

# Budget Planning Guide 2026: Security And Risk

July 10, 2025

By Jess Burn, Jeff Pollard, Heidi Shey, Andras Cser, Janet Worthington, Cody Scott, Paul McKay, Erik Nost, Allie Mellen, and Andre Kindness with Joseph Blankenship, Sandy Carielli, Geoff Cairns, Stephanie Balaouras, Kaylee Mahoney, and Michael Belden

FORRESTER®

## Summary

With volatility now the norm, security and risk leaders need practical guidance on managing existing spending and new budgetary necessities. This data-and-insights-driven report provides spending benchmarks and recommendations that will help you budget for an unpredictable near term while enabling the business and mitigating the most critical risks facing your organization.

# Plan Through Volatility Paralysis

Budget planning for 2026 requires [flexibility](#) — and fortitude. Markets rising and falling in time with geopolitical and trade tensions mean even the best-laid financial plans could change in an instant — and then revert. Although the current period of volatility in which organizations are operating are out of your direct control, don't fall into volatility paralysis and refrain from putting off decisions. Instead, develop plans for three equally likely scenarios: baseline, boom, and bust. A baseline plan focuses on protecting controls and tech investments tied to customers, regulators, and cyber insurance. Be ready to expand those investments and test emerging security tech if additional boom plan resources become available. Take steps now to eliminate inefficiencies so that you're better equipped to handle potential budget cuts in a bust plan. No matter which scenario plays out, find resources to support innovation on your team and within your organization's business units. Volatility causes stress, but it also creates opportunities. Small, strategic experiments can position your organization to seize competitive advantages over firms that retrench in uncertainty.

## Benchmark Your Current Spending

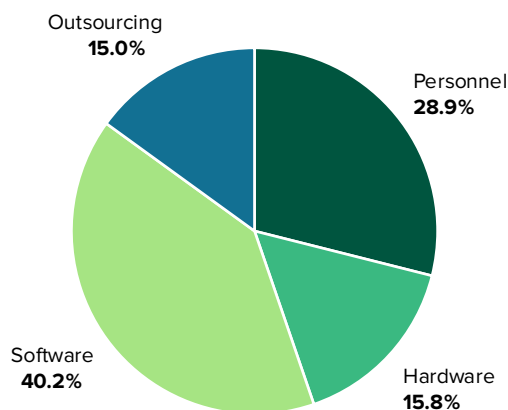
Planning through volatility doesn't mean immediately resorting to cost cutting. Ground your three scenarios in Forrester's annual budget planning data, providing you with an overview of priorities for security tech, staff, and services spend. Our data, collected across different regions and verticals, indicates that:

- **Software continues to eat more of security spend.** Data from Information Services Group indicates organizations are spending 40% of their cybersecurity budgets on software in 2025. This is more than hardware and outsourcing spend combined and 11% higher than costs allocated to the personnel expected to use and maintain the software (see Figure 1). Software's supersized slice of the budget reflects the layered approach many organizations take to security software investment. The expanding sprawl may be intentional — for example, having two or more email, messaging, and collaboration security solutions for greater phishing and business email compromise (BEC) protection. It may also be accidental — for example, having redundant capabilities like exposure management in both proactive security and detection-and-response vendor portfolios.
- **Security budgets will climb.** Over half of global security technology decision-makers responding to Forrester's Budget Planning Survey, 2025, expect sizable budget increases in the next 12 months. Fifteen percent of business and technology decision-makers anticipate a sizable jump of more than 10%, and 40% expect an increase between 5% and 10%. Geography is a factor in expectations for big budget increases. Just 9% of North American respondents expect increases of more than 10% in the next 12 months, and only 12% of EMEA respondents expect the same. In stark contrast, 22% of APAC respondents are looking for big budget leaps. Just under half of respondents do not share the budget boom exuberance, however, with 30% expecting increases between 1% and 4%. Given inflation in most advanced economies, modest increases essentially equate to a flat budget, while 10% of respondents expect their budget to remain the same. Five percent expect a decrease over the same timeframe (see Figure 2).

- **Cloud security, on-prem security tech, and security awareness top the list.** When asked about expected spending changes over the next 12 months in specific security tech or services areas, the largest percentages of decision-makers expect increases of 10% or more on items like cloud security (12%), new security technology run on-premises (11%), and security awareness and training initiatives (10%) (see Figure 3). On-premises technology holds two places among the top categories with 36% of respondents expecting to increase budgets for both new security tech and upgrades to existing security tech run on-premises by 5% or more. The survey results indicate regionally uneven cloud infrastructure adoption or maintenance as cost, security, and data sovereignty concerns lead organizations to keep some data and applications in-house or reclaim them from cloud providers. For example, 78% of APAC respondents plan to increase spending on new on-prem security tech, a full 10% higher than EMEA and 8% higher than North America.

