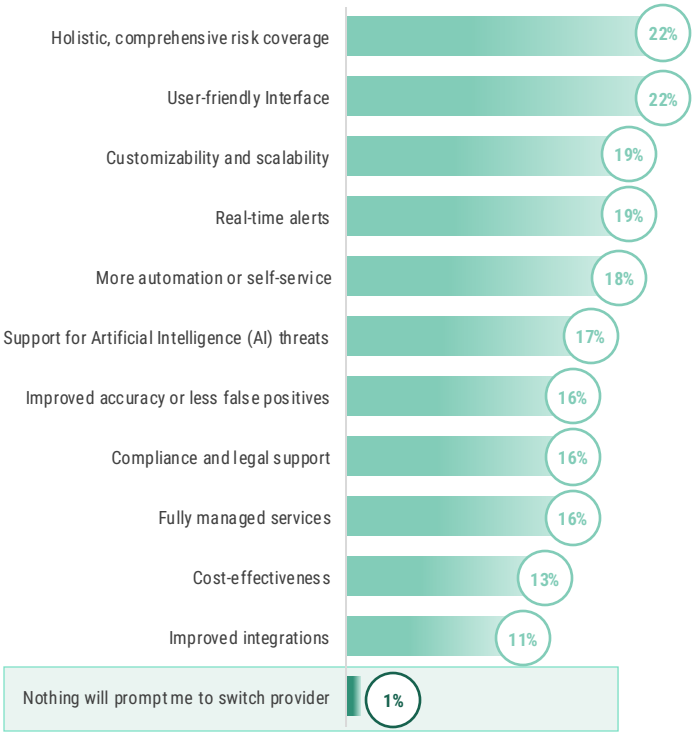

Figure 11: Factors Influencing the Decision to Switch Cyber Brand Protection Providers

The Impact of AI

Concerns About AI Threats to Cybersecurity

AI's impact on cybersecurity is a top concern, especially for organizations that have suffered greater financial losses.

With 99% of CISOs expressing concern about AI, the overwhelming consensus underscores the urgency surrounding AI's transformative—and disruptive—role in the cyber threat landscape.

This concern is especially pronounced among organizations that have experienced significant financial damage from cyber incidents. Among companies with losses exceeding $1 million, 40% report being "very concerned" about AI threats, compared to just 23% of those with smaller losses. This clear correlation between financial impact and heightened vigilance highlights how past experiences drive increased focus on AI-related risks.

