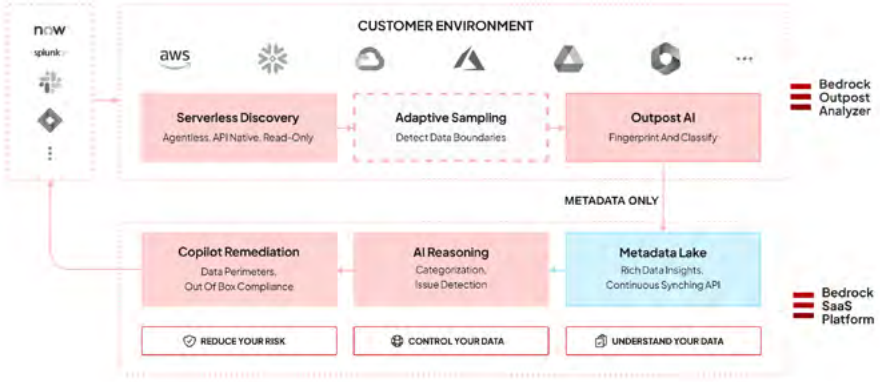
Bedrock Security: Unified Data Security and Governance at Scale

Overview

Enterprises face unprecedented data sprawl, fueled by cloud adoption and growing AI workloads. Yet, according to the **Bedrock 2025 Enterprise Data Security Confidence Index**, 82% of cybersecurity professionals report data visibility gaps. This data volume and complexity challenges cybersecurity, compliance, and data management teams, as regulators (SEC, GDPR, HIPAA, PCI DSS) tighten breach reporting rules, and 65% of security teams require days or weeks to locate sensitive data.

Bedrock delivers ubiquitous, AI-driven data security, enabling Security, GRC, and Data Management teams to share real-time insights. Its integrated Metadata Lake continuously captures data context—location, sensitivity, usage, and entitlements—enabling you to dynamically monitor data, assess risk, enforce policies, and streamline security workflows, ensuring your data ecosystem remains secure and compliant.

How It Works



Bedrock Architecture Overview

Understand Your Data

Understanding where your data resides is the first step to securing it. Bedrock provides continuous discovery and classification, ensuring GRC, Data Management, and Security teams have a unified, real-time view of all enterprise data.

Fast Deployment & Scanning: Bedrock's Outpost deploys in one click, scanning data across cloud services while preserving privacy. Only metadata is sent to the SaaS platform, ensuring real-time security insights without exposing raw data.

AI-Powered Data Discovery: Scans structured and unstructured data across SaaS, PaaS, and IaaS environments.

Key Benefits

Scalable Architecture

SERVERLESS ARCHITECTURE: Data categorization that classifies discovered data without rules by learning the topics that are critical to your business - automatically. These topics can be general (e.g., "Financial Data") or specific (e.g., "Income Statement") and add critical context that enables businesses to more effectively prioritize their datastores and detected risks for remediation, saving time and reducing risk of an impactful breach.

METADATA LAKE AS A SINGLE SOURCE OF TRUTH: The foundation of Bedrock's platform, it continuously ingests and updates metadata on data sensitivity, location, access, usage and 50+ other parameters to provide an authoritative, real-time security and governance source.

REAL-TIME DATA PROCESSING: Dynamically updates and correlates metadata across structured and unstructured data, enabling continuous risk evaluation, entitlement tracking, and compliance enforcement without requiring full dataset rescans.

Data Discovery & Classification at Scale

ADAPTIVE ENTITLEMENT & ACCESS MAPPING: Continuously analyzes and updates data access patterns, automatically identifying over-provisioned entitlements and reducing unnecessary exposure risks.

CROSS-TEAM ACCESSIBILITY: Security, GRC, and Data Management teams share a unified, real-time view of sensitive assets.

COPILOT AI INTERFACE: Enables natural-language investigations and policy validation across teams.

GenAI Data Security & Protection

TRUST BOUNDARIES: Automatically isolates sensitive IP and regulated data from AI model training.

AI-AWARE SECURITY: Automatically detects unauthorized AI data usage and flags exposure risks in AI pipelines.

CONTINUOUS AI GOVERNANCE: Ensures proper data access controls for AI/ML models with transparency using our unique AI Data Bill of Materials (DBOM) capability.

Contextual Classification: Automatically applies dynamic data labels (PII, financial data, intellectual property).

