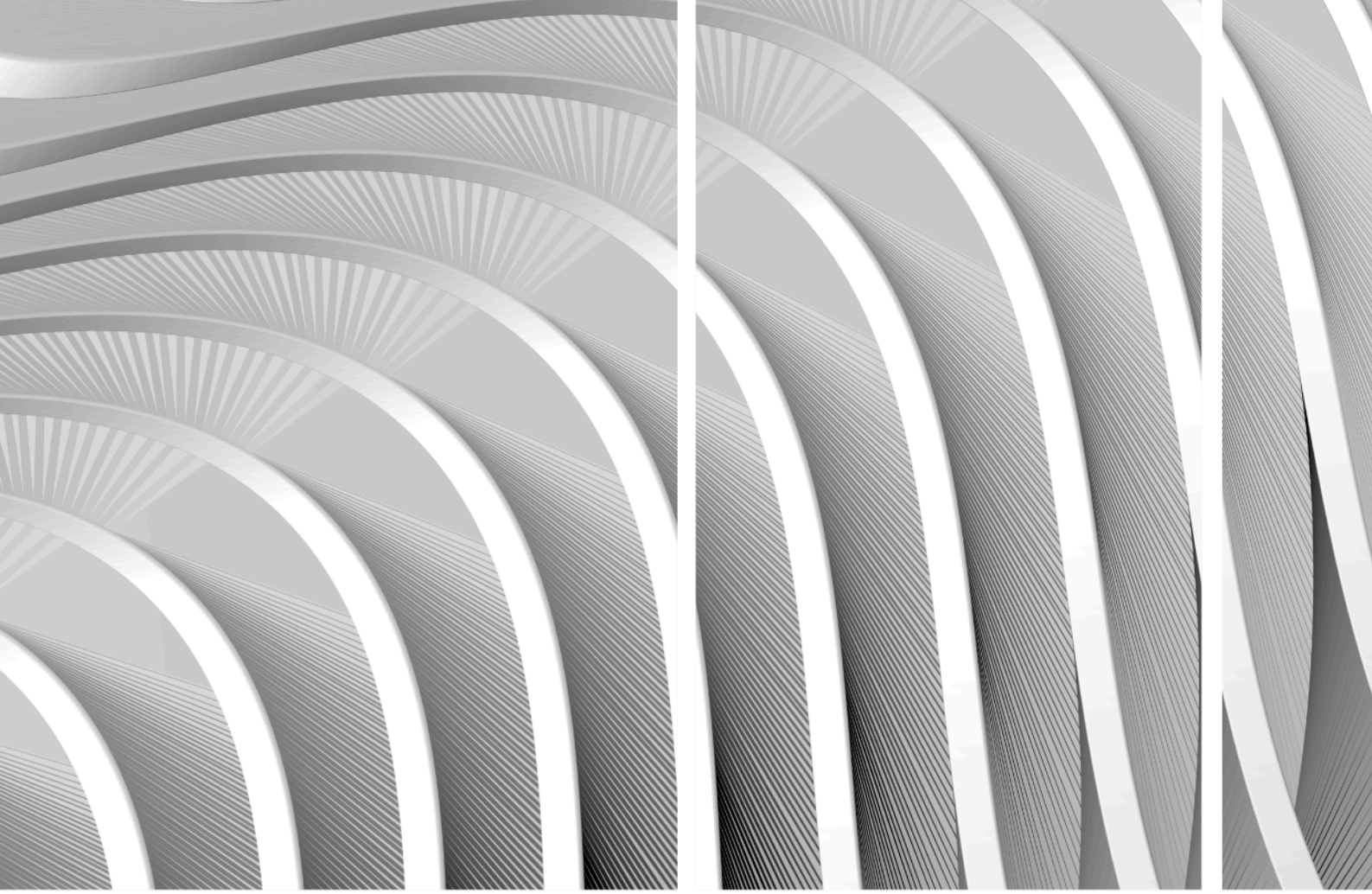


451 Research Vanguard Report

October 2025

Completing CNAPP with DSPM

Commissioned by

S&P Global
Market Intelligence

SentinelOne

Introduction

To say that cloud applications have transformed digital business is an understatement. Cloud applications represent a generational "step function" shift in how IT serves the enterprise. Capabilities such as ease of adoption and maintenance relative to enterprise-deployed physical infrastructure, as well as the scale and elasticity of provider-hosted solutions, have resulted in a substantial share of IT delivered via cloud applications. It is not lost on adversaries that those applications have also grown to handle a significant volume of sensitive data — data that becomes an attractive target for breach, ransom or compromise.

