Introduction to Bedrock Security

Executive Overview

Enterprises face unprecedented data sprawl, fueled by cloud adoption and AI workloads, yet according to the **Bedrock 2025 Enterprise Data Security Confidence Index**, 82% of cybersecurity professionals report data visibility gaps. This 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. Traditional DSPM tools fail to scale in cloud and AI-driven environments due to their reliance on static, rule-based classification.

Bedrock delivers unified, AI-driven data security that enables 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 automate security workflows, ensuring your data ecosystem remains both secure and compliant.

The Growing Challenge of Data Sprawl in Distributed Environments

Global data creation will surpass 175 zettabytes by 2025 (IDC), and most enterprises see monthly data growth between 63-100%. Yet, according to the **Bedrock 2025 Enterprise Data Security Confidence Index**, only 24% of organizations can generate a full data asset inventory within hours, while 11% require weeks or longer. Unmanaged data sprawl results in:

- **Expanded Attack Surface:** Cloud, SaaS, and AI datasets create misconfigurations and lateral attack risks. 79% of security teams struggle to classify AI training data, while 77% lack assurance on AI access controls.
- **Regulatory Pressure:** SEC, GDPR, HIPAA, and PCI DSS mandate faster breach detection and reporting, yet many organizations lack automation, increasing compliance risk.
- **Talent Shortages:** 4M unfilled cybersecurity jobs slow incident response and compliance enforcement **(ISC2, 2023)**. 66% of security teams lack people and processes for proper analysis.

With 51% of security teams now actively involved in AI data governance, the lines between Security, GRC, and Data Management are blurring. A unified, AI-driven approach is essential to ensuring enterprise-wide data security, compliance, and governance.

Introduction
to Bedrock Security

BEDROCK SECURITY

Why Legacy Data Security Falls Short

Most traditional security models revolve around endpoints, networks, and perimeter defenses and do not inherently protect the data itself. Legacy Data Security Posture Management (DSPM) tools have attempted to address this gap by using static rules or regular expression (RegEx), based classification, resulting in a slow, resource-intensive process that cannot adapt to fast-evolving cloud and AI workloads. This leads to both inefficiency and inaccuracy at high volumes of dynamic data. Traditional DSPM solutions suffer from:

Inability to Scale: Hard-coded classification rules cannot adapt to newly emerging data types, formats, or AI training datasets. Over time, these rule sets need constant manual tuning, which fosters alert fatigue and makes it difficult to scale effectively.

Poor Alignment with GRC and DataOps: Legacy DSPMs often treat compliance and data management as peripheral tasks. They provide standard integrations with SIEM and SOAR but not typically with the broader set of tools, like data analytics platforms, DLPs, CNAPP/CSPM, and compliance tools that GRC and Data teams depend on.

High Operational Cost: Traditional DSPMs often require extensive on-premises software installations or resource-heavy container deployments in the customer's environment. As data volumes scale, scanning becomes increasingly expensive, while gleaning real-time insights becomes unfeasible.

All of these factors cause friction not just for cybersecurity staff, but for everyone involved in data governance and usage. With no real-time, context-aware insight into data sensitivity or threat levels, organizations react to crises instead of preventing them.

Introducing Bedrock Security's Ubiquitous Data Security Approach

At the core of Bedrock Security's platform is the Metadata Lake, a continuously updated, authoritative repository of enterprise-wide metadata. Unlike traditional DSPM tools that rely on static, rule-based classification, Bedrock delivers real-time, AI-driven risk intelligence to unify security, governance, and data management.

Continuous Data Lineage, Sensitivity, and Entitlement Tracking: Automatically maps who has access to which data, where it resides, and how it moves across IaaS, PaaS, and SaaS environments.

API-First, Seamless Integration: Enriches SIEM, SOAR, DLP, CNAPP, and compliance tools with structured metadata for automated enforcement and policy validation.

