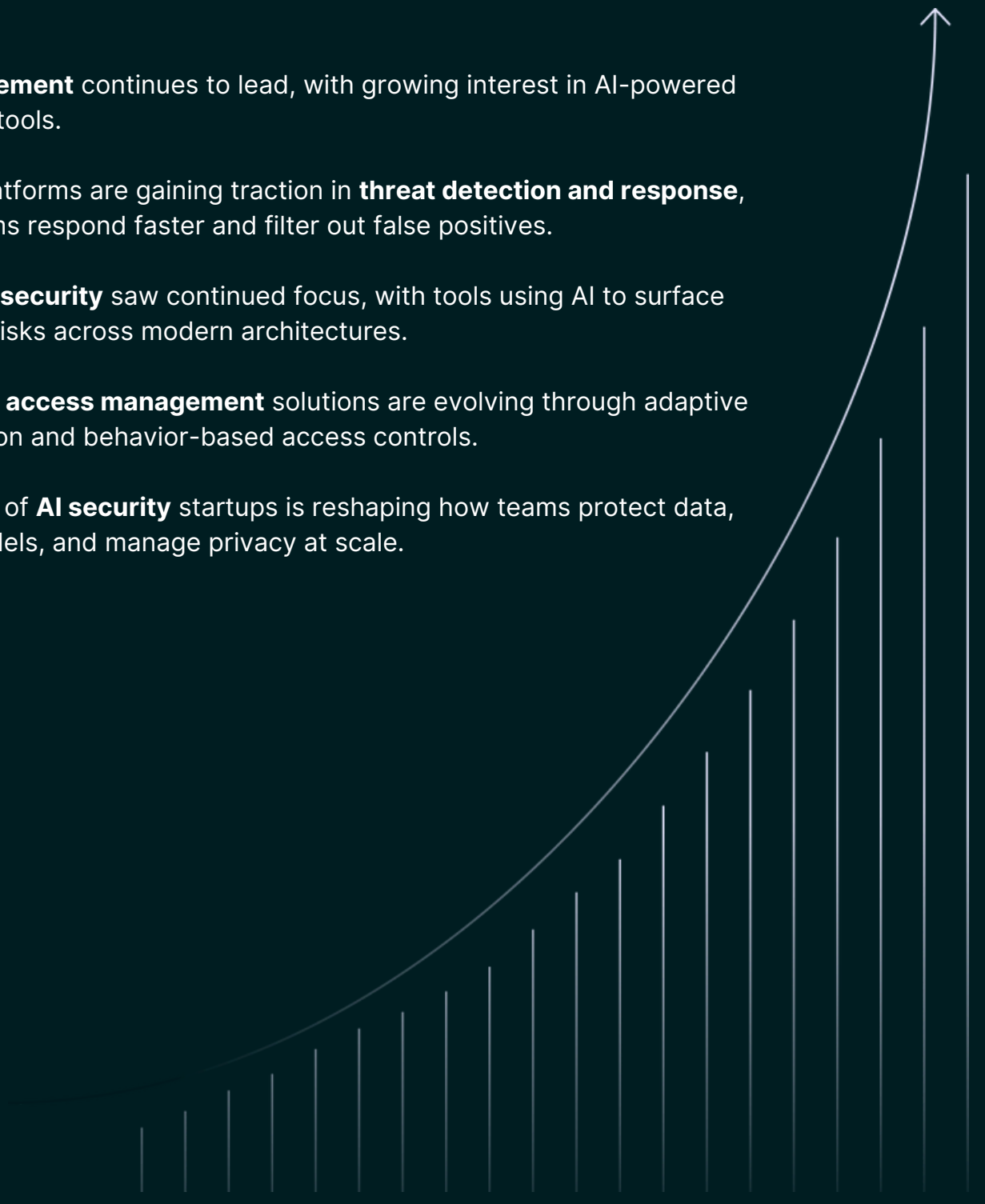
sagetap

Q1 2025 Cybersecurity Report
Published May 19, 2025

Security Insights From Verified Execs

Highlights

- **Risk management** continues to lead, with growing interest in AI-powered compliance tools.
- AI-native platforms are gaining traction in **threat detection and response**, helping teams respond faster and filter out false positives.
- **Application security** saw continued focus, with tools using AI to surface exploitable risks across modern architectures.
- **Identity and access management** solutions are evolving through adaptive authentication and behavior-based access controls.
- A new wave of **AI security** startups is reshaping how teams protect data, monitor models, and manage privacy at scale.



