Solution Brief

CipherTrust Data Security Posture Management

Five Fundamental Questions to Ask and Answer

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

The emphasis on DSPM reflects a broader shift in data security from perimeter-based defenses to data-centric approaches. As data continues to proliferate and disperse across hybrid multi-cloud environments, dynamically managing data security postures becomes increasingly crucial for organizations aiming to protect sensitive information and maintain trust.

What is Data Security Posture Management?

Data Security Posture Management (DSPM) provides visibility as to where sensitive data is, who has access to that data, how it has been used, and what the security posture of the data stored or application is.

Source: https://www.gartner.com/reviews/market/data-security-posture-management

Data Security Posture Management (DSPM) refers to tools and practices that help organizations protect sensitive data across their infrastructure. DSPM solutions automate data discovery, classification, protection, and risk assessment, providing visibility into where sensitive data resides and who has access to it. These tools identify vulnerabilities, generate alerts, and offer remediation guidance to address data security risks. By integrating with other security systems and enabling compliance reporting, DSPM helps organizations maintain a strong data security posture and meet regulatory requirements.

According to Gartner, DSPM tools automate the discovery, classification, and risk analysis of unstructured and structured data across a wide range of data store types, including data stored on-premises, in the cloud, in multi-cloud environments, and in hybrid clouds. These tools help continuously identify the location of sensitive data, its accessibility, and existing protection measures. DSPM solutions often provide recommendations or automation capabilities to remediate identified risks, and they ensure governance and compliance by aligning data security strategies with regulatory requirements.

Importance of DSPM in Today's Data Environment

Data security has recently transformed significantly due to technological and social changes, highlighting the need for a holistic and comprehensive Data Security Posture Management (DSPM) strategy.

The emphasis on DSPM reflects a broader shift in data security **from perimeter-based defenses to data-centric approaches.** As data continues to proliferate and disperse across hybrid multi-cloud environments, dynamically managing data security postures becomes increasingly crucial for organizations aiming to protect sensitive information and maintain trust.

A comprehensive DSPM strategy must incorporate structured and unstructured data and consider data stored across cloud environments. As data storage becomes more diversified and complex, the need for robust DSPM solutions grows. These solutions support operational integrity and regulatory compliance and form the backbone of any modern cyber defense strategy, protecting sensitive information from the ever-evolving landscape of threats. Today, DSPM must address new and emerging risks to protect data effectively.

Lack of Data Security Lifecycle Visibility:
Understanding the location and interaction of structured and unstructured data is crucial in today's complex data environments. However, accurately identifying and classifying data has become challenging with data spread across clouds, data lakes, and on-premises systems. According to the "Cloud Security Alliance: Understanding Data Security Risk 2025" report, 80% of respondents lack confidence in identifying high-risk data sources. Adding to the difficulty, data can be easily moved and shared, undermining control over its location. When users share data without proper security measures, sensitive information may end up in unknown or external locations, increasing vulnerability to data exfiltration attacks.

Credential Sprawl:
The rapid expansion of cloud computing has led many organizations to store increasingly sensitive data online. This shift has exposed them to new vulnerabilities and complex configurations that traditional security measures cannot adequately address. The swift adoption of cloud services, containers, and DevOps has scattered keys and secrets across platforms, repositories, and codebases. This uncontrolled spread increases the attack surface, with numerous breaches linked to exposed or mismanaged credentials. The 2024 Verizon Data Breach Investigation Report shows that 80% of data breaches involved stolen credentials. Strong oversight and consistent security measures are vital for securing sensitive credentials and preventing unauthorized access.

AI-Driven Risk to Credential Security:
AI-generated attacks, such as phishing campaigns, are more convincing, scalable, and harder to detect, increasing credential compromise risks. While multi-factor authentication (MFA) is necessary, it's not enough. Adding behavioral monitoring—tracking unusual access times, login locations, and unexpected data downloads—provides the layered defense to counter sophisticated AI-driven threats. Sapios research and Deep Instinct report that 75% of security professionals surveyed said they had seen an uptick in attacks over the past year, 85% attributing the rise to bad actors using generative AI. This evolving landscape underscores the importance of deploying an effective DSPM strategy to safeguard organizational data across all environments.

