IBM Enters the DSPM Space, Strengthening Cloud Data Security

Abstract

IBM has expanded its data security offerings by incorporating Guardium with data security posture management (DSPM) capabilities. DSPM addresses the critical challenge of safeguarding sensitive data within cloud and SaaS applications, making it an essential tool for modern organizations. This expansion of capabilities also addresses the challenge of "shadow data" – sensitive data that is not tracked or managed.

Background – The Shadow Data Challenge

The rapid adoption of cloud technology resulted in an exponential increase in cloud data for organizations. However, this growth also led to the challenge of managing and securing this data effectively. Much like how organizations previously struggled with "shadow IT," or unmanaged IT assets that organizations were unaware existed, they must now address the issue of "shadow data" in the cloud, or sensitive data that is not adequately tracked or managed.

IBM has incorporated innovative DSPM technology into its platform to tackle this problem. DSPM is an emerging cybersecurity segment that focuses on identifying where sensitive data is stored, who has access to it, and how it is used. DSPM uncovers vulnerabilities related to security posture, policies, configurations, and data usage. IBM's recent integration of DSPM capabilities aligns with the growing need for effective management and security of cloud and software as a service (SaaS) application data.

Key Ramifications

Guardium's integration with DSPM technology marks a pivotal moment in data security. There are many key ramifications of this integration.

- Comprehensive Data Security Platform: The integration of DSPM with IBM Security Guardium results in a robust data security platform that encompasses all data types and storage locations, including SaaS, on-premises, and public cloud infrastructure.

- Accurate Identification of Sensitive Data: The new integration's agentless platform swiftly and accurately identifies unknown and sensitive data, facilitating data classification and risk mitigation.

- Identifying and Mitigating Vulnerabilities: The solution identifies vulnerabilities, such as misconfigurations, overentitlements, and policy violations, and provides prioritized remediation reports. This empowers organizations to focus on critical security risks and compliance violations.

EMA Perspective

IBM has solidified its position as a leader in data security with the integration of DSPM capabilities into Guardium. By integrating DSPM technology, IBM offers a comprehensive solution that addresses the pressing challenges of cloud data security and shadow data. The integration aligns with IBM's commitment to empowering organizations with advanced cybersecurity capabilities and enabling them to navigate the complexities of the evolving digital landscape.

EMA believes that Guardium's integration of DSPM capabilities is a significant step toward ensuring the security of sensitive data in the evolving digital landscape. As organizations continue to embrace the cloud, having robust data security measures becomes increasingly crucial, and IBM's integration is a proactive step in that direction.