**Figure 1**  
**Software Consumes The Largest Slice Of Cybersecurity Budgets**

**Cybersecurity cost allocation**



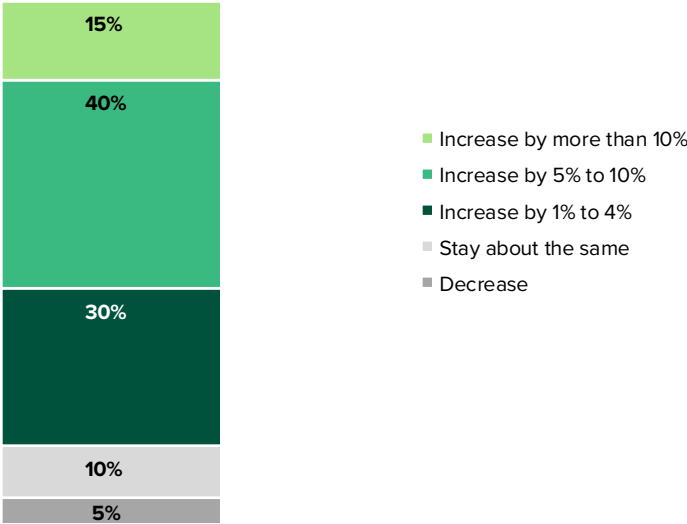
Note: Numbers may not total 100% due to rounding.

Base: 114 ISG 2024 global benchmarking data respondents

Source: © 2025 Information Services Group, Inc. Used with permission.

**Figure 2**  
**Expect Security Budgets To Increase In The Coming Year**

**“Which of the following describes any planned/anticipated change in your organization’s budget for security in the next 12 months?”**  
(Responses on a scale of 1 [decrease by more than 10%] to 7 [increase by more than 10%])