Post-Quantum Cryptography Risk:
Recent developments, such as Microsoft's Majorana 1 chip, indicate that quantum computing may soon reach a level where it can break asymmetric algorithms like RSA and ECC. With quantum computers running algorithms like Shor's, these encryption methods could be compromised, exposing sensitive data. The 2025 Thales Data Threat Report shows "Harvest now, decrypt later" attacks (70%) are the leading interest in post-quantum computing where cybercriminals are collecting encrypted data today to decrypt when quantum computing becomes available. This highlights organizations' need to prepare now by adopting quantum-resistant algorithms and embracing crypto agility.

Proactively Detect Risks:
Insider threats, including leaks and sabotage, are becoming increasingly sophisticated and challenging to detect. The 2025 Thales Data Threat Report highlights that respondents are equally concerned about exposure caused by employees as they are about external unauthorized access. Effective risk management through robust monitoring is essential to prevent breaches, as traditional perimeter security is insufficient.

Data Governance:
Global data protection regulations impose severe penalties for non-compliance, highlighting the importance of recognizing behavioral changes to identify threats before they compromise sensitive data. Security strategies must evolve, incorporating methods like DSPM to tackle emerging vulnerabilities and attack vectors.

Answering the five fundamental questions of Data Security Posture Management

Where is my sensitive data?

Understanding the location of sensitive data is the first step in securing it. This includes identifying both structured data (such as that found in databases and spreadsheets) and unstructured data (like emails, documents, and multimedia files). These data types are often spread across various storage environments, including on-premises servers and multiple cloud platforms (like AWS, Azure, or Google Cloud).

Importance

- **Implement Appropriate Security Controls:** Specific types of data may require particular security measures based on regulatory demands or business needs.
- **Manage Data Proliferation:** As data volumes grow and spread across hybrid and multi-cloud environments, keeping track of where sensitive data is stored becomes more challenging and more critical.
- **Comply with Regulations:** Compliance with data protection laws (GDPR, CCPA, HIPAA, etc.) often requires detailed knowledge of where specific types of data are stored.

Many organizations don't know where their sensitive data is or if it's dangerously exposed. Such blind spots create security risks that can lead to careless mistakes or create opportunities that attackers can exploit, often through hidden vulnerabilities or misconfigured databases you may not even know exist.

Enterprises today often employ a variety of storage solutions, such as on-premises servers, multiple cloud environments (both public and private), and SaaS platforms. This variety disperses sensitive data across many locations, complicating comprehensive tracking and management.

Modern organizations generate and process vast amounts of data at a rapid pace, encompassing both structured data (such as databases) and unstructured data (such as emails and documents). Continuously monitoring the real-time location of all this data presents significant challenges.

Additionally, data within an organization is dynamic; it is regularly moved, processed, and accessed by various applications and users. This constant movement complicates efforts to determine the precise location of data at any specific time without advanced monitoring tools.

It is critical to leverage data discovery and classification to automatically discover all data stores in your data estate – from structured to unstructured – across on-premises, cloud, multi-cloud, and hybrid environments. Automated discovery and classification are the only way to routinely and consistently discover and classify new or modified data stores.

Who has access to my sensitive data?

Controlling and monitoring who has access to sensitive data is essential for preventing unauthorized use and potential data breaches. This includes managing permissions for both internal employees and external partners.

Importance

- **Prevents Data Breaches:** By limiting access to sensitive data to only those who need it for their work, organizations can reduce the risk of insider threats and external attacks.
- **Supports Compliance:** Many regulatory frameworks require strict controls on data access. Knowing who has access helps in maintaining compliance with these regulations.
- **Enhances Data Management:** Monitoring who accesses data can help in auditing and tracking usage patterns, which can be vital for security and operational efficiency.

Many organizations struggle with limited visibility and oversight of data access due to a lack of comprehensive tools. Without effective means to aggregate and analyze access data across various systems and platforms, it becomes challenging to determine who currently has access to sensitive data.

Modern enterprises typically employ complex and layered access structures, including role-based access control (RBAC), attribute-based access control (ABAC), and other models. These intricate systems make it difficult to precisely understand who has access to what data and under which conditions. Additionally, in large organizations, different departments or divisions often manage their own IT resources independently, leading to inconsistent access controls and policies. This decentralization complicates the ability to track data access throughout the organization, further obscuring the visibility of who can access sensitive information.

Scanning your data store locations for granted user rights and displaying various details regarding user rights is critical to understanding your data posture by mapping users and privileges to database objects across all databases.