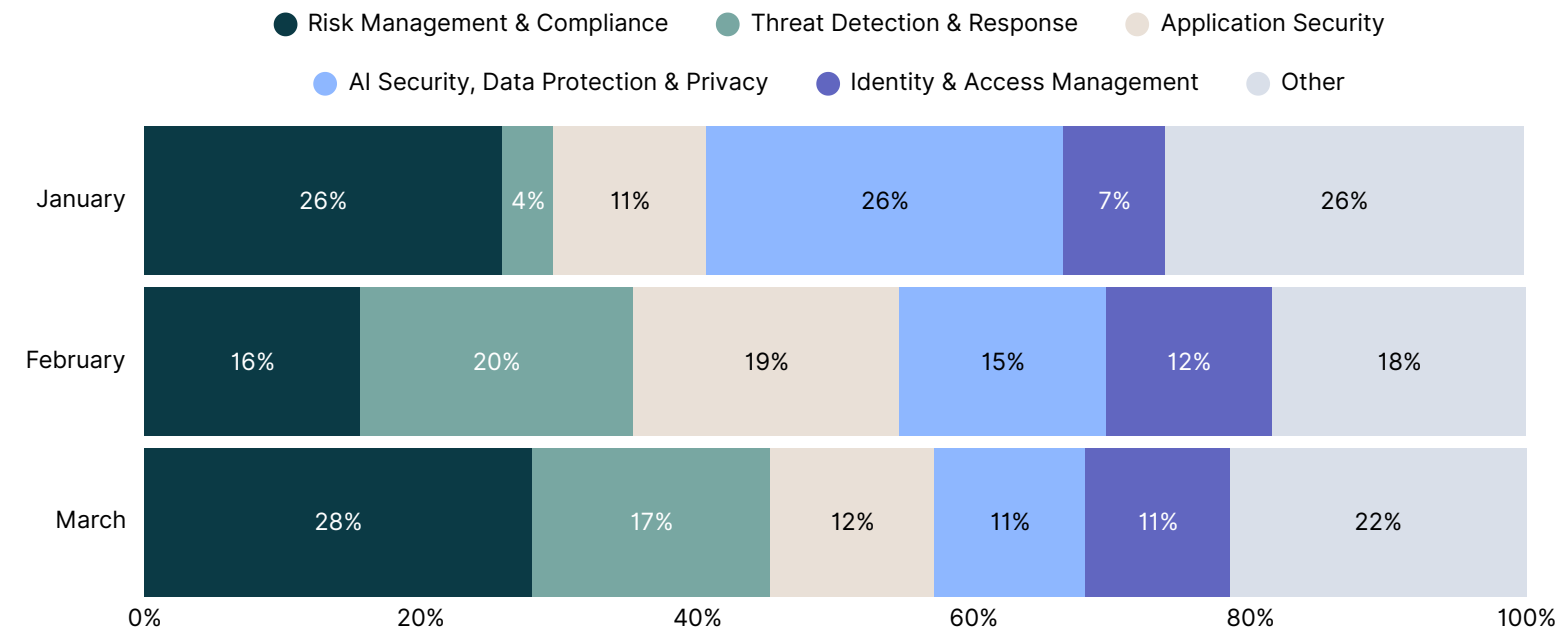
sagetap

Q1 2025 Cybersecurity Report

At Sagetap, we track trending technology initiatives and top products that enterprise security leaders on the platform ("Sages") are actively exploring to stay ahead of evolving challenges. This Q1 report highlights key cybersecurity trends based on Sages' initiatives, vendor meetings, and purchasing decisions.