Cross-Team Accessibility: Share a unified, continuous view of data assets.

Control Your Data

Once data is discovered, organizations need continuous monitoring, governance, and policy enforcement to ensure proper usage and security.

Continuous Risk Assessment: Continuously monitor for policy violations and entitlement risks.

AI-Aware Security: Automatically detects unauthorized AI data usage and flags exposure risks in AI pipelines with an AI Data Bill of Materials.

Adaptive Scanning & Continuous Alerts: Detects anomalies in access, movement and entitlements, and ensures that security operations teams receive immediate alerts when thresholds are exceeded with SIEM/SOAR integrations.

Trust Boundaries & Dynamic Data Protection: Keeps sensitive data from AI model training, unauthorized cloud regions, and policy violations. Works across diverse data stores (AWS, Snowflake, GCP, etc.) without requiring platform-specific configurations. Helps implement least privilege and monitors sensitive data movement across hybrid and multi-cloud environments.

Copilot: AI-Powered Query Interface: Security, GRC, and Data teams can get instant answers, reducing time spent on investigations and audits, by simply asking things like:

> **"Which data sets are at high risk right now?"**
>
> **"Who accessed regulated data this week?"**

Reduce Your Risk

Beyond visibility and monitoring, proactively reducing attack surfaces and governance risks is critical for enterprise security.

Entitlement Right-sizing: Implement least-privilege enforcement to reduce insider threats and external risks.

Proactive Compliance Monitoring: Ensure compliance is continuously monitored with built-in policy rules for GDPR, CPRA, PCI DSS, and emerging AI regulations. Simplify compliance checks and accelerate regulatory responses with Audit-Ready Reporting.

Stale Data & Redundancy Elimination: Identifies neglected or duplicate data to lower costs and compliance risks.

Extended Functionality: Bedrock integrates with SIEM, SOAR, CNAPP/CSPM, DLP, and other security and compliance tools via APIs, enhancing threat detection and automated response, misconfiguration detection and policy enforcement, data loss prevention and AI compliance monitoring, and risk-based prioritization with continuous governance.

Key Benefits (con'td)

Full-Stack Integration & Automation

BIDIRECTIONAL API INTEGRATIONS: Pushes data context to ticketing systems for automated workflows and pushes structured metadata to SIEM, SOAR, CNAPP, CSPM, and DLP for enhanced security automation and policy enforcement.

ACCELERATED RISK MITIGATION: Reduces Mean Time to Detect & Respond (MTTD/R) by automating risk analysis, triggering proactive alerts, and streamlining remediation through integrated ticketing and security workflows.

API-DRIVEN RISK PRIORITIZATION: Pushes classification tags and sensitivity metadata to CNAPP, DLP, and compliance tools, enabling prioritized security actions and automated policy enforcement based on actual data exposure and sensitivity.

Dynamic, Policy-Driven Control

AUTOMATED POLICY MONITORING: Automatically monitors data isolation policies to prevent data movement into unauthorized locations and provides insights to enable least privilege enforcement."

REAL-TIME RISK ASSESSMENT: Continuously monitors for policy violations and entitlement risks.

AUTOMATED COMPLIANCE: Provides built-in governance policies for GDPR, CPRA, PCI DSS, and emerging AI regulations.

Fastest Time-to-Value

ONE-CLICK DEPLOYMENT: Discover and classify data in minutes, not weeks with privacy-preserving analysis.

