privacera

WHITEPAPER

Activating Data Security Posture Management

privacera

contents

Data Security Posture Management Thinking

In today's data-driven landscape, the urgency to pinpoint and safeguard sensitive information has surged, spurred by regulatory mandates. With the clock ticking on incident assessment, CIOs face the daunting task of navigating vast data repositories to determine materiality swiftly. A recent SEC ruling mandates organizations file an 8-K for material incidents. And they have four business days to determine whether a detected incident is material. At the same time, the SEC wants to see public organizations prove they are doing more to prevent material incidents - demand also becoming evident in requirements for cyber insurance.

Balancing these compliance demands with proactive risk mitigation efforts is now paramount for organizations striving to stay ahead in the ever-evolving realm of data security. The problem is the proliferation of data across cloud service platforms and geographic boundaries has made it a requirement to discover and locate disparate data repositories containing sensitive data at scale.

At the same time, the surge in data proliferation across diverse platforms demands automation to swiftly and precisely identify sensitive repositories. Amidst the four-day window for incident assessment, CIOs grapple with how to determine materiality while navigating through labyrinthine data landscapes. This includes demonstrating proactive measures to thwart data security risks, highlighting the urgent need for robust posture management strategies.

CIOs we have talked to are candid: determining materiality today requires a significant amount of time and effort forensically because they do not necessarily know what is stored where and whether it is potentially material. This makes it business critical to automate the finding where high volumes of sensitive information are stored. For this reason, these organizations have to file and share how they have mitigated a growing array of data security and privacy risks

Cloud Data Proliferation

The rise of cloud data repositories has reshaped the data landscape, heralding both the need for business innovation and improved security over aging datacenters. While migrating to cloud architectures often enhances security and agility, it also fosters the proliferation of uncharted data, leaving organizations vulnerable to unseen threats. This unknown data sprawl can create shadow infrastructures, evading detection and protection measures, posing a significant risk to data integrity and compliance efforts. This is problematic because at times these data repositories are not tied to business projects which are not discovered or necessarily protected.

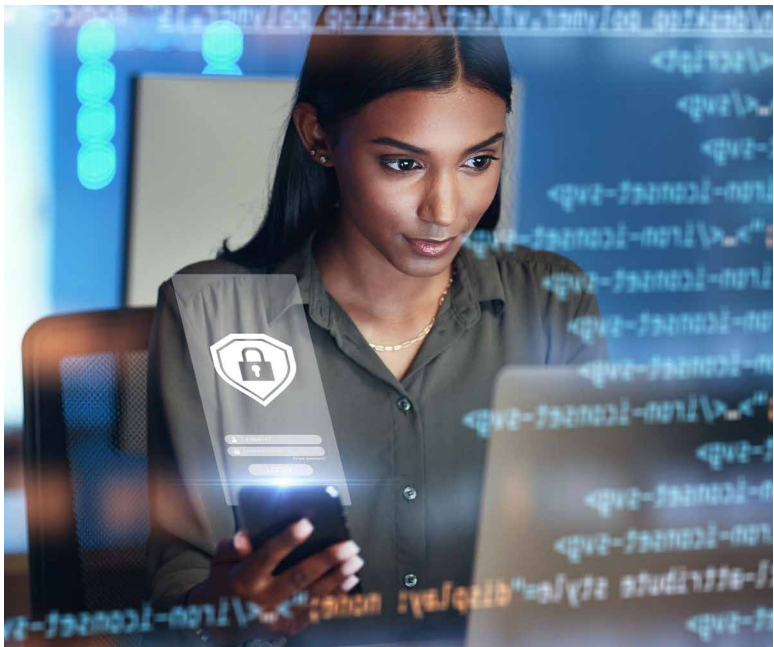
In the face of mounting data security incidents highlighted by reports like Verizon's, the imperative for solutions capable of unveiling and evaluating dormant data repositories becomes increasingly urgent, safeguarding against potential breaches and ensuring robust data governance in the cloud era. The Verizon's 2023 Data Breach Investigations Report which found that data breaches accounted for 5,199 and 16,312 security incidents.

While security teams can be tasked by business or compliance leaders with protecting specific data repositories and pipelines, some sensitive data locations can remain unidentified. This underlines the urgent need for technologies capable of unearthing hidden or dormant data repositories, assessing their exposure to risks concerning data residency, privacy, and security.

Why Data Security Posture Management?