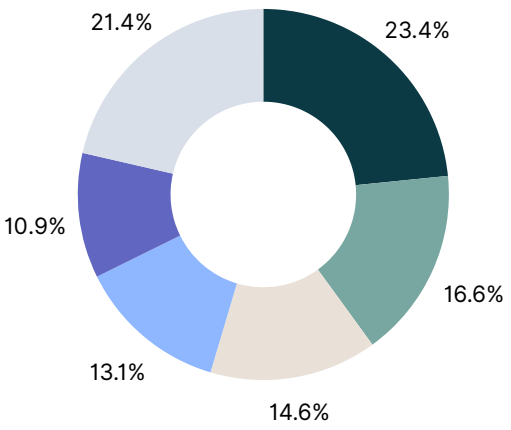
It reveals where high-performing security teams are focusing their attention and which areas show the most momentum, innovation, and early signals of future investment. AI is reshaping legacy categories like compliance, identity, and threat detection — and driving the creation of entirely new categories like AI security, data protection and privacy. Read along to stay in sync with where the industry is headed in 2025.

Security Leaders' Top Priorities in Q1



According to the distribution of Sages' meetings and purchasing interest in Q1, the top five categories in cybersecurity are:

1. Risk Management & Compliance
2. Threat Detection & Response
3. Application Security
4. AI Security, Data Protection & Privacy
5. Identity & Access Management

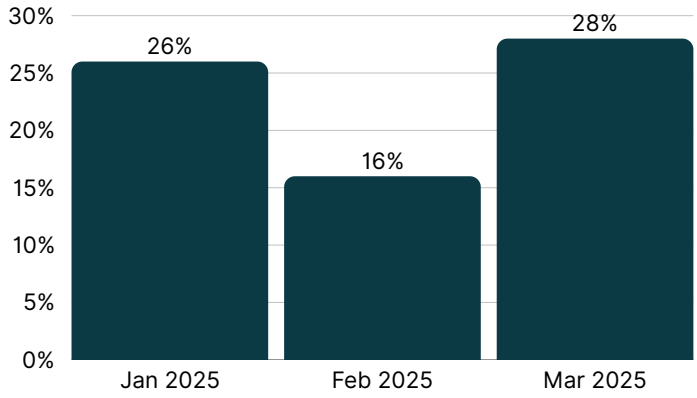


To browse peer initiatives and create your own, visit Sagetap.

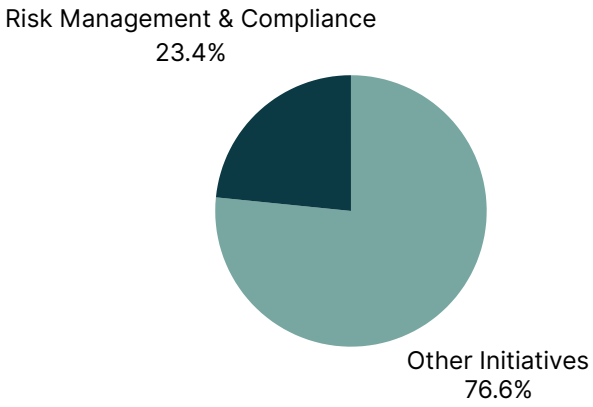
sagetap

Risk Management & Compliance

Percentage of Security Meetings on Sagetap for Risk Management & Compliance Initiatives



Meetings Focused on Risk Management & Compliance vs. Other Security Topics



Risk management and compliance remained the top category for Sages in Q1, and interest is rising in AI-powered platforms that reduce manual effort and improve control visibility. Sages are searching for smarter, more scalable ways to meet evolving regulatory demands.

What Sages Are Looking For

Automating & Scaling Risk Programs

- Security leaders are seeking tools that automate risk assessments, compliance tracking, and evidence collection across frameworks like SOC 2 and ISO 27001.
- AI-enhanced platforms are gaining traction for reducing audit fatigue and predicting potential control failures.