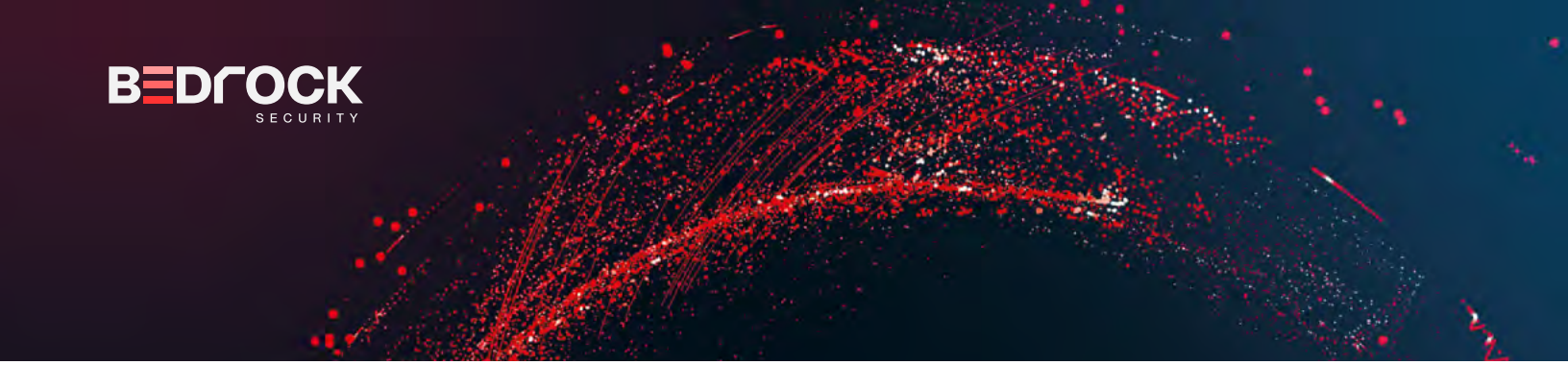
AUTOMATED CLASSIFICATION: AI-driven discovery classifies both structured, semi-structured, and unstructured data, reducing manual workloads for Security, GRC, and Data teams.

Speed, Scale & Cost Efficiency

SERVERLESS ARCHITECTURE: Scales to petabytes of data without operational overhead and seamlessly handles spikes in data creation, duplication, and movement across multiple datastores.

ADAPTIVE SCANNING TECHNOLOGY: Enables efficient, high-speed scanning without excessive compute costs.

LOW OPEX: Eliminates the accuracy-cost tradeoff of legacy DSPM solutions with patented scanning technology and serverless architecture efficiencies.



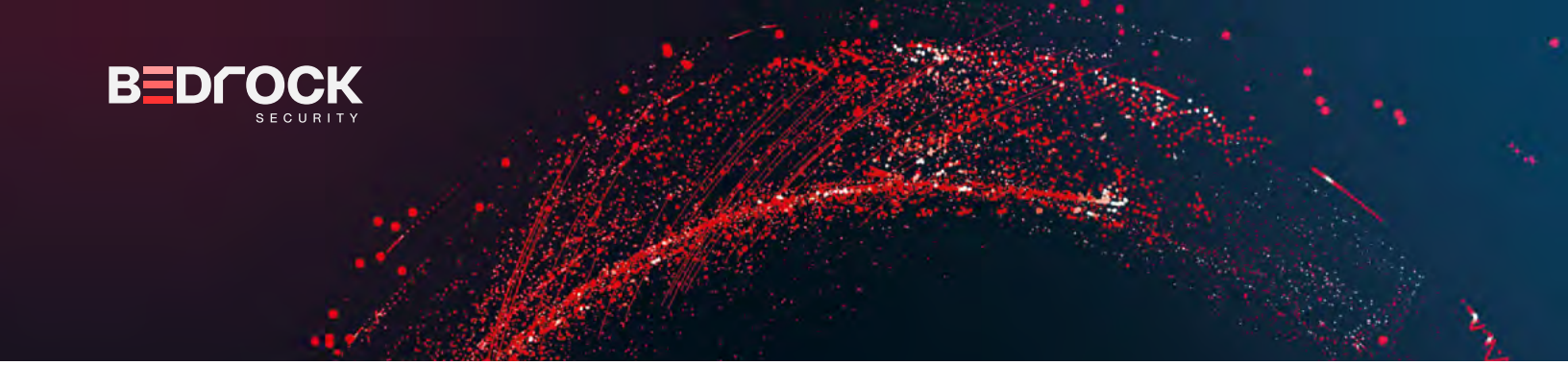
Metadata Lake: The Key Differentiator

Unlike legacy DSPM solutions, Bedrock's Metadata Lake continuously aggregates, updates, and contextualizes metadata across all data sources. This ensures:

- Continuous visibility into data sensitivity, access patterns, and entitlement risks.
- Lower cost and operational overhead through fast deployment, redundant scans and static rule tuning.
- Stronger compliance enforcement with historical data movement tracking and automated audit reporting.

