Forcepoint

Datasheet

Forcepoint Data Detection and Response

Continuous detection and response to protect your most sensitive information

Key Features and Benefits:

- **Continuous Threat Detection and Response:** Forcepoint DDR continuously monitors data activity to detect and respond to security threats dynamically, helping to contain and mitigate threats before they cause significant damage.
- **Advanced Data Analytics and AI Classification:** Leveraging advanced data analytics and the Forcepoint DSPM AI Mesh, Forcepoint DDR identifies data vulnerabilities and suspicious activities, enabling proactive threat management.
- **Comprehensive Data Visibility:** Forcepoint DDR provides extensive visibility across cloud and endpoint environments, preventing data breaches by ensuring potential vulnerabilities are addressed.
- **Enhanced Incident Investigation:** Offering forensic-level details by tracing a file's lifecycle, Forcepoint DDR enhances the investigation of security incidents, leading to more accurate remediation decisions and reducing false positives.

Organizations are grappling with an alarming increase in data breaches, driven by the rapid adoption of cloud computing and AI technologies. These data breaches are impacting businesses globally, resulting in significant financial losses and reputational damage. The challenge lies in the ability to detect and respond to these breaches before they occur, ensuring the protection of sensitive data.

Forcepoint Data Detection and Response (DDR)

Forcepoint DDR powered by GetVisibility is a key solution for addressing these challenges. It provides continuous threat detection and enhanced data risk visibility, ensuring that organizations can effectively see changes to data that are likely leading to data breaches. By leveraging AI-driven responses, Forcepoint DDR offers threat neutralization, helping organizations maintain robust security measures. Its extensive visibility across cloud and endpoints, combined with data lineage tracking, makes it an essential tool for safeguarding sensitive information, reducing financial losses and maintaining customer trust.

Continuous Threat Detection and AI-Driven Responses

Forcepoint DDR provides continuous threat detection and enhanced data risk visibility, ensuring that organizations can identify, monitor and respond to threats. Leveraging responses powered by Forcepoint's AI Mesh, Forcepoint DDR acts to neutralize threats, offering a robust defense against data breaches.

Extensive Visibility Across Cloud and Endpoints

Forcepoint DDR offers extensive visibility across both cloud and endpoint environments. This comprehensive view helps organizations prevent data exfiltration and ensures that potential vulnerabilities are monitored and addressed. The inclusion of data lineage tracking further enhances the ability to counter potential breaches accurately.

Enhanced Productivity and Cost Reduction

With continuous threat detection and dynamic responses, Forcepoint DDR enables security teams to focus, helping prioritize data and permissions changes pointing to potential data breaches in action. This enhances productivity and supports organizational goals of cutting costs, reducing risks and maintaining customer trust.

Key Addition to Forcepoint DSPM

As companies seek to secure their data posture, reducing risky data across cloud and on-prem locations, Forcepoint DDR brings continuous risk visibility to Forcepoint DSPM. Instead of needing to run a complete discovery scan of data locations first, Forcepoint DDR enables continuous monitoring of the data security posture immediately after being deployed. Even without prior discovery scans, Forcepoint DDR detects and enables remediation for new data risks as they are happening. This continuously prevents new risks to the overall data security posture.

By integrating these advanced features, Forcepoint DDR not only protects data but also secures the future of organizations in the age of GenAI and cloud computing.

FEATURE	BENEFIT
Continuous Monitoring	Gain continuous visibility into risky data activities allowing organizations to detect and respond to potential threats.
Automated Alerts	Reduces time to response to potential data breaches by prioritizing and sending alerts based on detected data risk threats.
Data Movement Detection	Ensures that data remains within authorized boundaries, protecting intellectual property and sensitive information.
Policy Violation Enforcement	Secures compliance with data protection regulations by detecting and alerting on policy violations.
Compliance Tools	Simplifies adherence to regulatory requirements with continuous monitoring and detailed data histories to simplify audits and compliance reporting.
Proactive Risk Management	Defines and enables enforcement for what constitutes risk within the organization using customizable governance policies.
Overshared File Tracing	Increases data exfiltration visibility, revealing a malicious chain of events or an accidental breach.
3rd Party Security Tool Integration	Improves incident response and threat management through integration with SIEM and SOAR solutions.
Cloud and Endpoint Coverage	Enables organizations to fully understand and secure their data providing extensive visibility across the data ecosystem.
Detailed data type and sensitivity classification	Provides data context visibility, enabling security teams to assess risks and respond effectively.
AI Classification (AI Mesh)	Provides superior data classification accuracy that is efficient and highly trainable.
Forensics Capabilities	Increased remediation accuracy and reduced false positives through thorough security incident investigation.
Dynamic Incident Investigation	Accelerates incident response times, reducing the impact of security incidents, and continuously improving the organization's overall security posture.
Data Lineage Visibility	Empowers organizations to fully understand the lifecycle of their data through detailed historical tracking of unstructured files.