Gaining Visibility & Control Over Data & Vendors

- A key focus is improving visibility into sensitive data usage, access, and classification across environments to stay ahead of compliance requirements.
- Centralized platforms with built-in intelligence are helping teams manage vendor risk more proactively.

Top Products Considered

DRATA

Drata automates security and compliance monitoring through continuous evidence collection and streamlined workflows that keep teams audit-ready.
Visit Drata

SAFE

SAFE quantifies an organization's cyber risk by merging internal signals, threat intelligence, and business context into a single, measurable score.
Visit SAFE

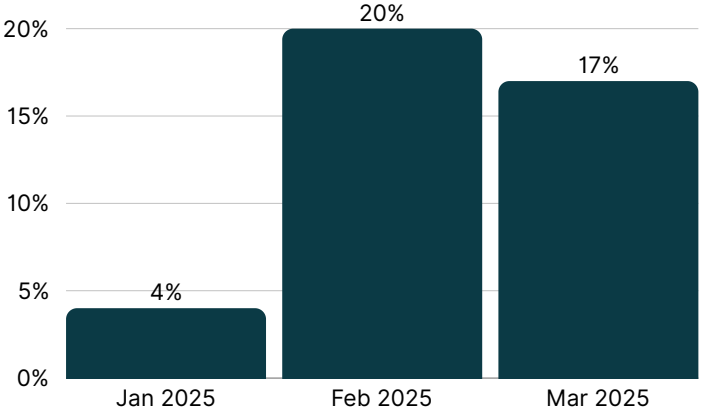
VISO TRUST

VISO TRUST uses AI to evaluate third-party risk from existing documentation, enabling fast, scalable vendor reviews without manual effort.
Visit VISO TRUST

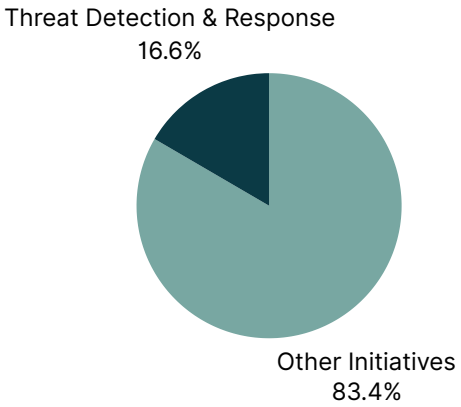
sagetap

Threat Detection & Response

Percentage of Security Meetings on Sagetap for Threat Detection & Response Initiatives



Meetings Focused on Threat Detection & Response vs. Other Security Topics



Threat detection and response was a key area of focus for Sages in Q1. Meetings commonly focused on leveraging AI and automation, unifying visibility across environments, and accelerating threat remediation. Interest continues to build around platforms that combine automation with real-time behavioral analytics.

What Sages Are Looking For

Helping Security Teams Work Smarter, Not Just Harder

- Security leaders are turning to AI and automation to eliminate noise, reduce alert fatigue, and help teams stay focused on real threats.
- Demand is rising for actionable threat intelligence that facilitates faster threat comprehension and response.

Gaining Visibility & Responding Faster

- Sages want to upgrade their security tools to get a clear view of threats across all their systems (computers, networks, cloud) in one place.
- AI-powered behavioral models and triage tools are helping surface high-priority threats faster and more accurately.

Top Products Considered

VEROSINT

Verosint stops identity-based threats in real time using AI-driven behavioral analytics and unified visibility across accounts and identity systems.
Visit Verosint

halcyon

Halcyon defends against ransomware with AI-powered detection, autonomous containment, and built-in recovery capabilities.
Visit Halcyon

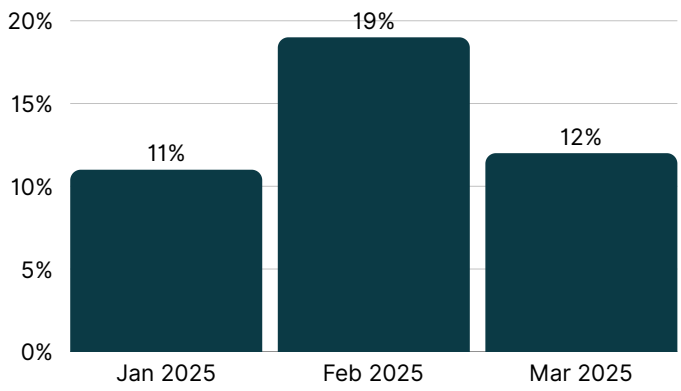
praetorian

Praetorian uncovers threats through a continuous exposure management platform that blends AI-enhanced automation with expert insight.
Visit Praetorian