How well are credentials protected?

Having safeguards over the metadata and credentials, such as encryption keys and secrets, that have the ability to unlock encrypted data to make it readable and usable is critical. This includes using cryptography that supports protecting data today and tomorrow where quantum computing will accelerate malicious de-encryption techniques.

Importance

- **Protect Associated Metadata:** Centrally managing keys and secrets away from encrypted data adds an additional layer of security to protect sensitive data.
- **Prepare for the Post-Quantum Reality:** Deploying crypto agile products allows the use of post-quantum computing (PQC) algorithms and keys today.
- **Halt Credential Sprawl:** Securing credentials and stopping the uncontrolled spread of keys and secrets is critical to reducing the attack surface and preventing unauthorized data access.

Many organizations leverage encryption as a fundamental tool for protecting data, but they often overlook the need to protect the keys and secrets that make encrypted data readable and usable. Like leaving the key to a house under the doormat, storing encryption keys and secrets close to the encrypted data makes them vulnerable.

Organizations often leverage multiple cloud providers to house data, meaning that the key creation, management, and rotation processes vary across CSPs. As organizations deploy an ever-increasing number of encryption solutions, they find themselves managing inconsistent policies and different levels of protection and experience escalating costs. The best way through this maze is often to transition into a centralized encryption key management system.

Centralizing key and secrets management for key generation, storage, rotation, backup, recovery, revocation, and termination effectively delivers separation of duties, ensuring the same person creating and managing the keys cannot access the protected data and reducing risk by dividing related responsibilities for critical tasks.

How has my sensitive data been used?

Tracking how data is accessed and used over time is vital for security and compliance. This includes understanding the context of data access and modifications, and detecting unusual patterns that could indicate a security threat.

Importance

- **Detect Anomalies:** Unusual access patterns or unexpected data modifications can be early indicators of a data breach.
- **Audit and Forensic Analysis:** Comprehensive logs of data usage are crucial for audits and can be invaluable during forensic investigations after a security incident.
- **Optimize Data Access Controls:** By understanding how data is used, organizations can refine access controls to better match actual business needs and security requirements.

Effective data usage tracking requires advanced monitoring and logging tools that provide detailed and accurate records of all data interactions. Many enterprises lack these tools or do not have them fully integrated across all systems, leading to gaps in data usage visibility.

Enterprises today operate in highly complex data environments that span on-premises systems, multiple cloud platforms, and a variety of end-user devices. Each of these environments can process and store data differently, making it hard to track exactly how data is accessed and used across the entire organization.

Various regulations require detailed logging of data access and usage (e.g., GDPR, HIPAA). Complying with these regulations across different jurisdictions adds another layer of difficulty to tracking how sensitive data is utilized.

Robust compliance and security are essential for data protection, ensuring visibility into usage, vulnerabilities, and access rights. As the digital economy drives exponential data growth, organizations require data-centric compliance and security solutions to reduce risks of non-compliance and breaches. Automating workflows and providing recommended actions streamline processes, helping security teams identify data risks before they escalate.

What is the security posture (i.e. current state of data security) of our data stores?

Assessing the security posture of data stores involves evaluating the effectiveness of implemented security measures, identifying vulnerabilities, and understanding the impact of potential threats.

Importance

- **Strengthen Defenses:** Identifying vulnerabilities and gaps in data security enables proactive improvements and helps prevent breaches.
- **Manage Security Resources Effectively:** By knowing where security is weakest, organizations can allocate resources more effectively to where they are most needed.
- **Ensure Resilience:** Regular assessments of the security posture ensure that defenses keep pace with evolving threats and changing business practices.

Effective posture management requires the latest regularly updated vulnerability definitions that are leveraged through scans to assess resources, search for vulnerabilities and determine risk. By scanning databases with predefined vulnerability tests based on CIS and DISA STIG benchmarks keeps organizations aware of databases susceptible to the latest threats. These scans, using CVSS, present risk by the vulnerabilities discovered in your network and data and assign a risk score. CVSS is "an open framework for communicating the characteristics and impact of IT vulnerabilities." It is maintained by the National Institute of Standards and Technology as part of the Security Content Automation Protocol (SCAP) framework. Scoring vulnerabilities using CVSS provides an accurate model for measuring the risk inherent in discovered vulnerabilities and prioritizing them for mitigation.

