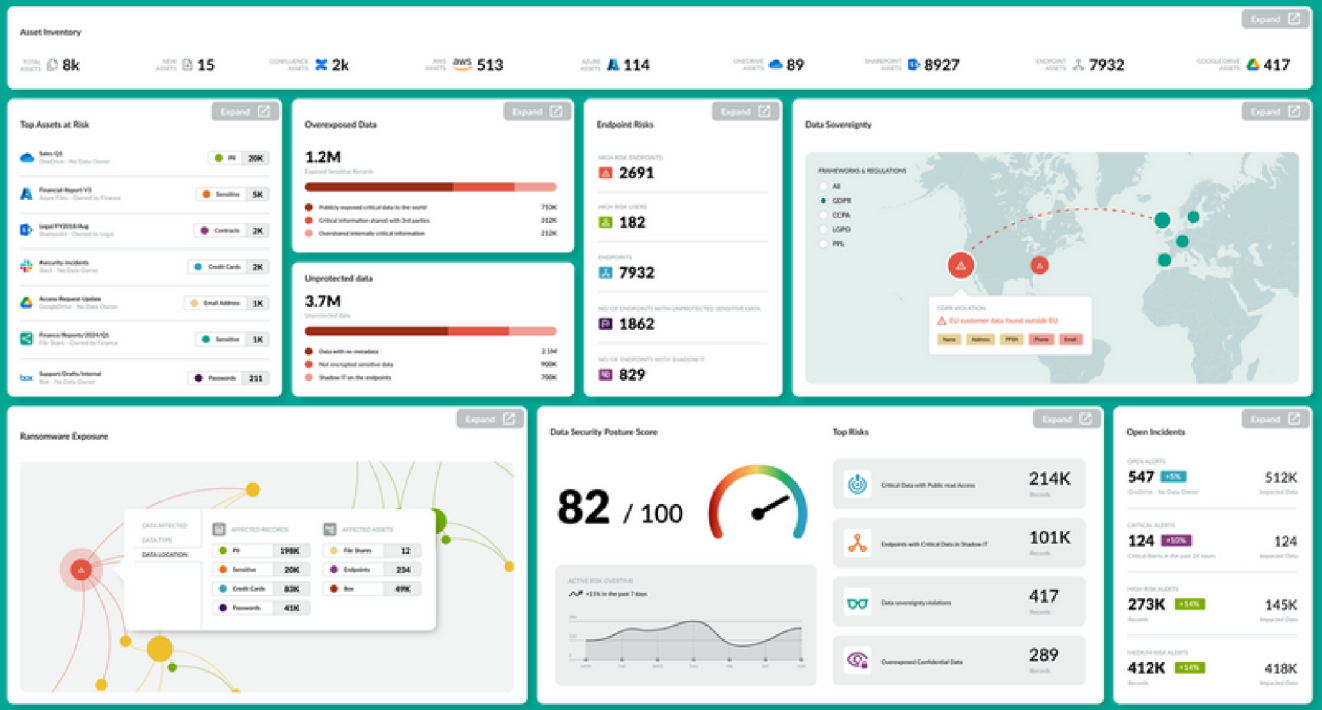


Protecting Your Data Landscape: How Forcepoint DSPM + and DDR Safeguard Sensitive Information