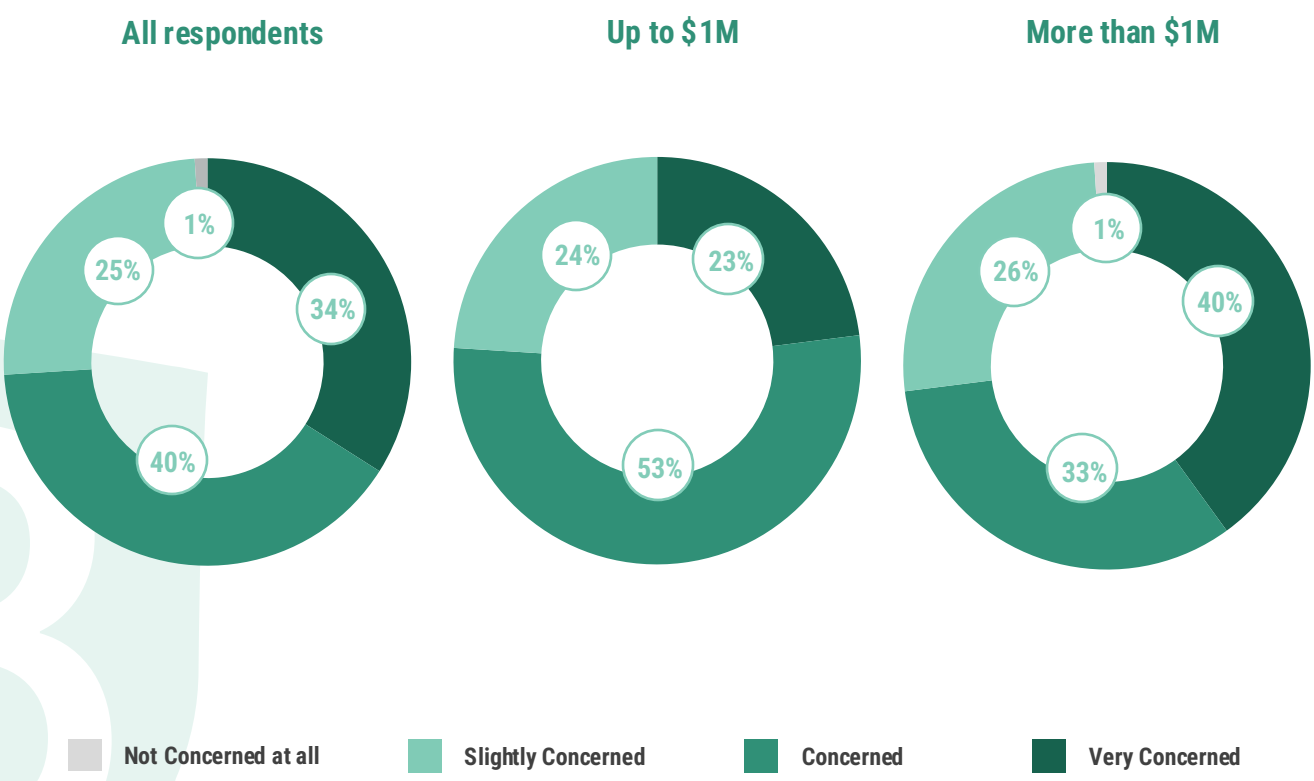

Figure 12: Concerns About AI Threats to Cybersecurity, by financial damage

Areas Where AI Poses the Greatest Cybersecurity Challenge

AI is rapidly transforming every dimension of cybersecurity.

Challenges span from technical integration to ethical considerations. The top tactical challenge is threat detection and response.

AI's influence extends across cybersecurity, affecting everything from technical infrastructure to workforce training and compliance. But can it also be an advantage? The key question for CISOs is not just how to manage AI-driven threats—but how to harness AI as a strategic asset in defense.

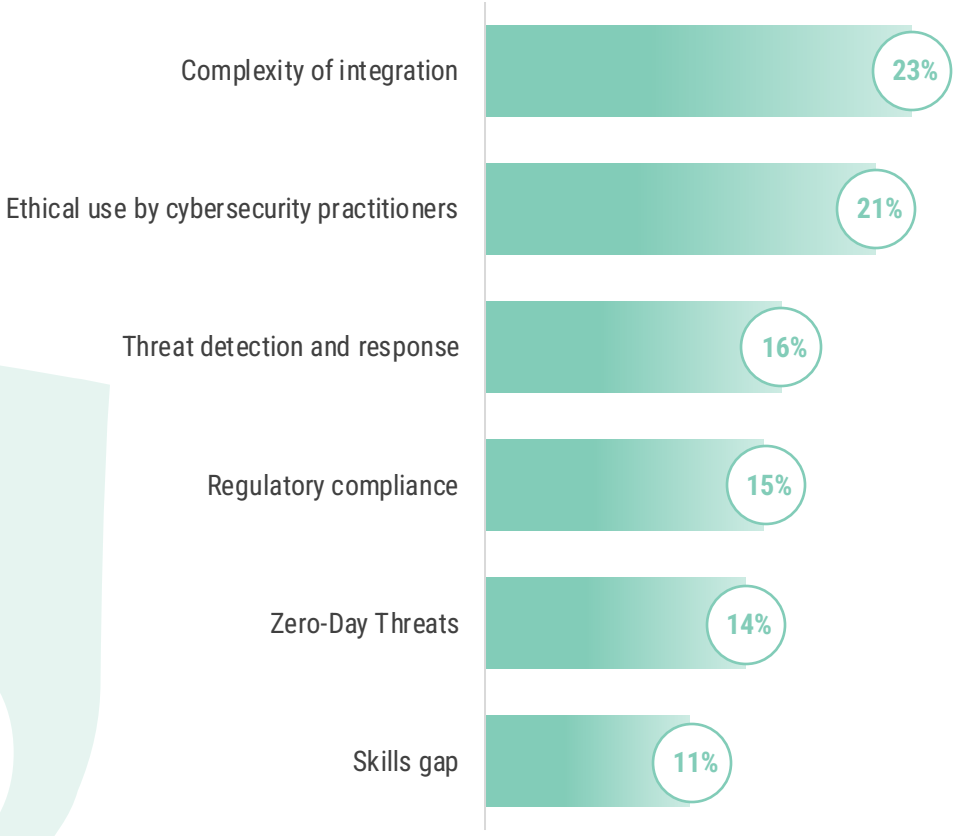

Figure 13: Areas Where AI Poses the Greatest Cybersecurity Challenge

Areas Where AI Provides the Most Cybersecurity Benefits

AI is a double-edged sword, presenting both challenges and opportunities for cybersecurity leaders.