These realities make cloud applications a major security concern: Cloud security is the top-cited pain point by a wide margin in 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2025 study. This, in turn, has given rise to cloud-native application protection platforms (CNAPP), and it has made CNAPP a priority for security investment.

But CNAPP too often neglects a critical aspect of cloud capability: the high volume and sensitivity of cloud application data. Cloud applications are more than a primary focus of business-critical data. They create data, often as an organization's high-priority product; handle data, with significant implications for business viability; and maintain data, playing a critical role in the care of what is often among an organization's most durable and persistent assets.

These factors lead to an eye-opening conclusion for security teams evaluating CNAPP options: Data security posture management (DSPM) is an important aspect of cloud security, and it should be an equally important aspect of CNAPP. However, practitioners are likely to find in their CNAPP evaluation journey that data security often lacks the attention it deserves.

The Take

CNAPP has become a center of gravity for incorporating multiple aspects of cloud application security. From cloud security posture management (CSPM), CNAPP has broadened to include coverage such as cloud workload protection, cloud infrastructure entitlement management and, more recently, cloud threat detection and response.

But security for sensitive data is too often incidental to CNAPP offerings, if it's covered directly at all. Historically, CNAPP products have focused on mitigating exposures in cloud application infrastructure, software or configuration — unsurprising given that CNAPP's success arose from a focus on emerging opportunities in these realms. Data-specific security was often seen as the purview of other technologies in other domains.

But if sensitive, high-priority data handled in the cloud is a primary target of many adversaries, CNAPP cannot credibly position itself as the center of cloud application security if it neglects security for business-critical data. Indeed, any strategy for securing cloud applications that omits or minimizes the security of vital data assets is incomplete. On the other hand, a strategy that fails to consider the advantages of CNAPP for securing sensitive cloud application data neglects the distinctive opportunity presented by CNAPP's unique role in security architecture.

In this report, we explore how CNAPP augmented with DSPM capabilities offers a more comprehensive solution across all these demands. Cloud security may be a top concern, but security for sensitive data is close on its heels, making these the top two spending priorities reported in 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2025 survey. Consolidation of this investment helps organizations unify these priorities and break down silos in security technology. As AI adoption spurs explosive growth in the volume of sensitive data in cloud applications, DSPM is an aspect of CNAPP that can no longer be overlooked.

The CNAPP advantage

CNAPP is designed to increase efficiencies in securing cloud applications by uniting visibility and control across multiple dimensions. It helps manage configuration and mitigate exposure of cloud assets to security and privacy risks. It provides continuous asset monitoring and recommendations to remediate gaps. These capabilities help simplify risk management for cloud applications, making security more actionable and effective for practitioners.

Given the relationship between access and exposure, CNAPP may also incorporate visibility and control into identity and access management, often by integrating cloud identity and entitlement management. More recently, CNAPP offerings have incorporated threat detection and response for cloud applications, with recommendations for remediation that may extend to automated processes and controls to ensure more timely and consistent response.

The CNAPP data security gap

Despite their advantageous positioning, CNAPP offerings may still have coverage gaps, and ensuring data-specific security, privacy and compliance may be among the most evident.

Data security has distinctive requirements, and neglecting them in CNAPP may lead to coverage blind spots. For example, managing access to cloud applications is not necessarily the same as orchestrating access, privileges and activity specific to the creation, handling and disposition of data throughout its life cycle, which may extend across many people and technology resources throughout an enterprise. While CNAPP often includes functionality such as attack path analysis and an understanding of attacker mission targets, those capabilities may miss important adversarial objectives if they overlook cloud data's sensitivity and attractiveness as a target. The required context may not be part of CNAPP inputs if those are taken primarily from cloud infrastructure, software or configuration data.