In a landscape plagued by shadow data and inconsistent protection measures, the necessity of data security posture management becomes self-evident. Traditional security tools often fell short in uncovering undisclosed repositories, leaving organizations susceptible to diverse risks. Bridging these gaps requires a proactive approach to discover and evaluate data across cloud platforms, ensuring adherence to data residency, privacy, and security standards, and establishing a consistent and robust security posture.

Data security posture management empowers data and security leaders to navigate the labyrinth of data pipelines and geographic expanses, pinpointing security and privacy risks with precision. By leveraging this approach, organizations can systematically evaluate their data security stance across diverse cloud providers, beginning with the formulation of robust security policies that strike a delicate balance between business imperatives and risk mitigation strategies.



In the realm of data security posture management, constructing comprehensive data maps serves as a crucial function, unveiling the intricate web of repositories sprawled across various cloud service models. These maps delve deep into data flows and pipelines, unearthing shadow repositories and scrutinizing for misconfigurations that can jeopardize data integrity. By exposing potential vulnerabilities, they mitigate the risk of security breaches and privacy infringements, fortifying defenses against evolving threats lurking in the data landscape. Such exposure can lead directly to security or privacy incidents or expose pathways down which risks can evolve.

In tandem with data mapping, the role of Data Security Posture Management (DSPM) extends to pinpointing data risks with precision. By scrutinizing user access privileges and scrutinizing data pipelines, DSPMs facilitate comprehensive bottom-up and top-down risk assessments. These assessments gauge compliance with governance standards and regulatory obligations, while swiftly identifying potential security threats. Equipped with this insight, organizations can enact targeted remediation measures, bolstering their defenses and safeguarding against data breaches and regulatory non-compliance.

In the pursuit of compliance and data protection, DSPMs play a pivotal role in safeguarding the confidentiality of personal information while fostering informed decision-making through robust policies and standards. DSPMs should identify confidentiality of user/individual's personal information and protect it from unauthorized access, disclosure, and alternation. By promoting awareness of evolving threats and enabling continuous monitoring and auditing, DSPMs bolster security measures. They should make people aware of the existence and modus operandi of threats to data security. This encompasses logging for event correlation, creating security metrics, and generating insightful reports for management, empowering them to identify security gaps and trends, thus fortifying defenses against potential breaches and ensuring regulatory adherence.

Continuous monitoring and auditing form the backbone of effective data security posture management, facilitating the identification of malicious events and policy breaches through insightful log analysis.

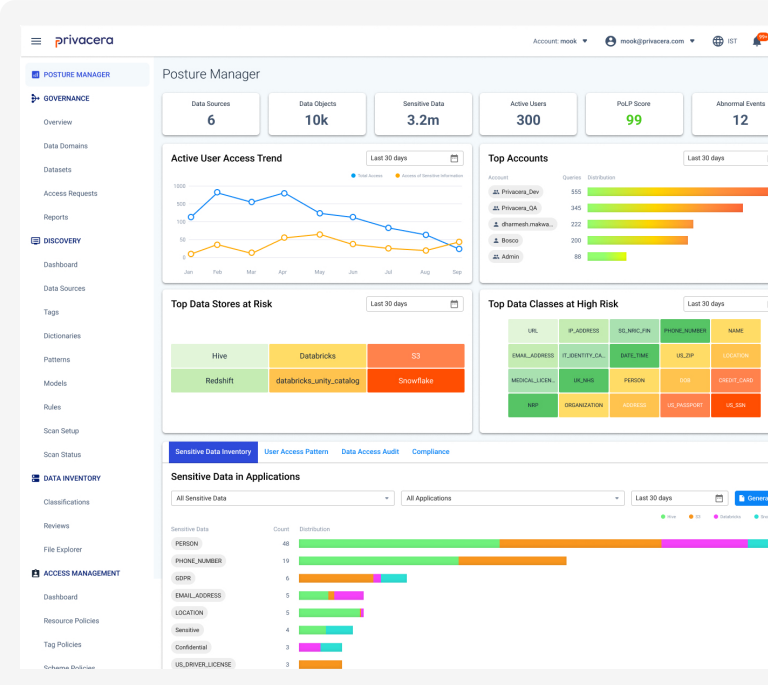
This proactive approach encompasses the creation of security metrics and comprehensive reporting, empowering management to discern security gaps and trends, thus enabling swift and informed decision-making to bolster organizational resilience against evolving threats.