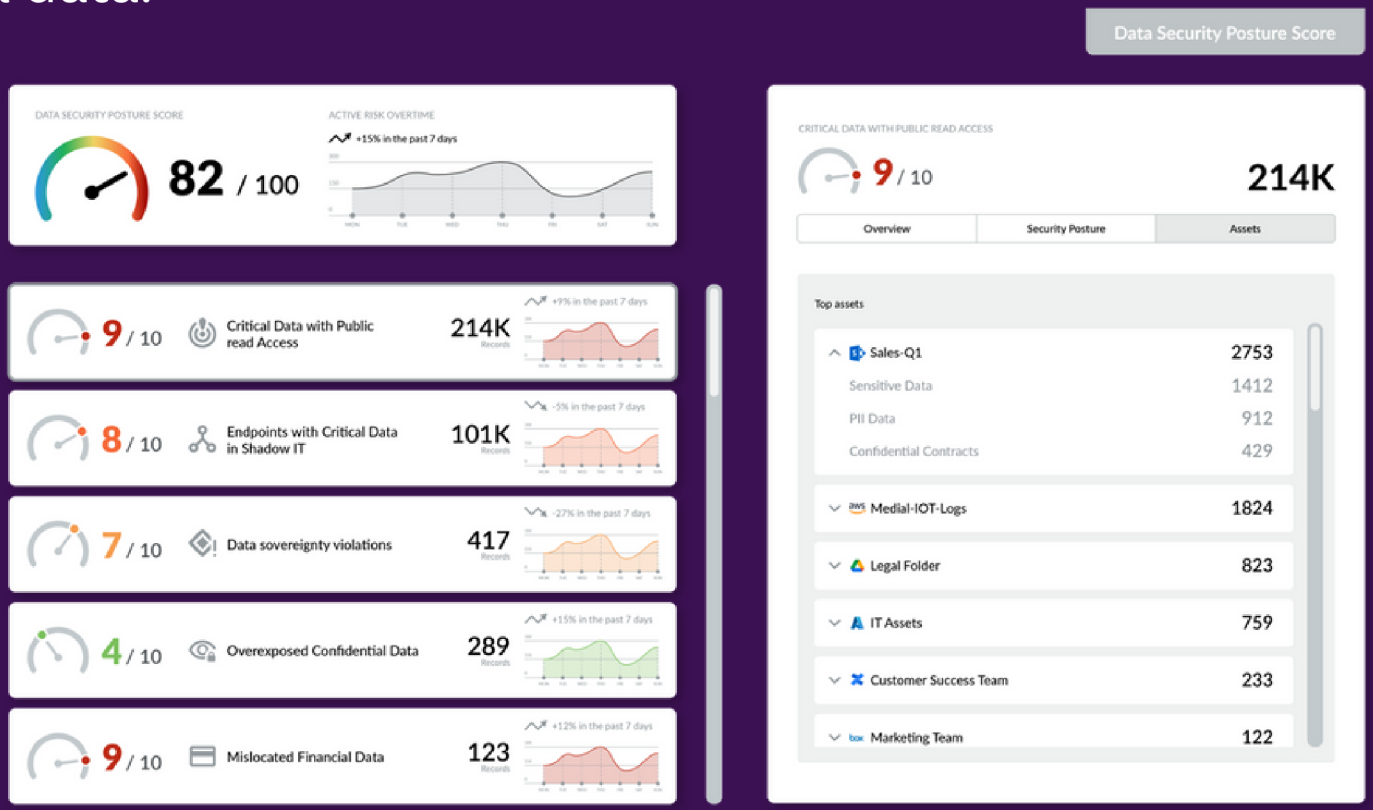
Introduction:

In the rapidly evolving landscape of data security safeguarding sensitive information has become an increasingly intricate and an urgent imperative. It is within this context that Forcepoint Data Security Posture Management (DSPM +) and Data Detection and Response (DDR) emerge as indispensable in the ongoing battle to protect against data breaches and mitigate the risks of data exfiltration. This paper delves into **Forcepoint DSPM** + and DDR, covering how their combined capabilities synergize to create a fortified data landscape capable of withstanding the multifaceted challenges posed by today's digital ecosystem.



Understanding Forcepoint (DSPM+)