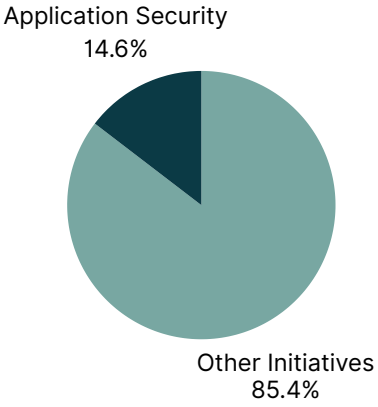
sagetap

Application Security

Percentage of Security Meetings on Sagetap for Application Security Initiatives



Meetings Focused on Application Security vs. Other Security Topics



Application security was a major priority, with a growing focus on securing modern architectures such as APIs and Kubernetes. Sages often aimed to embed security across the SDLC through DevSecOps practices. AI is gaining momentum for helping teams prioritize the most critical, exploitable risks.

What Sages Are Looking For

Securing Cloud Architectures & Prioritizing High-Impact Vulnerabilities

- Security teams are adopting next-generation DAST solutions tailored to APIs, integrated directly into developer workflows.
- Projects focused on securing Kubernetes workloads and containers highlight the need to address security challenges in modern cloud-native environments.

Embedding Security Throughout the SDLC

- There's a drive to embed secure code practices and tools like SAST and SCA into the CI/CD pipeline to detect vulnerabilities early in the development cycle.
- Organizations are looking to implement AI and ASPM for better visibility, risk prioritization, and automated remediation across their applications.

Top Products Considered

qwiet AI

Qwiet applies AI to surface vulnerabilities across code, dependencies, and infrastructure, offering contextual insights from a single interface.
Visit Qwiet

Jit

Jit embeds security into the development process by orchestrating tools and policies to deliver continuous, automated protection.
Visit Jit

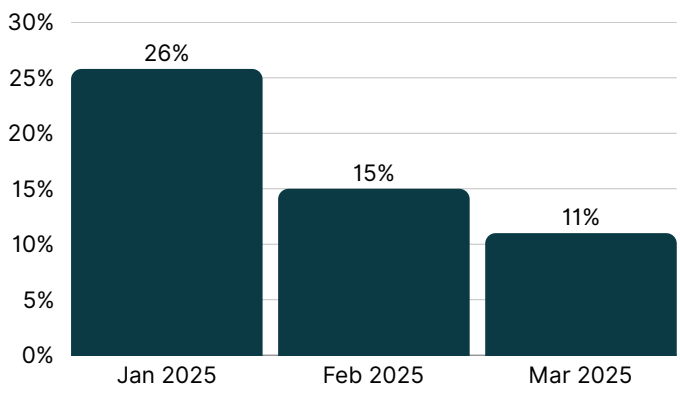
BACKSLASH

Backslash Security uses AI to give AppSec teams actionable visibility into reachable, exploitable risks, enabling faster remediation and better risk decisions.
Visit Backslash Security

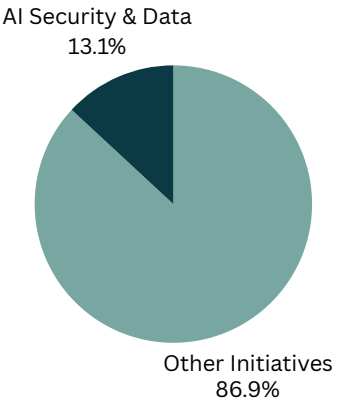
sagetap

AI Security, Data Protection & Privacy

Percentage of Security Meetings on Sagetap for AI Security, Data Protection & Privacy Initiatives



Meetings Focused on AI Security, Data Protection & Privacy vs. Other Security Topics



AI security, data protection and privacy emerged as a fast-growing category in Q1, driven by the need to govern AI use and secure sensitive data. Sages are exploring solutions that provide visibility into AI interactions, enforce usage policies, and combine threat detection with real-time data protection.