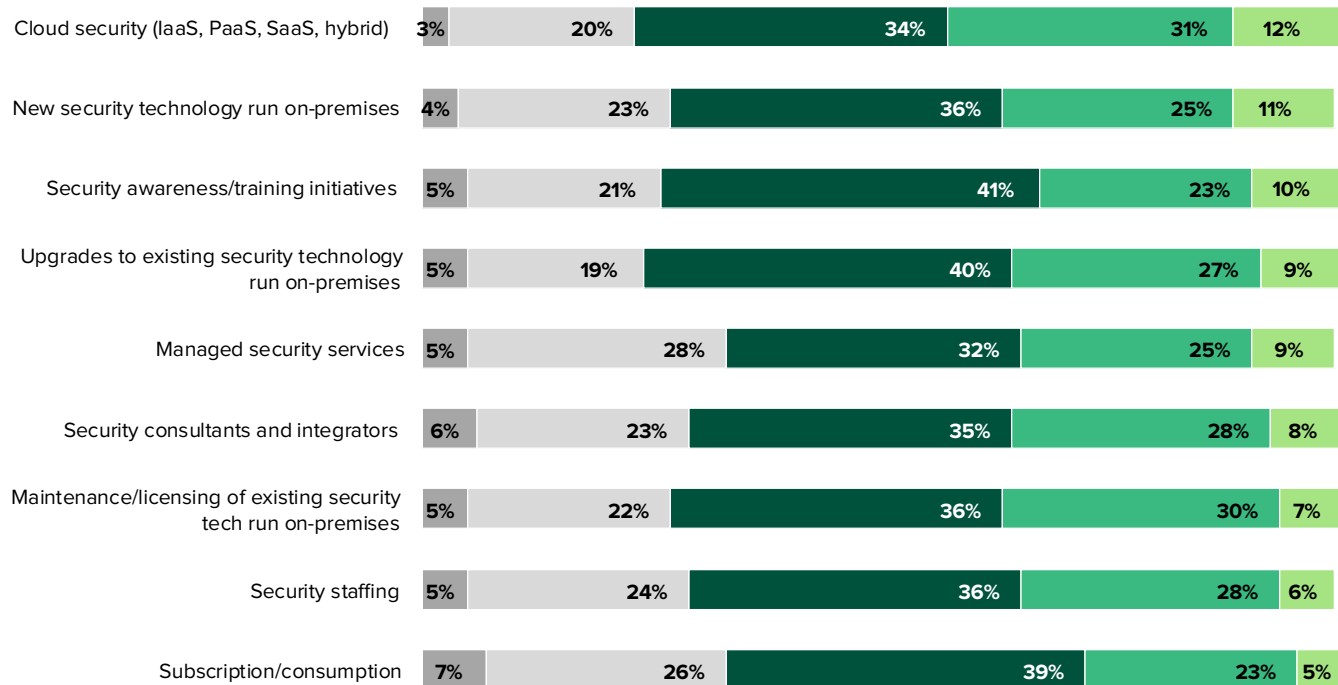


Base: 316 global technology decision-makers who work in information/IT security  
Source: Forrester’s Budget Planning Survey, 2025

© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 3

## Cloud Security And On-Premises Tech Top The List Of Anticipated Spending Increases



Note: Percentages may not total 100 because of rounding.

Base: 316 global technology decision-makers who work in information/IT security

Source: Forrester's Budget Planning Survey, 2025

© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

## Invest In Tech To Secure The Future (It's Here)

Whatever the volatile present has in store for organizations, all three of your budget planning scenarios should include investment in tools and tech that will secure the infrastructure and applications on which the business operates and the products and services the business sells. These tools will also play a critical role in meeting customer, regulatory, and cyber insurance requirements as regions and industries race to place guardrails and create standards on how sensitive data is used by AI models and agents — and on the access or permissions those entities are granted to complete tasks or produce insights. The time for experimentation is over. Invest now to:

- **Expand AI and ML security across the enterprise.** Generative AI (genAI) is reaching widespread deployment across enterprises that goes beyond standalone products. Productivity suites, CRM platforms, and help desk tools now include and promote native features and marketplaces filled with genAI capabilities. Secure genAI based on models, data, applications, and identities with tools that range from discovery, governance, vulnerability scanning, data security, and security posture to the most common concern for enterprises: prompt jailbreaking. Vendors offering security solutions for AI and ML include hyperscalers

with bundled offerings like [Google Cloud's AI Protection](#) and [Microsoft's Azure AI Content Safety](#). Traditional cybersecurity vendors are getting in the game as well, as illustrated by Palo Alto Networks' [recent acquisition of Protect AI](#). Earlier-stage companies like Knostic and CalypsoAI, featured in this year's [Innovation Sandbox at RSAC](#), all address various genAI security use cases.

- **Prepare for post-quantum security.** The urgency for migration to post-quantum cryptography (PQC) and enabling cryptoagility is accelerating despite the lack of clarity about “how to” and “by when.” NIST issued [draft transition timelines](#) for existing encryption algorithms and key establishment schemes. Most national governments are aligning to the NIST timeline of deprecation in 2030 and disallowed use in 2035. However, the Australian Signals Directorate (ASD) guidance calls for use of ASD-approved PQC algorithms by 2030. NIST also finalized [three standards](#) for PQC in August 2024, establishing a stable foundation for vendors to update their solutions. [Prioritize](#) by covering your critical asymmetric cryptography use cases first. These include protecting data at rest, in transit, and in use (desktop and mobile apps). Use cryptographic discovery and inventory capabilities to assess current posture, and partner with vendors offering cryptoagility solutions like Entrust, IBM, Keyfactor, Palo Alto Networks, QuSecure, SandboxAQ, and Thales as you define your migration path and [architecture](#).
- **Enable data discovery and classification — finally.** Understanding where your data is located and what data requires protection is an ongoing challenge. Enterprise AI deployments, AI app development, and quantum security planning reinforce how critical this capability is as a [foundation](#) for data security. AI and ML techniques have supercharged capabilities for automated data discovery and classification, improving accuracy and confidence in results. Offerings today can embed added-context sources such as data lineage to inform classification and provide visibility into data risks for data security posture management capability. Some can also discover secrets like API keys and credentials in source code or identify cryptographic algorithms in use. Vendors such as 1touch.io, BigID, Concentric AI, Forcepoint, IBM, Securi, Thales, and Varonis provide data discovery and classification. Startups such as Bedrock Security, Cyera, DataStealth, and LightBeam.ai bring different approaches to enable a variety of use cases across security and privacy.
- **Scale machine identity management.** Machine identities are pervasive in modern IT infrastructure. They can be found in apps, AI agents, infrastructure-as-code scripts, cloud environments, IoT devices, websites, access control systems, and container orchestration tools. As a result, and because of a variety of deployment methods, places of use, and large volumes, machine identities have gone beyond the point where humans can discover and externalize them from IT infrastructure. This is the business case for machine identity management. Machine identity management solutions can manage the lifecycle of machine identities and their day-to-day check-out and check-in to be used in IT infrastructure, key rotations, and role-based access control for administration. Vendors in this space include Akeyless, BeyondTrust, CyberArk, Delinea, HashiCorp, Keyfactor, and AppViewX as well as a host of recent startups such as Aembit, Astrix, Clutch, Entro, and Oasis Security.