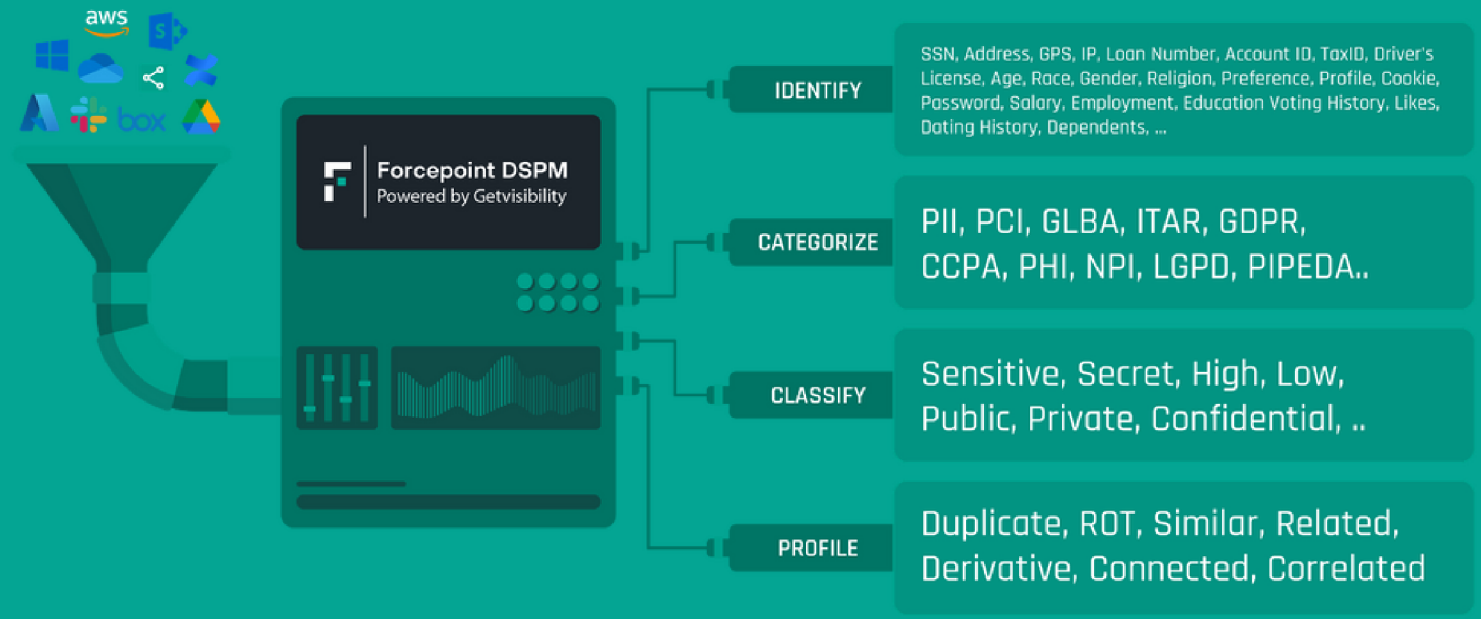
Forcepoint DSPM+ is a comprehensive platform that enables organisations to assess, monitor, and mitigate risks associated with data residing in multi-cloud environments, on premise and at the end-point. Its core focus is safeguarding sensitive information by examining data context and content, prioritizing the most important information including personally identifiable information (PII), medical records, and other critical data.



How Does Forcepoint DSPM+ Work?

1. Shining a Light: Data discovery in the cloud and across the network

Forcepoint DSPM+ provides unparalleled visibility into your cloud and network data inventory. The AI powered platform can pinpoint the location of sensitive data across various services like IaaS, PaaS, and DBaaS deployments, encompassing managed cloud warehouses, unmanaged databases, and object storage. This empowers organizations to identify potential risks associated with unstructured data storage and human error.