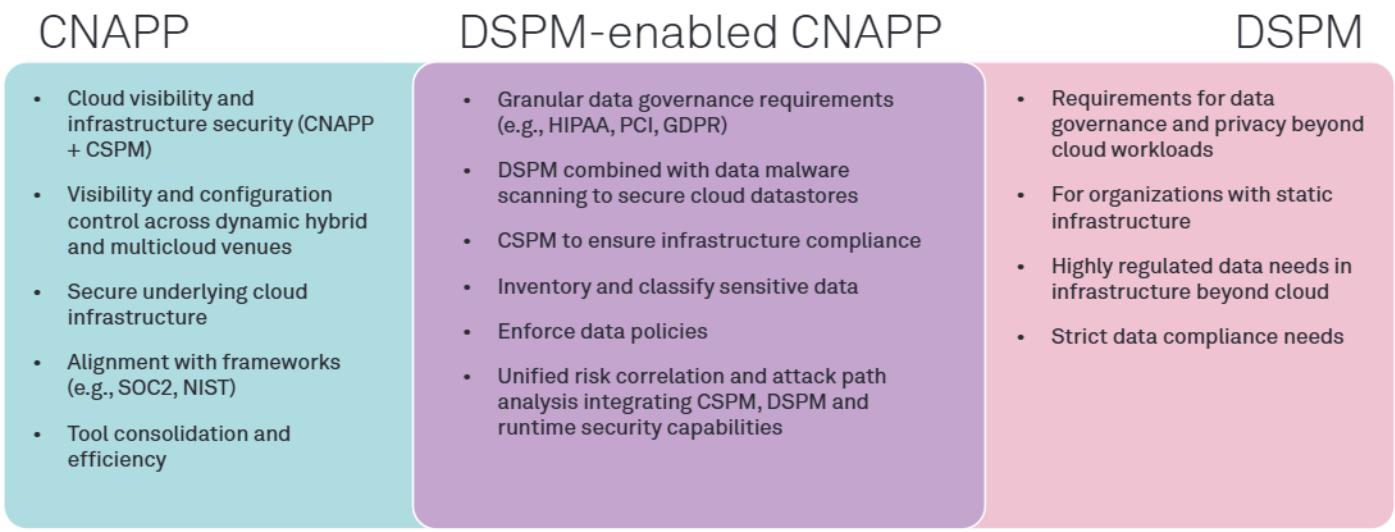
Incomplete fulfillment of compliance requirements may be a further issue. Many compliance mandates directly and prescriptively address data issues. This may result in unexpected liabilities if CNAPP tools fail to adequately and specifically address those mandated requirements. Data sovereignty is yet another issue that may require precise and ongoing documentation. Here, too, visibility and control must follow data throughout its life cycle.

The volume and sensitivity of data generated by AI workloads further compound the burden of addressing data security priorities. These workloads are often purpose-built to generate novel content based on proprietary inputs, which means cloud applications will handle added volumes of sensitive data. As with other aspects of data security, this data may be both product and asset, requiring careful handling to avoid exposing the organization to multiple aspects of loss and penalty. These are among the reasons why data access governance is the top-cited security area for which organizations have deployments in pilot, proof of concept or planned in the next 6-24 months, according to 451 Research's Voice of the Enterprise: Information Security, Technology Road Map 2025 study. By incorporating data security capabilities directly into CNAPP — combining security for AI-enabled cloud applications that generate and use sensitive data with controls to secure the data itself — organizations can get a handle on this ongoing data explosion.

Leveling up the CNAPP advantage: CNAPP + DSPM

A combined approach in CNAPP products that secure both cloud applications and data assets can collectively tackle many organizations' two highest cybersecurity priorities. If CNAPP is designed to secure cloud assets, augmenting CNAPP with DSPM helps organizations secure the "crown jewels" within those assets: their business-critical data.

Figure 1: Cloud application security must encompass data for a complete approach; DSPM-enabled CNAPP can provide a unified offering that streamlines common objectives



Source: S&P Global Market Intelligence 451 Research.

While CNAPP and CSPM functionality are often limited to cloud-specific assets, the data those assets handle is not. The classification of sensitive data tied to misconfigured datastores, for example, provides actionable context for cloud application security that CNAPP alone cannot. The combination of CNAPP plus DSPM can incorporate the full life cycle of data in cloud applications — from creation to handling, transmission and storage across networks and endpoints, on-premises and in the cloud. It is this very complexity of the data life cycle that gave rise to DSPM, and DSPM's capability to handle this complexity can augment CNAPP with the scope necessary for more complete cloud application security assurance.