# Divest From Standalone Tools With Nonexistent Integrations And Low Visibility

Removing tools that lack meaningful integrations and provide minimal visibility will speed the security program and increase its effectiveness. Standalone best-of-breed tools have a place for niche use cases, but overreliance on single-function tools leads to an expense-in-depth problem as multipurpose platforms become more commonplace. For tech, target platforms that offer ease of integration and use, delivering better automation and higher productivity. We recommend that security and risk leaders:

- **Divest from interactive application security testing (IAST).** Launched over a decade ago, IAST promised the accuracy of dynamic application security testing (DAST) with the code-level insights of static application security testing (SAST). While it identifies vulnerabilities by observing runtime behavior, operational challenges have limited adoption of standalone IAST tools. Teams must instrument the runtime environment with agents and insert hooks into their applications. In addition, IAST relies on automated test suites that many application development teams lack. IAST, therefore, is often not utilized. Reallocate your budget to a combined IAST/DAST solutions from vendors like Invicti and HCLSoftware, where DAST drives testing, or invest in solutions to protect your modern application architecture components such as APIs and containers.
- **Shift spend away from security service edge (SSE).** SSE filled a market gap between the adoption of software-defined WAN (SD-WAN) and the emergence of a unified secure access service edge (SASE) solution. SD-WAN requires embedded Zero Trust principles as the lack of security was the biggest hurdle for SD-WAN implementations. During COVID-19, Zero Trust network access (ZTNA) emerged to solve the mobile-worker problem VPNs couldn't handle. As a result, SSE vendors started offering ZTNA and SD-WAN security solutions. For a short time, networking vendors delivered SD-WAN capabilities and security vendors provided SSE solutions. Merging SSE with SD-WAN into SASE, however, increases operational efficiency, allows faster response to changes, and reduces security issues. Security leaders should bypass standalone SSE, SD-WAN, and ZTNA solutions and look for unified SASE providers as standalone contracts reach end of life. Now, 23 vendors offer a unified SASE offering, including Palo Alto Networks and Netskope.
- **Avoid spend on standalone cybersecurity risk ratings (CRR) products.** [CRR products](#) have been used by security, risk, and procurement leaders as a due diligence check when onboarding or renewing third-party relationships. Security leaders use these products and associated data in a variety of processes, including third-party risk management (TPRM), external attack surface management (EASM), and monitoring organizational cyber posture. CRR products are a signal in your tech stack. To be effective, they must be well integrated with the risk technology suite, spanning [attack surface management](#), [TPRM](#), [governance, risk, and compliance](#) (GRC), and [cyber risk quantification](#) (CRQ) solutions to provide a full picture of first-through-nth-party risk exposure. Divest from standalone CRR products. They generate more noise for security leaders and often lack strong remediation support

requiring integration and context. Focus on an integrated TPRM and continuous monitoring approach that facilitates [continuous risk management](#). Consider offerings from UpGuard, Panorays, and RiskRecon.

- **Consolidate endpoint security and SIEM tooling.** Endpoint detection and response (EDR) and endpoint protection platform (EPP) providers have been pushing consolidation for years. Consolidating simplifies agent management, reduces resource consumption, and provides centralized context for endpoint threats, improving [analyst experience](#) (AX). Now that EDR providers have moved to [extended detection and response](#) (XDR), there's another opportunity for consolidation: capabilities that replace security information and event management (SIEM) tools. In addition to native XDR capabilities, many vendors are providing third-party data ingest for detection, correlation, investigation, and response (mostly cloud, identity, and email detection). The features aren't yet as comprehensive as a [security analytics platform](#). But security pros seeking an SIEM tool with higher-quality detections can look to XDR as an effective option to improve AX, consolidate tooling, and potentially reduce costs. Microsoft, CrowdStrike, and Palo Alto Networks offer consolidated XDR and SIEM.