Monitoring is a key phase in the data management lifecycle that delivers real-time information that includes system events, alerts, violations, blocked sources, gateway and agent status, system warnings, database auditing information, file server auditing information, archiving information, and more.

Monitoring events, alerts, and violations can take on many aspects. Depending on your specific implementation, there may be several types of users with varying roles and associated security policies. You can use the pre-configured severity ratings or customize your policies to fine-tune how events are interpreted to determine if an alert is a false positive, an attack, or something else.

A Single Platform that Goes Beyond Risk to Keep Your Data Safe

Data is your most valuable resource and drives economies of scale. With the adoption of modern innovations like AI, organizations will generate more data than ever before. This exponential growth of data and data repositories equates to more data blind spots and more vulnerabilities that leave data exposed. In order to protect data while also leveraging its vast potential, it is mission critical to effectively identify sensitive data and fortify its security, governance, and compliance.

Understand your data estate

CipherTrust DSPM automates the discovery and classification of both structured and unstructured data across a wide range of data stores, including on-premises, cloud, multicloud, and hybrid-cloud environments.

- **Scanning and Identifying Data:** CipherTrust DSPM systematically scans data environments—whether on-premises or in the cloud—to discover data repositories. This includes databases, big data platforms, cloud storage, and file systems.
- **Classifying Data:** Following discovery, CipherTrust DSPM classifies the data based on its type and sensitivity. This automated classification helps organizations understand the data they hold and prioritize their security accordingly.
- **Understand User Access:** CipherTrust DSPM provides user rights management, monitoring data access, and activities of privileged users to identify excessive, inappropriate, or unused privileges. It also provides security and IT teams full visibility into how data is accessed, used, and moved around the organization.

Fortify your data security posture

A comprehensive data protection strategy is crucial for Data Security Posture Management (DSPM), yet it is often neglected. Establishing a solid foundation for data protection through encryption and effective credential management is vital for maintaining a robust data security posture. CipherTrust DSPM identifies sensitive data and protects it using industry-leading technologies. It ensures the security of credentials and metadata, thwarting unauthorized access by users and applications and reinforcing your organization's overall data security and compliance framework.

- **Protect Sensitive Data:** Implementing key data protection like encryption, data masking, and tokenization ensures that sensitive data is only usable by authorized applications and personnel while protecting sensitive information like credit card information, intellectual property, or personal identification information (PII).
- **Secure the Metadata that Unlocks Your Encrypted Data:** Encryption and data masking are the first steps in protecting data. However, it is equally critical to secure the keys and secrets that unlock the protected data, leveraging centralized key management. To effectively do this, keys and secrets should be detected and inventoried across the hybrid cloud environment.
- **Be prepared for the post-quantum reality:** Quantum computers present a significant cybersecurity threat due to their ability to break commonly used encryption methods. This could lead to data breaches, compromised communications, and vulnerabilities in blockchain and authentication protocols. Organizations need to transition to quantum-resistant cryptography and adopt proactive security measures to mitigate this threat.
- **Halt Credential Sprawl:** Encryption, Tokenization, and Data Masking safeguard credentials so as not to be shared past authorized audiences. These techniques maintain that data is unreadable or unusable, preventing the creation of rogue data stores that contain sensitive data.

When you establish a robust data protection foundation, CipherTrust DSPM empowers organizations to conduct proactive risk analysis, effectively identifying and prioritizing risks linked to their managed data. This intelligent risk analysis delivers critical insights that enable organizations to pinpoint where vulnerabilities lie swiftly. With this knowledge, they can implement strategic plans to mitigate these risks, significantly enhancing their data security posture and ensuring the safety of their most valuable asset - their data.

- **Assess Risks:** By evaluating how data is stored, accessed, and shared, CipherTrust DSPM can identify vulnerabilities, risky configurations, and improper access controls that could lead to data breaches. CipherTrust DSPM offers a centralized view of data security risk across all environments, allowing organizations to see where sensitive data is located, the level of protection, and how it is protected, as well as identify key or secret misuse that indicates insider threats.