Among the areas DSPM-enabled CNAPP can address:

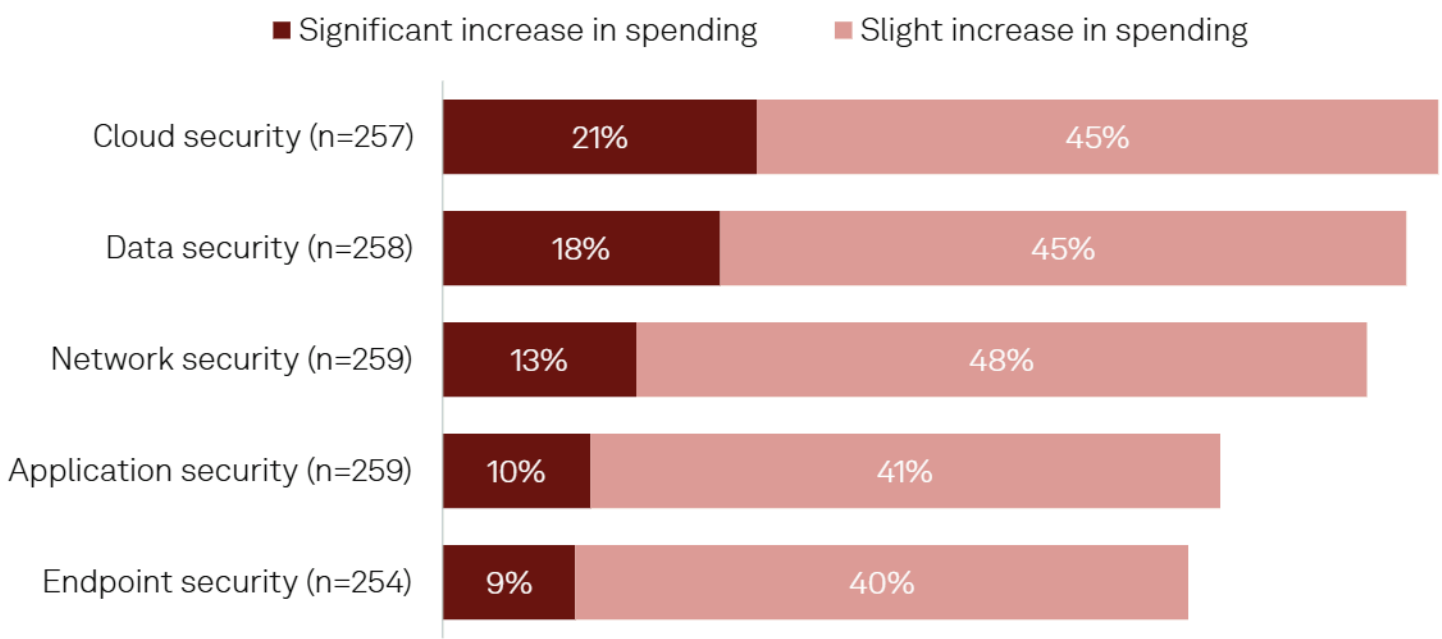
- **Regulatory and compliance priorities:** Compliance mandates that govern data security and privacy may require controls that go beyond cloud environments. They may have prescriptive requirements for data security and privacy, and may be specific to a geography or region. In some cases, DSPM may be used, for example, to honor a data subject access request (DSAR) as part of a privacy function, or to support overall privacy operations. This capability is not typically native to a CNAPP or CSPM tool. DSPM-enabled CNAPP, however, can support data classification within datastore inventory dashboards to accelerate audits, DSARs and risk reduction related to sensitive data.
- **Threat detection and response:** Threats to cloud assets often target data. It's no secret that data breaches are among the most damaging attacks. Cloud application protection must recognize this critical connection. CNAPP features such as attack path analysis are more effective when the platform understands where data resides and how it is accessed. Linking factors such as data exposure to infrastructure misconfigurations via CNAPP can simultaneously address business-critical cybersecurity priorities for both cloud applications and data. Furthermore, incident response may depend on awareness of how data security and privacy requirements affect response priorities. For example, the exposure of sensitive data assets uncovered in an incident investigation may have bearing on data security and privacy outcomes — such as required breach notification or privacy mandates, or incident reporting requirements for publicly traded companies — as well as significance for legally defensible forensic evidence.
- **Identity, access and entitlements:** Assessing and mitigating risk requires more than visibility into access policy and activity alone. Understanding the implications of this activity across both data and cloud assets is critical to risk assessment and control. While CNAPP or CSPM tools may incorporate aspects of these functions for cloud environments, DSPM often goes further, considering that data is often created on endpoints and transmitted via networks, accessed by users, and handled by applications that may reside both in and outside of cloud environments. This may require visibility into non-cloud identity and access management resources, as well as implementation of a broad range of data privacy and security controls beyond cloud applications alone.
- **Governance:** CNAPP focuses on the life cycle and requirements of cloud-specific assets, including the compute, networking, API and other resources that cloud applications depend on. CNAPP may have a comprehensive scope within the life cycle of cloud applications. However, data governance has a different — and in some ways, even more comprehensive — life cycle across content creation, access, sharing, modification, storage, management, disposition and disposal. For this purpose, effective security technology must span multiple venues beyond cloud alone, regardless of whether data is created, managed, used or stored in cloud applications.