While concerns about AI-driven threats remain significant, 98% of CISOs recognize AI's potential to enhance cybersecurity defenses. The top perceived benefits are enhanced threat detection and improved response strategies.

These findings reinforce AI's dual nature in cybersecurity. As threats evolve, organizations must not only defend against AI-powered attacks but also harness AI-driven solutions to stay ahead. By leveraging advanced AI capabilities to counter emerging threats, CISOs can turn this disruptive force into a critical advantage.

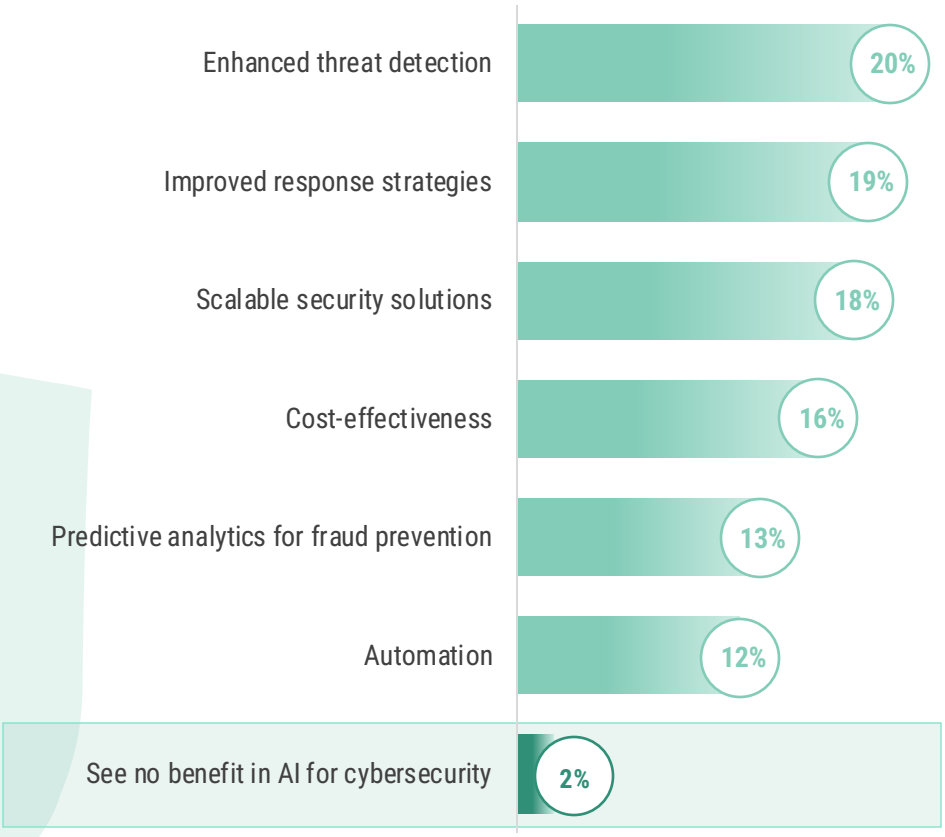

Figure 14: Areas Where AI Provides the Most Cybersecurity Benefits

Impact of AI Threats on 2025 Security Budget

100% of CISOs cite AI threats as influencing their 2025 security budgets, with those having suffered more cybersecurity damages valuing it more significantly.

Companies that have suffered financial losses exceeding $1 million are particularly attuned to AI's impact, with 28% expecting it to significantly shape their budgets—nearly double the 16% among organizations with smaller losses.

Having faced substantial financial setbacks, these leaders are taking a proactive stance against AI-driven threats, recognizing the urgent need to strengthen defenses against evolving risks.