What Sages Are Looking For

Governing AI Use Across the Enterprise

- Organizations are prioritizing AI governance to manage risks associated with the rapid adoption of generative AI tools like ChatGPT, Claude, and Copilot.
- Visibility into AI tool usage and data flows is critical for compliance with emerging regulations such as the EU AI Act and internal data protection policies.

Proactive, AI-Driven Data Security

- Enterprises are shifting to AI-enhanced security platforms that combine threat detection, DLP, and sensitive data discovery into a unified solution.
- Demand is growing for tools that reduce false positives, track sensitive data in real time, and secure LLM interactions.

Top Products Considered

CYERA

Cyera uses AI to discover and classify sensitive data across cloud environments, helping security teams enforce access and mitigate exposure.
Visit Cyera

harmonic

Harmonic Security secures unstructured data by applying AI to detect sensitive content and prompt users with in-the-moment security actions.
Visit Harmonic Security

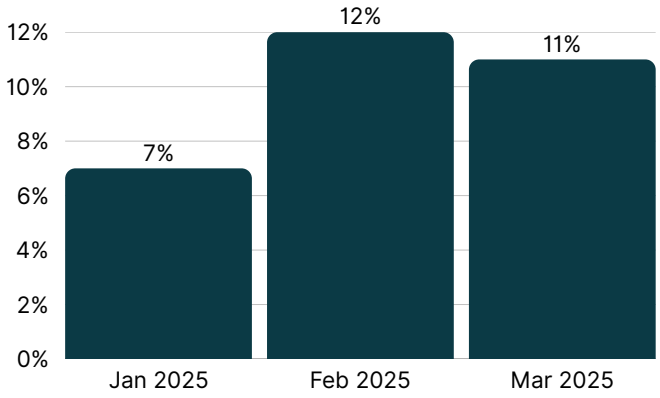
skyflow

Skyflow isolates and protects sensitive data using a zero-trust data privacy vault with intelligent controls that simplify secure sharing and usage.
Visit Skyflow

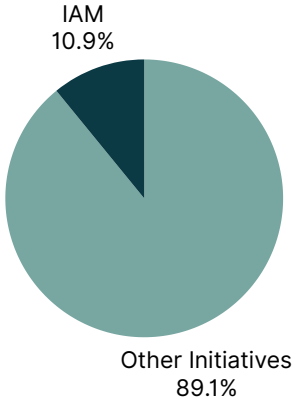
sagetap

Identity & Access Management

Percentage of Security Meetings on Sagetap for Identity & Access Management Initiatives



Meetings Focused on Identity & Access Management vs. Other Security Topics



In Q1 of 2025, identity and access management remained a focus for Sages, with projects and related meetings spanning internal identity centralization as well as seamless, secure customer login experiences. AI is shaping how teams detect access anomalies and automate identity workflows.

What Sages Are Looking For

Centralizing Identity & Access Management (IAM)

- Sages want to manage all user identities in one place to improve operational efficiency and strengthen access controls.
- They're increasingly interested in platforms that use AI to monitor behavior and flag unusual activity.

Improving Customer Identity & Access Management (CIAM)

- Sages aim to make it easy and secure for customers to access their services with solutions like centralized identity and SSO.
- Adaptive authentication flows powered by AI are gaining attention for improving both security and user experience.