## Experiment With Tech Providing Rapid Remediation And Enhanced Experience

If budgets remain flat or increase, CISOs can plan to maximize the use and utility of current security and risk management technologies. If there is a hiring freeze or cuts to the security team, security leaders should better understand the still largely free genAI features that exist in their current tech stack to find efficiency gains.

Exploring genAI use cases can save staff time on mundane tasks and free them to fill the widening skills gap needed to secure agentic AI and genAI in other parts of the organization. Selectively invest in new tools or capabilities that allow your organization to seize opportunities, address emerging customer requirements, and differentiate from competitors through demonstrated organizational readiness and resilience. We recommend that security and risk leaders:

- **Establish a trust center.** Initially embraced by high-tech firms as a repository for GDPR compliance info and security attestations like SOC 2 and ISO 27001, trust center adoption is growing in healthcare, financial services, and nonprofits. Trust centers serve as centralized hubs for information and transparent communication about security policies and practices, privacy measures, and compliance status for key customers, partners, and regulators. Security leaders are using trust centers to drive self-service and streamline customer acquisition, contract renewals, and annual inbound third-party risk assessments. Additionally, trust centers use AI to automate responses to security questionnaires, leveraging a knowledge base of pre-approved answers and documentation to reduce time to respond. Provider choice has also increased, with nearly 20 vendors now offering trust center solutions. Investigate offerings from providers like Safebase, Vanta, Conveyor, and Drata. Pilot trust center use with a subset of customers, prospects, and partners for which self-service may be appropriate.



- **Embrace automated remediation.** [Proactive security](#) solutions have matured in visibility through [attack surface management](#) features and in prioritization through [exposure management](#) and [continuous security testing](#) features. Once organizations have good visibility and prioritize exposures, they have to remediate them. With visibility and prioritization assessed more continuously, security teams need automatic response and remediation to keep up with growing backlogs. Many proactive security solutions automate response efforts, like building dynamic remediation projects that add new issues and automate ticketing. Automated remediation is improving to support use cases in patch management, asset containment, and application blocking. Vendor solutions include Microsoft's MDVM, which integrates with Intune to automatically block vulnerable applications, and Tanium's autonomous endpoint management that analyzes and deploys available patches. Startups like Mondoo automate fixes for DevOps teams to pull into their pipeline.
- **Deploy deepfake detection.** Video, audio, and image deepfakes — boosted by genAI and increasingly cheap computational power — have become [indistinguishable from their genuine counterparts](#). Defenses that may have worked six to 12 months ago (e.g., asking subjects to turn their head sideways, blink, and move their hand in front of their face) are now largely useless due to advances in genAI. Protecting employee identity verification and transactional authentication and integrity — without affecting the user experience — remains a priority. Ensemble models in modern deepfake detection solutions now use spectral, artifact, image noise, skin tone, lighting, echo, and device identity reputation analysis on real-time streaming media. Deepfake defense solutions can provide risk scores for deepfake media in real time, explain their risk scores using reason codes, and provide additional case management and reporting features. Sample vendors include GetReal Security, Sensity, and Reality Defender.
- **Automate compliance with continuous control monitoring (CCM).** AI-driven automation, real-time analytics, and integration with cloud-native environments have transformed CCM into a practical and affordable solution. No longer reserved for “high maturity” security and GRC teams, CCM continuously validates security controls against multiple frameworks and standards across complex IT ecosystems by: 1) setting technical control parameters (e.g., account management policies, vulnerability-patching timelines, log retention rules, etc.); 2) automatically testing control performance; and 3) gathering evidence to justify findings. CCM streamlines traditional security audits and control assessments by providing visibility into control effectiveness and enables proactive risk detection — capabilities key to resilience, materiality-focused governance, and [continuous risk management](#). Consider vendors such as CyberSaint, Drata, Secureframe, Thoropass, and Vanta for robust control and assurance automation.

# We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

## Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer-obsessed.

### Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

[Learn more.](#)

### Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

[Learn more.](#)

### Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

[Learn more.](#)

FOLLOW FORRESTER



Contact Forrester at [www.forrester.com/contactus](https://www.forrester.com/contactus).

Forrester, 60 Acorn Park Drive, Cambridge, MA 02140 USA

Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | [forrester.com](https://forrester.com)

Not Licensed For Distribution.

© 2025 Forrester Research, Inc. All trademarks are property of their respective owners.

For more information, visit the [Citations Policy](#), contact [citations@forrester.com](mailto:citations@forrester.com), or call +1 866-367-7378.