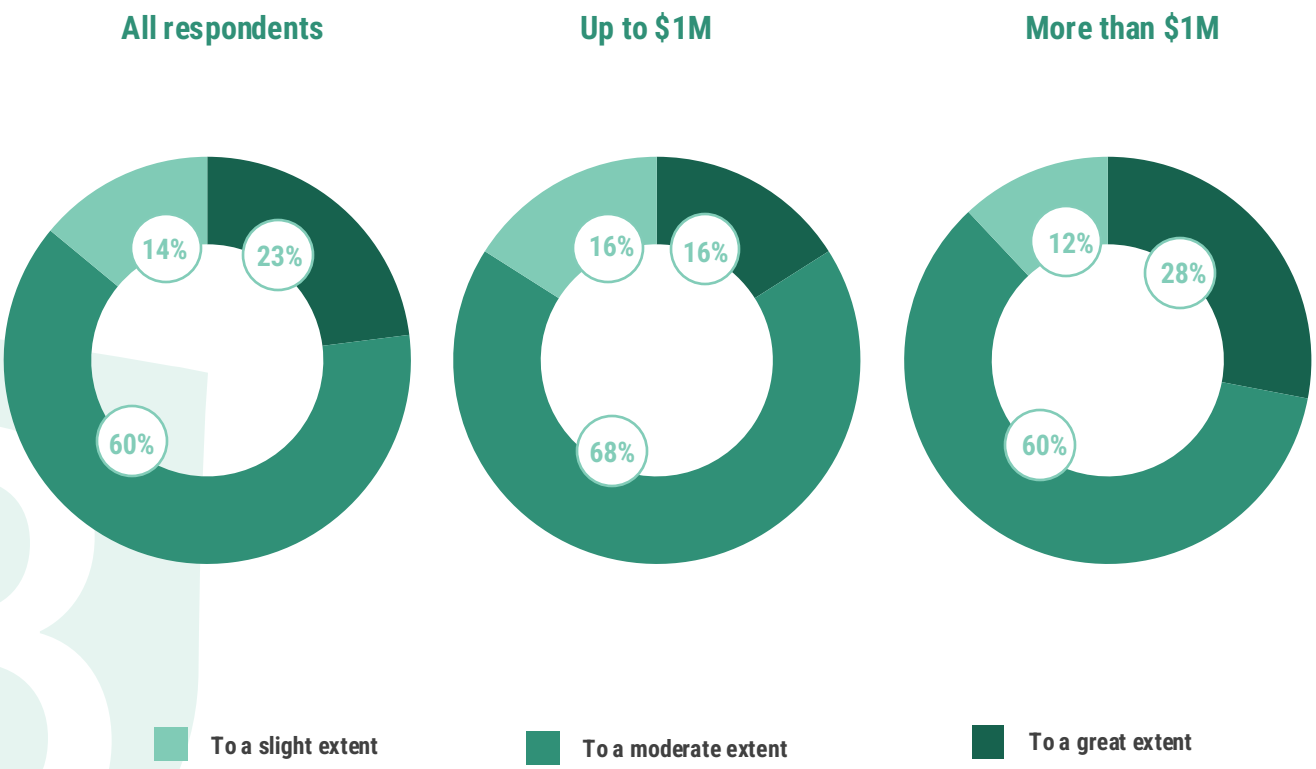

Figure 15: Impact of AI Threats on Your 2025 Security Budget, by financial damage

Strategy to Address AI-Related Threats in 2025

CISOs are approaching AI-related threats with a multifaceted strategy, integrating AI across various security initiatives.

Interestingly, AI-human collaboration is a top priority, emphasizing AI's role as a supportive tool rather than a replacement for human expertise. Also noteworthy is the balanced focus on AI's role in both threat detection and incident response, highlighting its value in both proactive and reactive security measures. With relatively close distribution across these approaches, it is clear that CISOs recognize the need to embed AI in every aspect of cybersecurity strategy— from training and compliance to collaboration and incident response.