Top Products Considered

Teleport

Teleport secures infrastructure access with identity-based authentication, replacing secrets and improving operational resilience.
Visit Teleport

descope

Descope provides a no-code platform for CIAM, letting developers build secure, adaptive authentication flows without adding backend complexity.
Visit Descope

Doppler

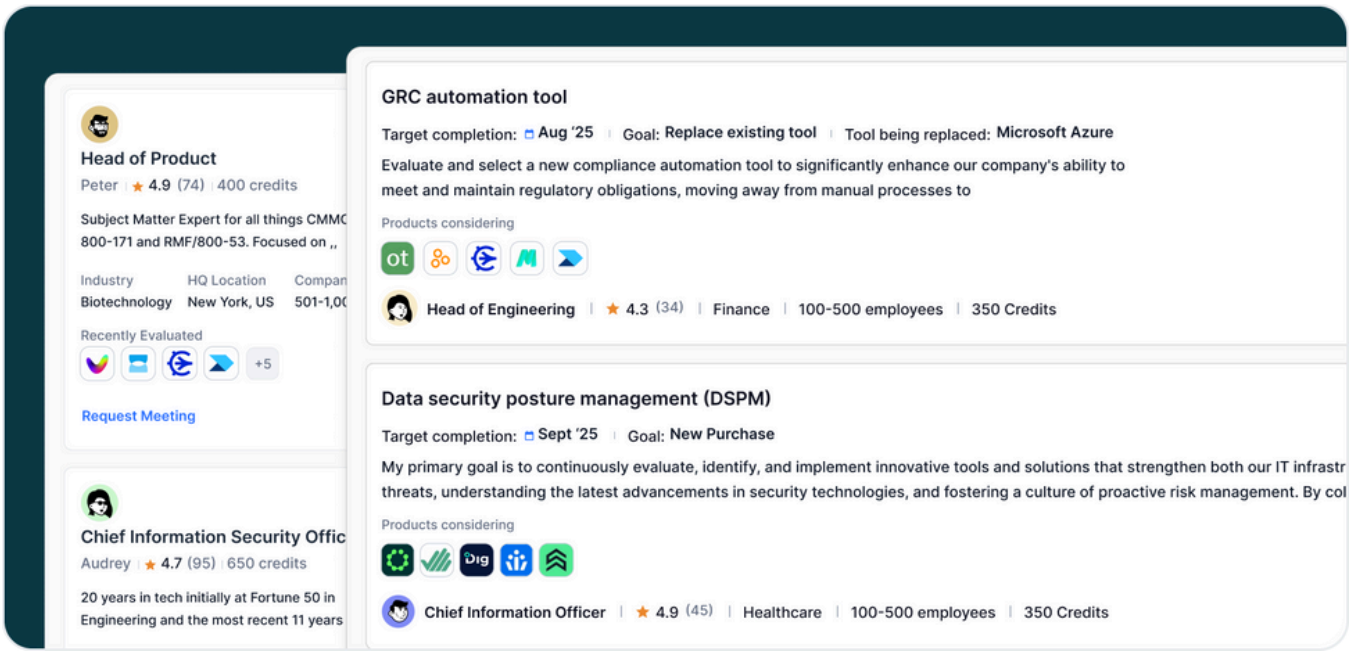
Doppler manages secrets across environments from a single source of truth, ensuring consistent and secure access for every team.
Visit Doppler

sagetap

This report provides a data-driven perspective on the current priorities of security leaders. It highlights where interest is accelerating — and where AI and other emerging technologies are reshaping the cybersecurity landscape. Use these insights to anticipate the market's direction, refine your strategy to stay competitive, and pinpoint areas for investment across key cybersecurity domains.

Join Sagetap for personalized product recommendations that align with your team's top initiatives.

Explore tailored solutions for free →



Showcase Your Expertise to Peers

Build detailed user profiles that highlight your expertise, ongoing projects, and contributions.

Engage with Trusted Anonymity

Meet anonymously until you're ready, maintaining full control over every engagement.

Learn from Peer-Driven Insights

Gain insight from real practitioners who've implemented the tools you're evaluating.

Accelerate Technology Adoption

Monitor product performance and peer outcomes at every stage of evaluation.

Manage Your Evaluation Process

Document your requirements, track evaluation recordings, and score each solution.

See the Gaps, Shape the Future

Discover personalized product recommendations that align with your enterprise goals.