Conclusion: A whole greater than the sum of its parts

A unified approach to DSPM-enabled CNAPP fulfills the vision of CNAPP as a comprehensive platform for securing cloud applications as well as the data they create and handle. Such an approach can simplify risk assessment and mitigation across both priorities, as well as the overall cost of tooling and the expertise required of practitioners. Each domain can be reinforced with the strengths of the other, as with threat detection and response that incorporates threat intelligence specific to both cloud and data security, privacy and integrity priorities.

A unified approach can also consolidate investment across the top identified categories of growth in technology investment.

Figure 2: Top five categories of expected year-over-year security spending increase in 2025



Q. For each of the following vendor-based security tools, how will your organization's spending change in 2025 — if at all — compared to 2024?
Base: All respondents.
Source: 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2025.

As new tools and tactics emerge, the platform approach supports their more efficient incorporation into a comprehensive strategy. With threats to identity and access controls, for example, the ability to deploy tactics such as deception within a threat detection and response system can significantly increase visibility into actual threats targeting an organization, facilitating mitigation across both cloud and data security priorities. As organizations increasingly harness AI to optimize security technology, the combination of cloud application and data security provides a unified center for AI application to optimize security across the scale and diversity of enterprise cloud resources and data assets. These may represent hundreds if not thousands of cloud application instances and related infrastructure, and an optimal opportunity for CNAPP plus DSPM to demonstrate the efficiencies that will be required to address emerging cloud application innovation.

SentinelOne (NYSE:S) is a global leader in AI-powered cybersecurity, enabling modern enterprises to protect, detect, and respond at machine speed. Singularity Cloud Security from SentinelOne is a unified, AI-powered CNAPP combining proactive exposure management with autonomous protection to block attacks at runtime. From real-time threat detection to intelligent automation, SentinelOne is redefining what's possible with AI in cybersecurity.

To learn more about SentinelOne and its AI-powered CNAPP: s1/ai/cnapp

About the author

Scott Crawford

Research Director, Information Security

Scott Crawford is research director of the Information Security channel at S&P Global Market Intelligence 451 Research, where he leads the industry analyst team covering innovation, disruption and strategic players in cybersecurity and cyber risk. Scott joined S&P Global through its 2019 acquisition of 451 Research, where he has led the Information Security channel since 2015.

In addition to directing the Information Security channel's research efforts, Scott covers forces and events shaping cybersecurity. He maintains a focus on areas including security operations, cyber risk management, the intersection of AI/machine learning and cybersecurity, and related interests.

About S&P Global Market Intelligence

At S&P Global Market Intelligence, we understand the importance of accurate, deep and insightful information. Our team of experts delivers unrivaled insights and leading data and technology solutions, partnering with customers to expand their perspective, operate with confidence, and make decisions with conviction.

S&P Global Market Intelligence is a division of S&P Global (NYSE: SPGI). S&P Global is the world's foremost provider of credit ratings, benchmarks, analytics and workflow solutions in the global capital, commodity and automotive markets. With every one of our offerings, we help many of the world's leading organizations navigate the economic landscape so they can plan for tomorrow, today. For more information, visit www.spglobal.com/marketintelligence.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia-Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html