Real-Time Risk Prioritization: Goes beyond static rules to factor in actual data sensitivity and access patterns, prioritizing alerts for rapid, targeted remediation.

Privacy-Preserving Deployment: The Outpost model ensures raw data never leaves customer environments, sending only structured metadata to Bedrock's SaaS platform.

Scalable, Cost-Effective Architecture: Unlike legacy DSPM solutions, Bedrock's serverless design eliminates redundant scanning and lowers OpEx while handling petabytes of data with near real-time updates.

Copilot: Enables teams to query the metadata lake using natural language, instantly uncovering risk, compliance gaps, and data insights. It acts as a first-level analyst, streamlining security investigations, compliance validation, and data optimization—no SQL required.

With Metadata Lake, organizations achieve continuous visibility, security automation, and compliance enforcement, turning fragmented data governance into a seamless, AI-powered process.

Delivering Business Value to Security, GRC, & Data Teams

Bedrock Security ensures that Security, GRC, and Data Management teams share a real-time, unified view of data risk, access, and compliance—eliminating silos and manual inefficiencies.

Security Teams:

Proactive Risk Reduction & Faster Threat Response
Security teams need real-time, automated visibility into data risks to prevent breaches and minimize exposure. Bedrock Security enables faster detection, response, and remediation by continuously analyzing data sensitivity, entitlements, and threats.

Risk-Based Prioritization: Highlights sensitive data exposure, maps vulnerabilities to data stores, and prevents alert fatigue by focusing on high-impact risks.

Seamless Incident Response Integration: Reduces Mean Time to Detect & Respond (MTTD/R) by automating ticketing workflows and integrating with SIEM, SOAR, and CNAPP to escalate and resolve threats efficiently.

Trust Boundaries for Least Privilege Access: Prevents overexposed data access, limiting insider threats and external risks without manual rule configurations.

GRC Teams:

Continuous Compliance & Simplified Audits
GRC teams must enforce regulatory mandates (GDPR, HIPAA, SEC, PCI DSS) while reducing manual audit burdens. Bedrock delivers real-time compliance validation, automated governance, and instant audit readiness.

Continuous Compliance Monitoring: Automatically enforces security policies, ensuring data never moves into unauthorized locations and remediates violations in real-time.

Audit-Ready Reporting: Metadata Lake provides an up-to-date record of data access, usage, and entitlements, making regulatory audits seamless.

AI-Powered Policy Validation: With Copilot, teams can instantly surface policy violations, misconfigurations, or non-compliant data handling practices, drastically shortening reporting cycles.

Data Management Teams:

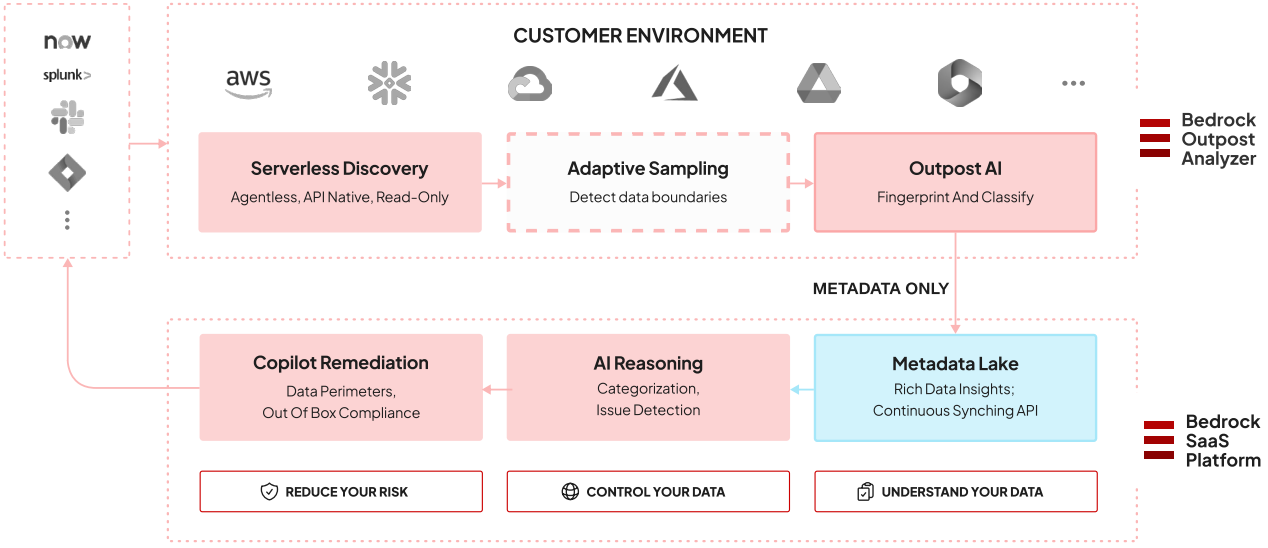
Smarter Data Utilization & Cost Optimization: Data Management teams must eliminate redundant data, optimize storage, and ensure business-critical data remains protected. Bedrock simplifies classification, lineage tracking, and access control, reducing manual overhead.

