S&P Global
Market Intelligence
451 Research
Business Impact Brief

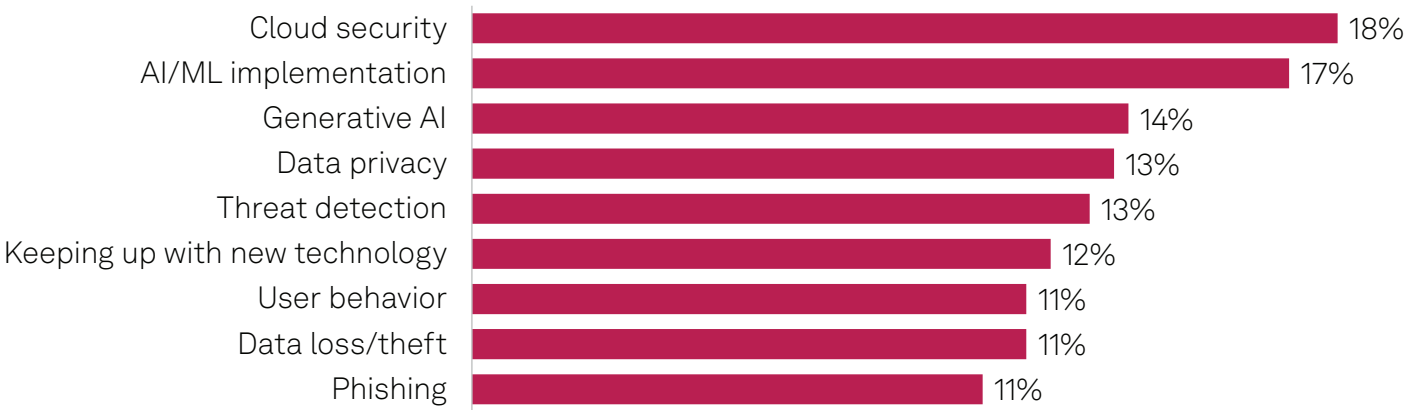
Managing risk across a rapidly changing IT landscape

The Take

Organizations are increasingly adopting highly virtualized, cloud-native IT architectures, including containerized and serverless applications, which offer benefits such as scalability, elasticity and potentially lower costs. AI systems have accelerated these deployments, as many run in public and private cloud environments. However, these approaches can also entail higher risks due to constantly changing and expanding attack surfaces that are difficult to monitor and secure.

Organizations on average allocate about one-third of their total IT security budget to securing off-premises cloud architectures, according to 451 Research's Voice of the Enterprise (VotE): Information Security, Cloud Security 2025 study. And while most organizations have two or more cloud service providers, only about half of third-party security tools and services in use are designed for multicloud environments. This issue is echoed in 451 Research's VotE: Information Security, Budgets & Outlook 2024 study, where participants ranked cloud security as their top information security pain point.

Top information security pain points



Q. What are your organization's top information security pain points? Please select up to three.
Base: All respondents (n=370).
Source: 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2024.

Two in five respondent organizations (40%) use open-source tools and libraries, with lower cost and high reliability cited as the primary advantages driving their adoption. Unfortunately, many organizations are unaware of the extent of open-source usage, and thus a lack of security is the top-cited challenge associated with its use.

Business Impact

Improving risk and vulnerability assessment/management was the top strategic security objective for 2024, according to 451 Research's VotE: Information Security, Budgets & Outlook 2024 study. This challenge typically stems not from a lack of data but from the inability to effectively gather, centralize, normalize and de-duplicate data from multiple sources. If security practitioners cannot identify high-value signals for actionable insights, it becomes difficult to determine and prioritize risks, which is essential for eliminating high-priority risks and establishing compensating controls. Data lakes and data fabrics based on the Open Cybersecurity Schema Framework standard, along with advanced data integration, transformation and analytical tools, are helping to address this issue. Additionally, combining generative AI with traditional AI/ML technologies in security use cases shows potential to help security analysts respond more quickly to emerging incidents and proactively resolve security issues.

One contributing factor to these challenges is the high number of IT infrastructure platforms in use — multiple public clouds, SaaS, private cloud, on-premises and mobile endpoints — combined with a corresponding proliferation of tools to manage and secure them. Tool sprawl often leads to fragmented visibility and contextual switching (i.e., "swivel chair management"), resulting in long detection, analysis and resolution times, which can cause unacceptable production downtimes. One strategy to address these issues is to replace many specialized tools with a single security management platform that centralizes data and analytics, providing a single source of truth for troubleshooting.

Continuing skills shortages also contribute to security challenges. In 451 Research's VotE: Digital Pulse, Technology Skills 2024 study, information security ranked as the No. 2 area facing technical skills shortages, behind AI/ML and ahead of IT infrastructure and systems, and cloud platforms and operations. This shortage hampers organizational goals to implement "shift-left" DevSecOps models, which require that developers have the tools and expertise to detect and address security issues early in development. Teams must prevent suspicious builds from reaching production. One potential solution is to implement self-service software templates that ensure compliance with security practices during code writing, minimizing developer overhead while addressing burnout.

Looking Ahead

Organizations seeking to reduce overall risk from cloud environments and open-source technologies should consider the following actions:

1. Simplify security tool stacks by adopting tools that support multiple cloud providers and on-premises architectures and can leverage a centralized platform and data lake strategy.
2. Transition to an integrated DevSecOps platform that supports security across the application life cycle, providing "code-to-cloud" security management capabilities.
3. Combine posture management with detection and response to enable proactive risk-based remediation alongside threat detection and response capabilities that gather, normalize, de-duplicate and prioritize issues, recommend remediation actions and streamline processes.
4. Adopt a consistent, best-practices security strategy that includes a risk-based approach and continuous improvement methodology, such as the NIST CSF 2.0 framework.
5. Deploy tools designed to ensure security across the software supply chain, including open-source scanning and verification of software components and dependencies.
6. Ensure that security tooling aligns with regulations and internal policies. Compliance with internal, industry and governmental regulations such as GDPR, HIPAA, PCI-DSS and NIST is essential for virtually every organization. Security solutions must meet monitoring and reporting requirements, retain log data for at least a year, and provide anomaly detection, incident response and daily log review capabilities. Data sovereignty issues may also arise, requiring compliance with regulations regarding data storage in specific countries or geographies.
7. Monitor AI-driven innovation, including GenAI-driven assistants, improvements in traditional AI/ML techniques and hyperautomation, which combines classic AI/ML models and agentic AI into intelligent agents capable of autonomous and semi-autonomous orchestration and actions.