S&P Global
Market Intelligence

AI growth increases demands for hybrid cloud security

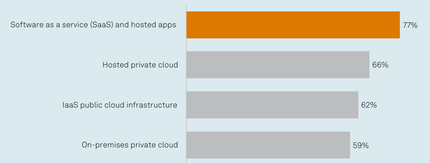
Four key trends are projected to increase the need for **unified hybrid cloud security platforms** in 2025:

- Hybrid cloud security challenges
- Demand for unified security platforms
- The impact of generative AI
- Increasing data centralization

1. Hybrid cloud security challenges

Organizations are **struggling to secure hybrid environments** that often include public and private clouds, SaaS and on-premises systems. The use of siloed security solutions can result in increased attack surfaces, security blind spots and heightened risk.

Over the next two years, adoption of SaaS and hosted apps is projected to reach 77%. Public cloud, hosted and on-premises private cloud growth will also be significant.

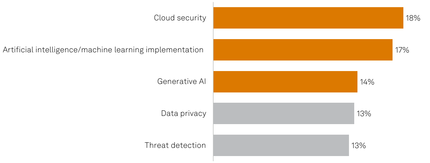


Q. In which of the following types of locations - if any - has your organization currently deployed IT infrastructure or applications? Please select all that apply.
Q. Which of the following (additional) types of locations will your organization deploy IT infrastructure or applications into during the next two years? Please select all that apply.
Base: All respondents (n=1021).
Source: VotE: Digital Pulse, Cloud, & Datacenter, Workload Placement & Migration (Combined Study) 2024.

2. The impact of generative AI

The emergence of generative AI adds complexity to cloud workloads, requiring specialized security measures and advanced analytics. AI-driven applications often operate in multicloud environments, exacerbating security challenges. Security strategies must adapt to address risks from AI workloads, ensuring robust protection across all deployments.

Cloud security, AI/ML and generative AI are respondents' top three information security pain points in 2024.



Q. What are your organization's top information security pain points? Please select up to 3.
Base: All respondents (n=370).
Source: 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2024.

3. Increasing data centralization

Centralizing security data via a data lake strategy can improve security data fidelity. Normalizing and consolidating data from various sources **reduces the volume of alerts** and **enhances the ability to detect and respond to threats**, alleviating the burden on security teams and improving their efficiency.

A centralized security analytics platform can **unify controls**, **provide ecosystem-wide visibility** and **reduce tool sprawl**. It can also **minimize manual coordination between systems**, **reduce costs** and **improve consistency**, thereby strengthening security posture, simplifying compliance and minimizing risks.

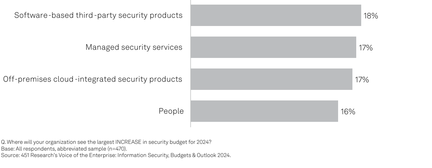
4. Demand for unified security platforms

SOC teams on average say they are typically **unable to investigate over 40% of SIEM and security analytics alerts** — a byproduct of increasing volumes of noisy, low-fidelity data and tool sprawl.

In response, organizations seek to streamline security operations through **a unified security platform** that can provide centralized visibility across hybrid, multicloud environments.

These platforms help reduce tool sprawl, enhance operational efficiency, and improve security posture by integrating security functions into a **cohesive framework to manage complex IT infrastructures.**

60% of organizations surveyed seek to adopt an integrated operating model with seamless interoperability between IT environments over the next two years. Respondents also indicated that investments in SaaS-delivered third-party security products were their top choice in 2024.



Q. Where will your organization see the largest INCREASE in security budget for 2024?
Base: All respondents, abbreviated sample (n=470).
Source: 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2024.

Considerations for selecting a modern cloud platform to drive data security and compliance

451 Research's Voice of the Enterprise: Digital Pulse, Cloud & Datacenter, Workload Placement & Migration 2024 study indicates that delivery models such as **SaaS can offer the following benefits**:

Reduced operational burdens by offloading to a specialized provider, while expenditures shift to an opex model

Expert support, proactive monitoring and automated updates to ensure the platform remains secure and optimized without requiring in-house resources

Improved cost predictability and reduced risks due to built-in compliance and security features coupled with faster implementation

Organizations with hybrid on-premises and cloud workloads could benefit from a cloud security platform with its feet firmly planted — and capabilities well established — **in both worlds**.

AI-driven, cloud-based platforms can deliver unified security and insights, **enabling faster threat detection**, **investigation and remediation.** Support for all major cloud service providers' management and security regimes is also a key consideration.

With hosted (SaaS) solutions, additional factors may include **adherence to compliance standards and regulations** such as SOC, ISO, PCI-DSS, HIPAA, FedRAMP, DoD and IRAP; implementation of security regimes such as the Cloud Security Alliance Cloud Controls Matrix; and support for specific industry and governmental compliance requirements.