- **Identify Behavioral Changes:** Changes in user and entity behavior are a key indicator of risk and potential environmental threats. With the emergence of AI-powered threats, behavioral analytics has proven to be a valuable tool when subtle changes occur that can identify modern phishing tactics or other low and slow attacks.
- **Identify risks caused by artificial intelligence:** With the increasing use of artificial intelligence to empower employees, organizations must contend with a new generation of risks. It is crucial to be able to identify shadow AI services, prevent sensitive data leakage caused by AI, and detect and respond to abnormal AI behavior.
- **Understand Incident Relationships:** Utilize AI analytics to merge user behavior with application and data context to understand external and insider threats and combat "low and slow" attacks.
- **Prioritize Areas of Focus:** With customizable risk scores, organizations can go beyond merely identifying risks; they can determine what areas require the most attention based on severity and impact. This allows them to efficiently invest in areas that will have the most success in improving their security posture.

Continuously improve data security operations

Once risks are identified, it is critical to act quickly and effectively to remediate those risks. CipherTrust DSPM not only identifies risks but also offers recommendations on how to mitigate them. Through playbooks, organizations can establish automated actions that will take action on behalf of data security, whether it is to quarantine users showing risky behavior or to open a threat ticket to be investigated.

- **Suggest Security Enhancements:** Based on the risk assessments, CipherTrust DSPM offers actionable insights and recommendations to tighten security controls where they are most needed.
- **Automate Security Policies:** CipherTrust DSPM can automate enforcing security policies across different platforms, reducing the manual effort required to secure data assets.
- **Escalate Incident Prioritization:** CipherTrust DSPM facilitates efficient incident management and problem resolution by enabling quick identification of affected systems and the severity of the policy violation.

Data governance and compliance initiatives establish policies and processes to ensure organizational data's quality, security, and availability throughout its lifecycle. CipherTrust DSPM helps organizations align their data security strategies with governance and compliance by offering visibility into data access, usage, and transfer.

- **Support Compliance Initiatives:** Meet compliance regulations such as GDPR, HIPAA, CCPA, and others by ensuring that sensitive data is adequately protected and access controls are correctly implemented. To meet emerging compliance requirements, organizations must be able to audit usage keys and secrets.
- **Generate Reports:** CipherTrust DSPM provides detailed reports that can be used to demonstrate compliance to auditors and other stakeholders.

DSPM solutions are crucial for organizations aiming to secure sensitive data comprehensively. These solutions answer the Five fundamental questions that underpin effective data security strategies.

CipherTrust DSPM: Integrating Key Technologies Essential for DSPM

Data Discovery
CipherTrust DSPM excels in discovering sensitive data across diverse environments from on-premises to the cloud, automating the identification and mapping of critical information. This facilitates enhanced compliance management and breach protection.

Data Classification
With CipherTrust DSPM, data is meticulously classified according to its sensitivity and regulatory needs, enabling precise application of security measures and prioritization of data protection.

Data Encryption, Masking and Tokenization
CipherTrust DSPM allows you to secure, anonymize, and encrypt data at rest and in motion across the IT ecosystem and ensure the keys to that data are protected and only under your control.

Static Risk Analysis
The system's static risk analysis preemptively identifies vulnerabilities within the data infrastructure, allowing organizations to address potential threats before they are exploited.

Assess and Exposure Risks Identification
CipherTrust DSPM continuously monitors data access points and exposure levels to swiftly detect and mitigate unauthorized access or data leaks, safeguarding the integrity of sensitive information.

Alerts on High-Risk Vulnerabilities
Real-time alert system warns of severe vulnerabilities, prioritizing issues based on their potential impact to enable quick and effective organizational responses.

Risk Reporting and Assessment
This capability provides in-depth risk assessments and customizable reporting, aiding organizations in understanding their security posture and identifying vulnerabilities for proactive mitigation.

Remediation Guidance
CipherTrust DSPM advises on corrective measures for identified security vulnerabilities, offering practical, actionable guidance that aligns with best practices and industry standards.

Enterprise Readiness
Designed with scalable architecture, CipherTrust DSPM integrates smoothly with existing enterprise systems, supporting complex data environments and adapting to evolving organizational needs.

Integration with Security and Orchestration Services
Improve security operations by integrating CipherTrust DSPM with security and orchestration services, facilitating synchronized management of various security tools and enhancing operational efficiency.

Playbook Automation
CipherTrust DSPM utilizes playbook automation to provide standardized responses to common security incidents, streaming threat management and minimizing response times and damage.

Compliance Auditing and Reporting
CipherTrust DSPM supports compliance and auditing processes with detailed reports that document all aspects of data security management, from access logs to risk assessments.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

cpl.thalesgroup.com

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us