Bedrock vs Legacy Solutions

SUBSECTION	DSPM & LEGACY SOLUTIONS	BEDROCK SECURITY (WITH METADATA LAKE ADVANTAGE)
Time-to-Value	Significant time for initial setup from days to weeks. Requires extra tools for policy enforcement, remediation, and forensics. Needs continuous rule tuning for data changes and evolving threats.	Deploys in minutes with AI-powered automation, removing the need for tuning and rule adjustments. AIR Engine accelerates time-to-value by automatically learning data and business context. Metadata Lake continuously updates data context, reducing the need for manual re-scanning and rule adjustments.
Deployment	Some DSPMs expose customer data to their employees. DSPMs have heavyweight and complex deployment models.	Outpost model ensures Bedrock never sees customer data. CloudFormation-based one-click deployment simplifies onboarding. Metadata Lake stores metadata, not raw data, ensuring privacy while maintaining security insights.
Visibility	Cannot process petabytes of data in minutes. High operational costs (compute and people) require lots of tuning. Large gaps of data visibility and slow updates increase risk.	Maps datastores, identities, and access relationships continuously across IaaS, PaaS, and SaaS platforms. No gap visibility with continuous data lineage, entitlements, sensitivity, and 50+ parameter updates.
Data Categorization	Uses rule-based, RegEx-driven classification. Limited customization and weak data lineage tracking. High false positive rates.	AI-driven classification detects data types and regulatory categories with no RegEx or fragile rules, incorporating business context for accuracy. Ensures precise, automated classification that adapts to evolving data environments.
Risk Prioritization	Lacks deep impact analysis, "blast radius" visualization, and limited entitlement analysis. Makes remediation prioritization difficult.	Ranks risks by exposure and impact with "blast radius" visualization and historical trends. High accuracy for proactive risk reduction and post-breach forensics with full entitlement chain analysis for human and non-human identities.



Bedrock vs Legacy Solutions

SUBSECTION	DSPM & LEGACY SOLUTIONS	BEDROCK SECURITY (WITH METADATA LAKE ADVANTAGE)
Reporting	Reporting varies based on the DSPM provider.	Exports reports and allows scheduled reports. Provides dashboards for a high-level security and compliance overview. Metadata Lake powers advanced reporting, allowing GRC teams to analyze historical trends in data movement, access patterns, and regulatory compliance adherence.
API Integrations & Automation	Some DSPMs only integrate with SIEMs, ticketing solutions, and SSO providers. Most DSPMs lack seamless security automation.	Provides pre-integrated ingestion and workflows with a range of security products. Enables metadata lake information to be shared with SIEM, SOAR, CNAPP/CSPM, DLP and other security and compliance tools. Push down classification tags enhance DLP accuracy.
Scalability & Cost Efficiency	Slower scanning speeds and higher costs due to brute-force data scanning.	Bedrock's serverless Adaptive Scanning eliminates redundant scans, reducing compute costs significantly. Metadata Lake ensures that organizations don't need to rescan entire datasets, allowing security teams to focus on real-time changes rather than redundant full-scale scans.
Responsible AI: Gen AI LLM	Limited AI governance and model training transparency. Poor visibility into AI/ML data usage.	Tracks datasets in AI models, creates Data Bill of Materials (DBOM), and prevents unauthorized GenAI usage with Trust Boundaries.
User Base	Primarily Security	Multifunctional. Equally benefits GRC compliance, Data Management, and Security roles.

Real-World Impact

- **60+ hours saved/week** - A healthtech firm automated compliance audits, allowing teams to focus on strategic initiatives.
- **10,000+ critical IP sequences protected** - Leading biotech used Trust Boundaries to isolate sensitive R&D data from unauthorized GenAI training sets.
- **2 PB+ discovered & classified in 24 hours** - A large HR tech enterprise leveraged serverless scanning to unify data posture across multiple cloud facilities.

> “Bedrock’s ability to automatically learn what data is most material to the business and put boundaries between sensitive data and GenAI models is a game-changer.
>
> CISO, Fast-Growing Global Tech Firm

About Bedrock Security:

Bedrock Security, the ubiquitous data security and management company, accelerates enterprises’ ability to harness data as a strategic asset while minimizing risk. Its industry-first metadata lake technology and AI-driven automation enable continuous visibility into data location, sensitivity, access and usage across distributed environments. Bedrock’s platform continuously catalogs data, enabling security, governance and data teams to proactively identify risks, enforce policies and optimize data usage — without disrupting operations or driving up costs. Trusted by leading financial institutions, healthcare providers and Fortune 1000 companies, Bedrock Security empowers organizations to improve data security posture management (DSPM), confidently deliver Responsible AI initiatives, and manage the exponential data growth.
Learn more at www.bedrocksecurity.com.