Towards The Era Of Active Posture Management

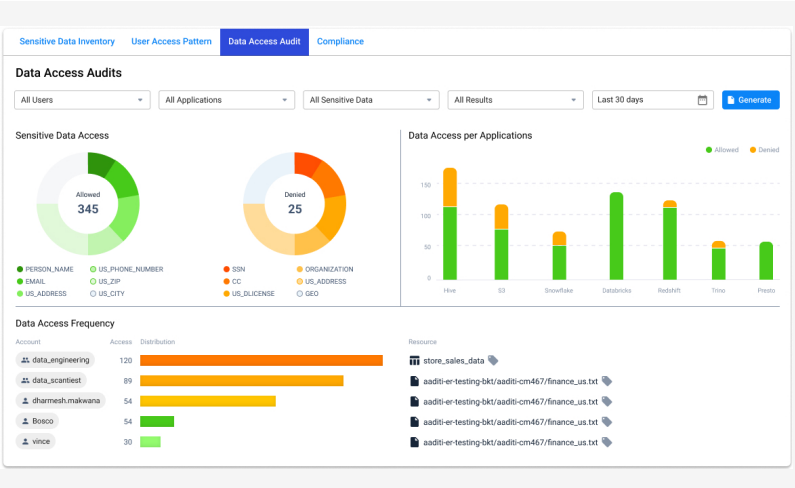
A challenge with existing data security posture management solutions in the market today is that it primarily focus on the scanning, discovery and visualization of sensitive data in your data estate to provide in essence your security posture. What is clearly needed as a next step is to mitigate the risks identified via some form of access control, encryption or masking to ensure we are actually improving our posture over time. Increasingly, as organizations mature they will need to orchestrate these capabilities together to provide a closed loop data security governance system that can Map the posture, Manage identified risks through active access controls, and the continuous Monitor to ensure there is no negative drift in your posture.

Introducing Privacera Posture Manager

With the introduction of Posture Manager, Privacera transforms data security posture management by offering both passive and active monitoring, providing organizations with a clear visualization of their sensitive data landscape, combined with our class leading data security platform to automate and simplify data security and access governance. Through advanced discovery and visualization techniques, Privacera unveils the intricate set of capabilities around sensitive data, access privileges, and usage patterns across hybrid data environments. By creating comprehensive sensitive data maps, it empowers organizations to pinpoint the location of structured and unstructured sensitive data, ensuring proactive protection and compliance measures are in place.