2. Prioritizing risks through AI powered classification

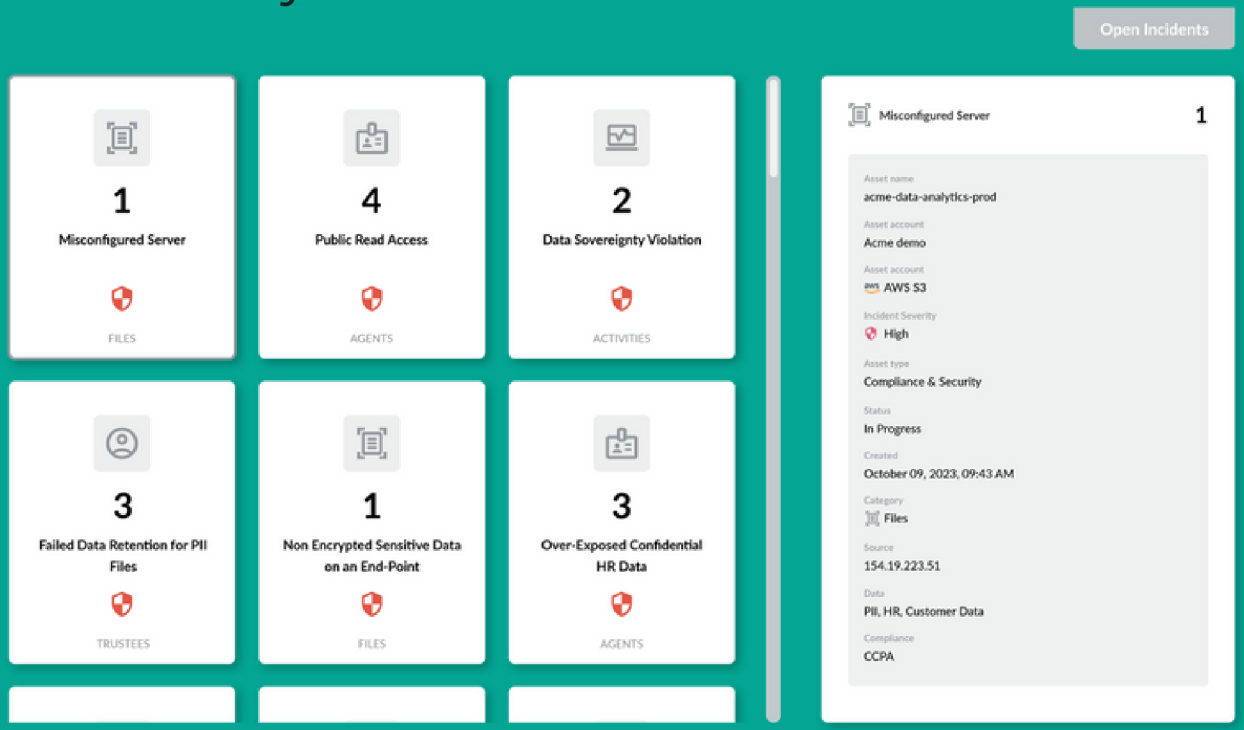
Not all sensitive data is created equal. Forcepoint DSPM+ automatically classifies each dataset based on its sensitivity level. This allows security teams to prioritize policy enforcement and incident response efforts on the most critical assets. Imagine a dataset containing customer PII taking precedence over anonymized user data – this prioritization is what effective classification enables.



3. Continuous Monitoring for Enhanced Security

Once Forcepoint DSPM+ discovers and classifies sensitive data the platform enables hardening of the overall security posture by analyzing access controls and security configurations associated with data storage.

This continuous monitoring helps identify misconfigurations, improper access controls, and vulnerabilities that could lead to data breaches. By addressing these issues promptly, organizations significantly reduce the likelihood of security incidents.



The Business Case for Forcepoint DSPM +

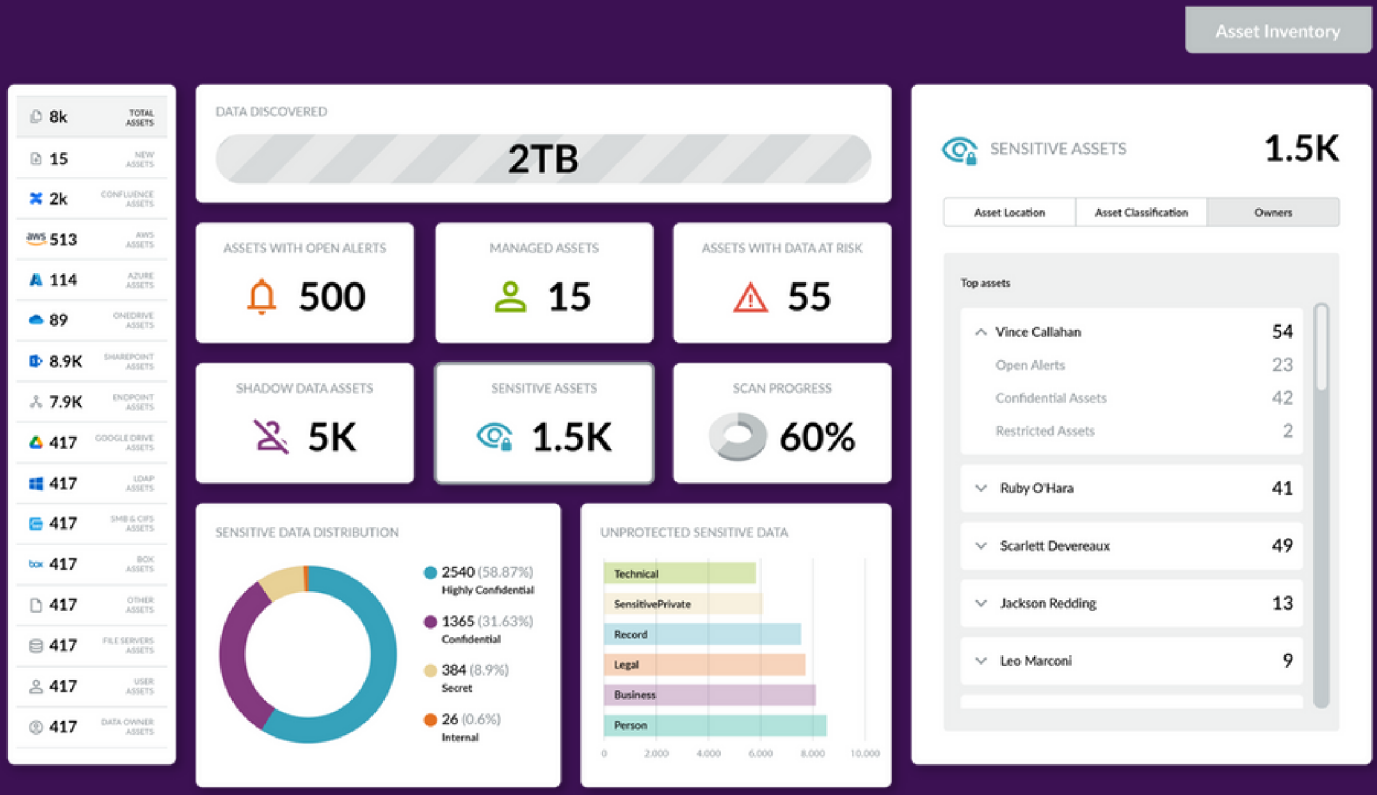
Data breaches can be devastating, leading to reputational damage, financial losses, and regulatory fines. Here's why prioritizing data security with DSPM is essential:

- **Reduced Risk of Data Breaches:** The primary objective of Forcepoint DSPM+ is to prevent data breaches and minimize data exposure if a breach occurs.

- **Enhanced Regulatory Compliance:** Forcepoint DSPM+ assists with adhering to data privacy regulations like GDPR and CCPA, and healthcare data legislation like HIPAA.

- **Mergers and Acquisitions Data:** During mergers and acquisitions, a clear picture of data assets is crucial. Unsecured data can pose significant risks and impact deal valuations.

- **Cost Optimization:** Improved data security posture translates to cost savings. This includes reduced insurance premiums and streamlined security processes through workflow automation.



Forcepoint DSPM+ vs. Other Cloud Security Tools

While Forcepoint DSPM+ offers distinct advantages, it's important to understand how it complements other cloud security solutions:

- **Data Loss Prevention (DLP):** DLP solutions focus on preventing data exfiltration from endpoints. Forcepoint DSPM+ with DDR capabilities acts as a cloud-based DLP, working in tandem with Forcepoint award winning DLP

- **Cloud Access Security Brokers (CASBs):** CASBs enforce security policies between users and SaaS applications. They don't cover data storage on IaaS, PaaS, or DBaaS, which is DSPM's domain.

- **Native Cloud Security Solutions:** While cloud providers offer native security solutions, they often have limitations, supporting only one cloud environment or service type. Forcepoint DSPM+ provides holistic coverage across multi-cloud environments.

The Power of Proactive Detection: Data Detection and Response (DDR)

While the capabilities discussed so far address static risks (identifying and classifying data), maintaining an effective security posture requires continuous monitoring of user behavior and data access patterns. This is where DDR comes in.

DDR in Action: Protecting Your Data Dynamically

DDR offers real-time monitoring and alerts to help security teams swiftly detect and respond to potential threats and suspicious activities, prioritizing those that endanger sensitive data. By leveraging AI and advanced analytics, DDR can identify anomalies in user behavior and access patterns that might indicate a compromised account or insider threat.

Conclusion: A Fortified Data Landscape

In today's data-driven landscape, where the threats to sensitive information are constantly evolving, it's imperative for organizations to fortify their data defenses. By implementing **Forcepoint DSPM+** and DDR together, organizations can build a formidable data security posture. Forcepoint DSPM+ lays the groundwork with thorough data discovery, classification, and risk management, while DDR enhances this foundation by providing real-time threat detection and response capabilities. This synergistic approach equips security teams to take proactive measures in safeguarding sensitive data, mitigating the risk of data exfiltration, and ensuring compliance with regulatory requirements. In essence, the combination of Forcepoint DSPM+ and DDR creates a fortified data landscape that is resilient against the ever-growing array of cyber threats.