**Question allowed more than one answer and as a result, percentages will add up to more than 100%*

Figure 16: Strategy to Address AI-Related Threats in 2025

Survey Respondent Profile

Region, Industry, Company Size

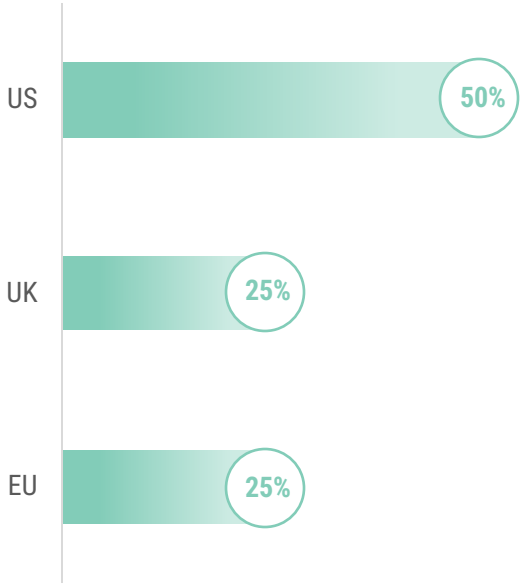

Figure 17: Region

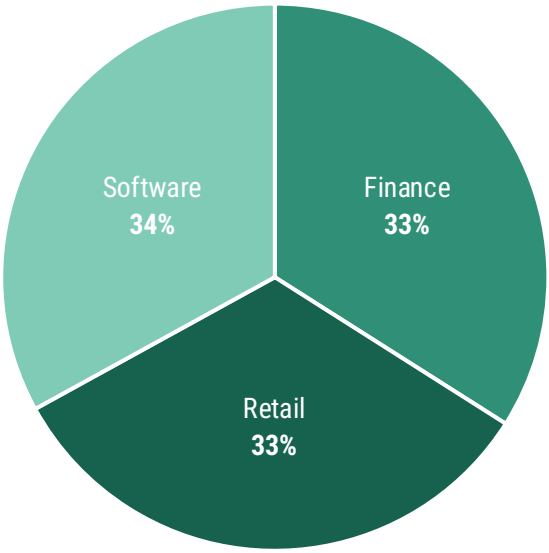

Figure 18: Industry

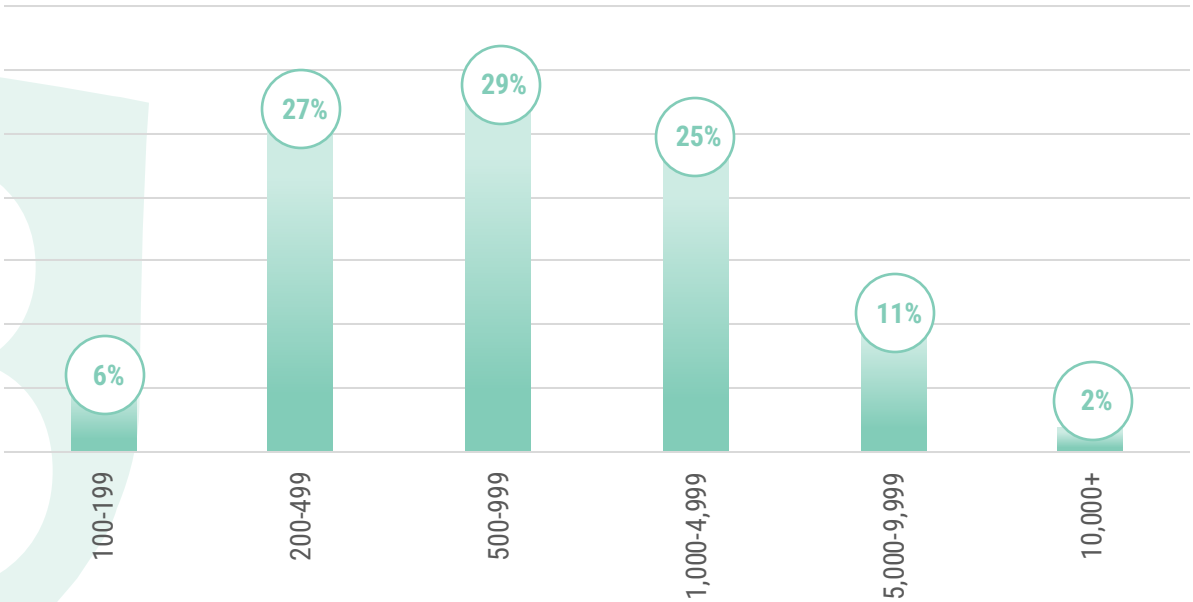

Figure 19: Company Size

About Brandshield

BrandShield is an AI-powered online brand protection and external cybersecurity solution dedicated to safeguarding customer trust in brands. The platform addresses a wide range of threats, including phishing, domain squatting, rogue mobile applications, dark web risks, counterfeiting, brand impersonation, and other malicious activities targeting brands.

As an easy-to-deploy SaaS solution, coupled with a fully managed takedown service executed by cybersecurity and intellectual property legal experts, BrandShield ensures the swift removal of harmful content and threats to brand integrity.

Trusted by industry leaders across finance, retail, e-commerce, and pharmaceuticals—including eToro, Arc'teryx, Dropbox, Tiffany & Co., and Levi's—BrandShield provides unparalleled protection for organizations with significant brand recognition. The platform integrates advanced technology with expert insights, enabling brands to concentrate on growth while their security requirements are expertly managed.

Book Your Free Demo

For more information, please visit us:

Email: info@brandshield.com