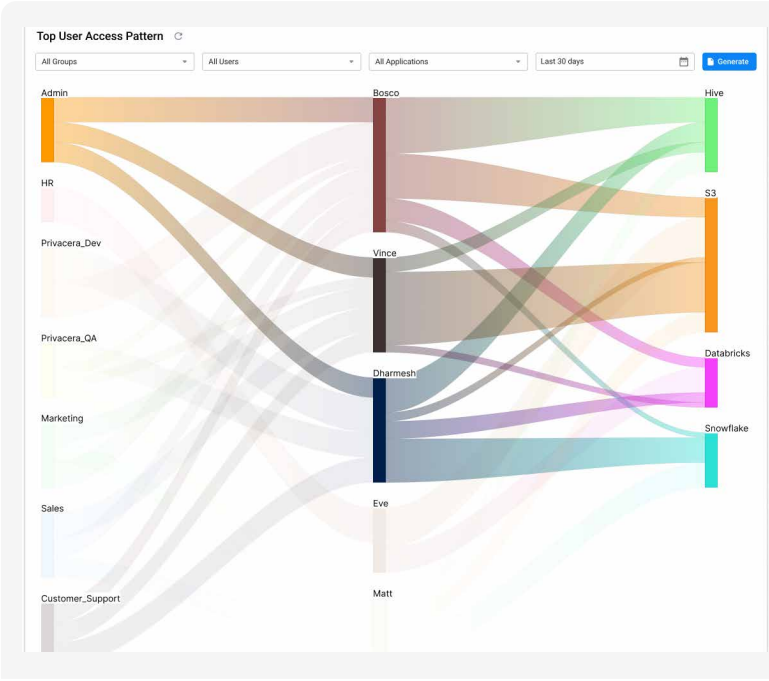


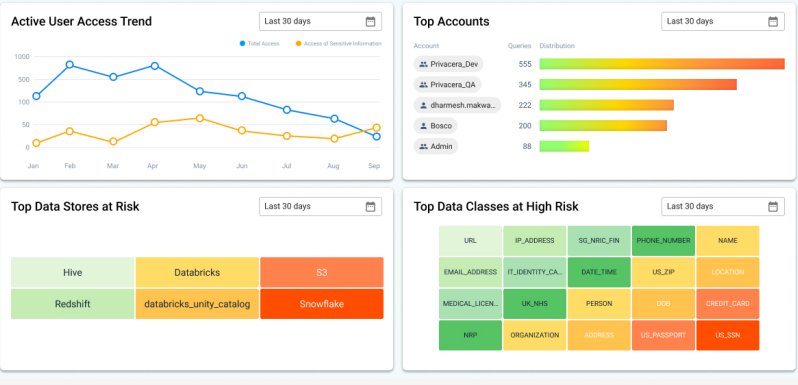
Privacera's data map offers a comprehensive view of structured and unstructured sensitive data, access privileges, and usage patterns, enabling organizations to evaluate associated business risks. Building on this foundation, Privacera facilitates risk impact assessments, identifying and rectifying inappropriate data usage through active posture management. By highlighting areas of overprovisioning and suggesting policy and control adjustments, Privacera empowers organizations to proactively enhance their data security posture and mitigate potential threats.



Privacera dives deep into user access patterns, identifying anomalies and flagging potential security risks through abnormal event metrics. By detecting unusual activities, Privacera equips business and data leaders with actionable insights to prioritize and address vulnerabilities swiftly. This proactive approach empowers organizations to fine-tune their individual posture and mitigate risk exposure effectively, ensuring robust data security measures are in place.

Privacera goes beyond by correlating access and usage patterns with access provisioning, then seamlessly integrates posture data with our existing access control and privacy solutions. Through Privacera's open integration framework, Privacera connects with security analytics platforms and SIEM solutions, providing organizations with a comprehensive view of their data security posture. By generating risk scores based on data source and category, Privacera's Posture Manager enables business and data leaders to understand their organization's posture and identify potential risk exposure, empowering informed decision-making and proactive risk mitigation strategies.



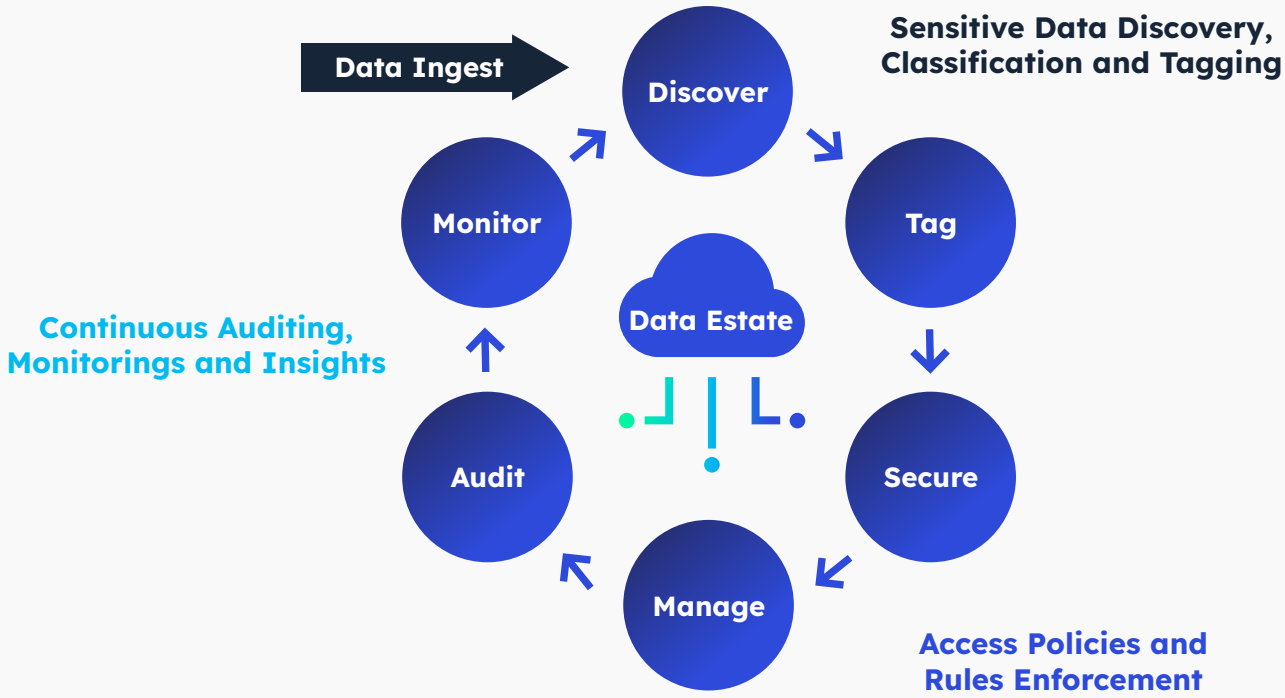


Privacera assesses user access against the principle of least privilege, measuring the alignment between access permissions and job requirements. By evaluating the extent to which users possess only the minimum access necessary for their roles, Privacera ensures that access grants are tailored to specific business functions. This meticulous approach enhances data security by minimizing the risk of unauthorized access and ensures that access