End-to-End Data Lineage: Tracks how data moves across IaaS, PaaS, and SaaS, ensuring visibility into sensitive information and preventing uncontrolled sprawl.

Stale & Redundant Data Cleanup: Identifies low-use, duplicate, or obsolete data, helping teams reduce storage costs and improve performance.

Instant Data Insights: Copilot enables you to ge instant answers to critical data questions, such as “Where are my largest, least accessed datasets?” or “Which assets contain regulated data?”, improving efficiency.

Building a Strong Data Security Foundation for the Future
Most organizations begin their data security journey with a fundamental layer of visibility, then evolve toward more sophisticated capabilities as they mature. It’s critical to recognize your organization’s current stage and chart a path forward that addresses today’s explosive data growth without creating unnecessary friction for security teams—or the broader business.



Bedrock Architecture Overview

STAGE 1: Understand Your Data

The first, and arguably most critical, step in establishing a robust data security program is to discover and accurately classify all data across the enterprise thoroughly. Many legacy tools claim to offer visibility but rely on rigid or partial scanning, leaving Security and GRC teams either inundated with false positives or missing key information. In contrast, Bedrock Security takes an AI-driven approach that continuously scans structured and unstructured data within SaaS, PaaS, and IaaS, then stores rich, context-aware metadata in the Metadata Lake to provide visibility across security and governance. This ensures that classification remains timely and precise, forming a solid basis for all subsequent risk management efforts.

Accurate Risk Assessment as the Cornerstone

By ingesting data context into the Metadata Lake, Bedrock pinpoints each data type, location, and access pathway to reveal how and where data might move. This end-to-end visibility covers well-known datasets and previously undocumented information, significantly reducing blind spots. As a result, teams gain the foundational clarity needed to identify and mitigate risk properly, right from the start.

Contextual Classification

Instead of applying static rules, Bedrock's AI reasoning engine automatically discovers data and analyzes its business context. This process attaches relevant attributes—such as sensitivity level, ownership, and usage patterns—to each asset. The result is a highly accurate classification system with fewer false positives, less manual intervention, and more confidence in the overall risk assessment.

Entitlement Visibility

By mapping identities to data and highlighting which roles have what level of access, Bedrock enables you to build initial security policies quickly. This streamlined approach simplifies early-stage governance, ensuring that each data set's actual risk profile is accurately reflected in the discovery process and downstream compliance efforts.

> **"I believe that effective security requires looking at the full lifecycle of how customer data is handled. This means getting accurate visibility, enabling data perimeters, and proactively reducing data risk. Bedrock's innovation excites me and aligns with how I think about protecting data and managing risk effectively**
>
> Mukund Sarma, Sr. Director Product Security,
> Fastest Growing US Fintech Co.

Stage 2: Control Your Data

Once your organization has accurately discovered and classified all data, the next step is to build advanced, continuous data security that can handle both shifting business needs and dynamic threats.

Adaptive Sampling & Real-Time Alerts

Bedrock employs Adaptive Sampling, which enables it to monitor large volumes of data in a time-and cost-efficient way. This approach reduces the mean time to detect/respond (MTTD/R) by swiftly surfacing anomalies, policy violations, and high-risk changes in data posture.

Integrated Detection & Remediation Workflows

Beyond flagging issues, Bedrock's built-in detection and remediation workflows minimize manual intervention. Policies can be configured to spot compliance breaches and suspicious activity, and immediately alert teams.

Seamless Integration With SIEM, SOAR & GRC dashboards

For continuous protection, Bedrock integrates with common security platforms—SIEM, SOAR, and GRC dashboards—ensuring essential updates, such as newly discovered or misconfigured data, always reach the right teams at the right time. This reduces security blind spots while enabling a faster, more coordinated response.

> **Within a week of implementing Bedrock, we noticed some unexpected data in our lowest development environment. This prompted us to review our system configurations and ensure everything was aligned with our protocols.**

Andrew Kuhn
Product Security Engineer, House Rx

STAGE 3: Reduce Your Risk

Building on a strong foundation of discovery, classification, and continuous monitoring, the final stage is to proactively reduce the data security attack surface. Organizations can drive down risk and complexity by implementing measures that minimize overexposure.

Least-Privilege & Entitlement Right-Sizing

With a clear view of who has access to what, and how they obtained it, security teams can trim unnecessary entitlements, preventing dormant or "ghost" privileges from granting attackers easy inroads.

De-Cluttering & Hardening

Bedrock's AI-driven insights also identify stale or redundant data, making it possible to remove what's no longer needed. This frees up resources and narrows the window of potential exploit. For data that must remain accessible, techniques like masking or encryption harden it against unauthorized use.

Protecting Core Intellectual Property (IP)

Whether you're safeguarding high-value IP, personal data governed by privacy laws, or regulated financial records, Bedrock's AI-enabled fingerprinting and threat graphs trace data lineage and usage. These capabilities allow security teams to closely monitor and protect key assets in real time, reducing friction across lines of business.

> **"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. This capability reduces friction and enables us to safely and responsibly bring GenAI to customers faster.**
>
> Suha Can
> CISO, Grammarly

Embrace the Future of Data-Driven Security & Governance

Organizations stand on the cusp of significant transformations in data use, from harnessing AI for new product innovations to integrating sophisticated cloud services that streamline business processes. While these shifts promise remarkable gains, they also carry heightened security, compliance, and management requirements.

Bedrock Security offers a practical, scalable, and cost-efficient framework to handle these evolving demands. AI-driven classification and real-time metadata significantly reduce manual overhead while dramatically improving risk detection and compliance posture. With natural-language query capabilities, all stakeholders—Security, GRC, and Data teams—can collaborate on a single, trusted view of the organization's data ecosystem.

In short, Bedrock Security frees teams from chasing scattered logs and reacting to threats after the damage is done. Instead, they can operate on proactive, real-time insights and enforce compliance across the board. From rapidly addressing newly discovered vulnerabilities to ensuring that sensitive data never drifts into unauthorized environments, the platform transforms data from a liability into a strategic asset.

Next Steps

1. **Assess Your Current Posture:** Identify where your most significant data blind spots lie.
2. **Request a Demo:** Experience how Bedrock Security integrates seamlessly with existing tools and processes.

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 innovate securely in an era of cloud transformation, AI adoption and exponential data growth. Headquartered in Silicon Valley and backed by Greylock, the company is led by experts in cloud, GenAI cybersecurity and data storage. Learn more at **www.bedrocksecurity.com**