privileges are aligned with organizational roles and responsibilities.

Privacera delves into the organization's data landscape, meticulously mapping sensitive data locations across systems, databases, and applications. By pinpointing data exposure points, Privacera provides invaluable insights into potential areas of risk, empowering organizations to fortify their defenses and safeguard sensitive information effectively. This proactive approach ensures comprehensive data protection measures are in place, mitigating the risk of breaches and ensuring regulatory compliance.

Privacera completes the data security puzzle by meticulously tracking who accesses sensitive data and how, leveraging data access patterns and audit logs. Through active posture management, organizations also gain the ability to mitigate, secure, and monitor risks, ensuring a proactive approach to data protection. This integrated process empowers organizations to stay ahead of threats, fostering a culture of continuous improvement in data security posture.



By translating policies and sensitivity tags into actionable controls across discovered data lakes and datasets, we streamline data access management. With the exponential growth of data estates, maintaining consistency in control mechanisms becomes increasingly challenging. Active posture management not only simplifies this process but also aligns with the fundamental principle of IT efficiency: simplicity fosters effectiveness.

Transitioning from system-specific controls to a unified approach ensures transparency, consistency, and auditability, transforming organizations from a futile game of Whac-A-Mole. Piecemeal strategies drain engineering resources and hinder compliance efforts due to their inherent opacity and limited control. By centralizing security and access policies across analytics platforms, organizations can efficiently manage governance, enabling consistent security measures and enhancing overall security posture. Adopting an active, unified data security governance model drastically streamlines the administrative load and the ability to meet rigorous compliance mandates.

Privacera's active posture management extends to continuous monitoring and auditing, ensuring the seamless management of the entire data security process. By meticulously maintaining detailed audit logs of every data access event, Privacera captures crucial information on who accessed what data, when, and under what protections. This wealth of data isn't just for record-keeping; it's a powerful tool for integration with data security analytics platforms, enabling real-time alerts and monitoring to enhance data analysis capabilities. With Privacera, you're not just tracking data access; you're proactively safeguarding your data ecosystem, ensuring compliance, and unlocking faster, more powerful data insights.

Conclusions

In our exploration of data security posture management, we've traced its origins to the proliferation of data across diverse platforms, spurred by regulatory mandates and evolving cyber threats. We've clarified how data security posture management equips organizations with the tools to discover, assess, and mitigate risks across their data landscapes. Through both passive and active approaches, Privacera emerges as a key ally, offering comprehensive solutions to address the challenges inherent in data security posture management. Whether it's mapping sensitive data repositories, enforcing access controls, or facilitating continuous monitoring and auditing, Privacera empowers organizations to navigate the complexities of data security with confidence and resilience.

Fortune 500 enterprises trust Privacera for their universal data security, access control, and governance. Discover how to streamline data security governance with Privacera.

Take a unified approach to data access, privacy, and security with Privacera.

REQUEST A DEMO CONTACT US

Privacera, based in Fremont, CA, was founded in 2016 by the creators of Apache Ranger™ and Apache Atlas. Delivering trusted and timely access to data consumers, Privacera provides data privacy, security, and governance through its SaaS-based unified data security platform. Privacera's latest innovation, Privacera AI Governance (PAIG), is the industry's first AI data security governance solution. Privacera serves Fortune 500 clients across finance, insurance, life sciences, retail, media, consumer, and government entities. The company achieved AWS Data and Analytics Competency Status, and partners with and supports leading data sources, including AWS, Snowflake, Databricks, Azure and Google. Privacera is recognized as a leader in the 2023 GigaOm Radar for Data Governance; was named a 2022 CISO Choice Awards Finalist; and received the 2022 Digital Innovator Award. The company is also named a "Sample Vendor" for data security platforms in the Gartner® Hype Cycle™ for Data Security, 2023. Learn more at Privacera.com.

privacera