# Product Data Sheet

Bedrock Security delivers enterprise data discovery, classification, and protection at the scale and speed required by modern businesses. Our solution ensures quick time-to-value, whether your organization seeks visibility and compliance, detection and response (DDR), or to minimize the data security surface.

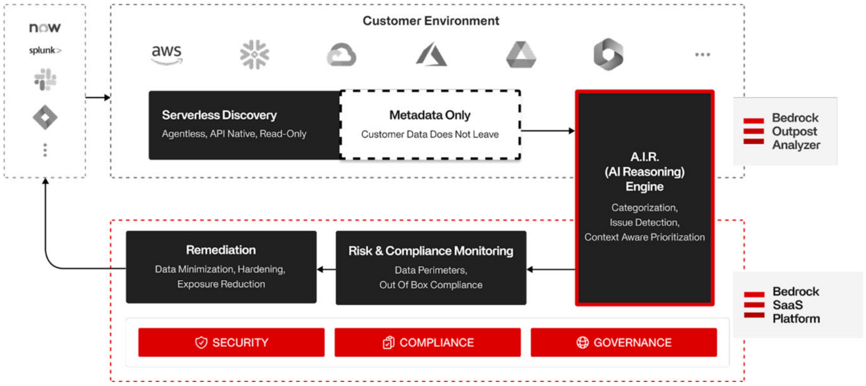
## How It Works

1. **Quick Time-To-Value**

   Bedrock's deployment wizard automatically configures and deploys the Bedrock Outpost Analyzer with one click. The Outpost discovers and classifies all relevant datastores across your platforms, without requiring input.

2. **Speed and scale**

   Bedrock's Outpost Analyzer discovers and classifies customer data onsite, only sending metadata to the Bedrock SaaS Platform. This means that Bedrock never sees customer data, ensuring complete privacy. For example, if there is a database column with "Passport Number" as the name of the column, and the column contains passport numbers, Bedrock would know the name of the column and would know that it contains passport numbers, but Bedrock would never see the actual passport numbers.



### Bedrock Architecture Overview

Bedrock is comprised of two components: the Bedrock Outpost Analyzer, which deploys via infrastructure as code in the customer's environment, and the Bedrock SaaS Platform, which ingests metadata for processing through Bedrock's AI Reasoning Engine (AIR) and offers a user interface for security, compliance, and governance users.

## Key Benefits

**NO RULES** 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.

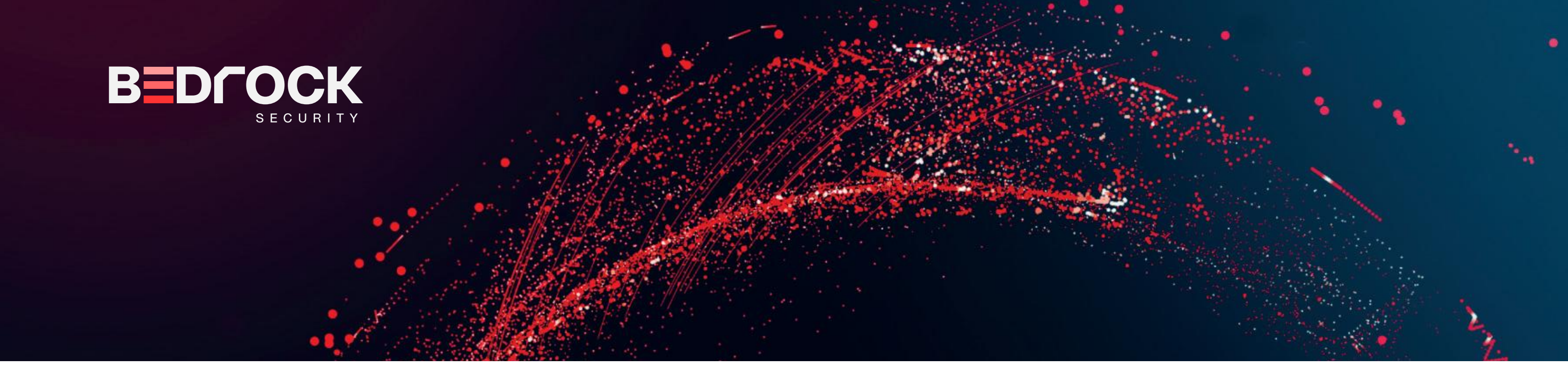
**SPEED AND SCALE** Bedrock can discover, classify, and analyze risk for TBs in minutes. Through its unique Adaptive Sampling technology and a highly efficient serverless architecture, enterprises can ensure they can adapt to data and threat changes as often as they like without incurring more costs.

**LOWEST OpEx** Bedrock eliminates the accuracy-cost tradeoff through a serverless architecture. This enables frequent scans and rapid issue resolution, unlike legacy DSPMs which incur high compute run costs.

**DYNAMIC POLICY** Bedrock's dynamic Trust Boundaries, based on superior classification, simplify data and access management with user-friendly policies and enhanced violation detection capabilities

**COMPLETE INTEGRATION** Bedrock integrates seamlessly with platform APIs for streamlined remediation, reducing mean time to resolution (MTTR) and accelerating the closure of security gaps.

**GENAI READY** Advanced fingerprinting, Trust Boundaries, and DBOMs to ensure GenAI security and compliance.



### Serverless Discovery

Bedrock's Outpost Analyzer uses your infrastructure's existing APIs to discover datasets – structured or unstructured – across datastores, accounts, and infrastructure providers. Simply point Bedrock to your accounts and the system takes care of the rest - at scale, without agents, and ensures your data remains in your environment.

### AIR Engine

The AI Reasoning Engine (AIR) is the heart of being able to understand what data means and its material value to the business. AIR processes metadata from a customer's environment to discover data, categorize and classify it, assess against a multi-dimensional set of criteria to alert on security or compliance issues, and determine prioritization for remediation based on context of data and risk factors.

### Remediation

Bedrock provides remediations for all discovered issues with a menu of relevant options to contain and mitigate risk. Using API integrations, Bedrock can apply many of these remediations with one click, or can automatically create a ticket in a user defined workflow tool with detailed instructions.

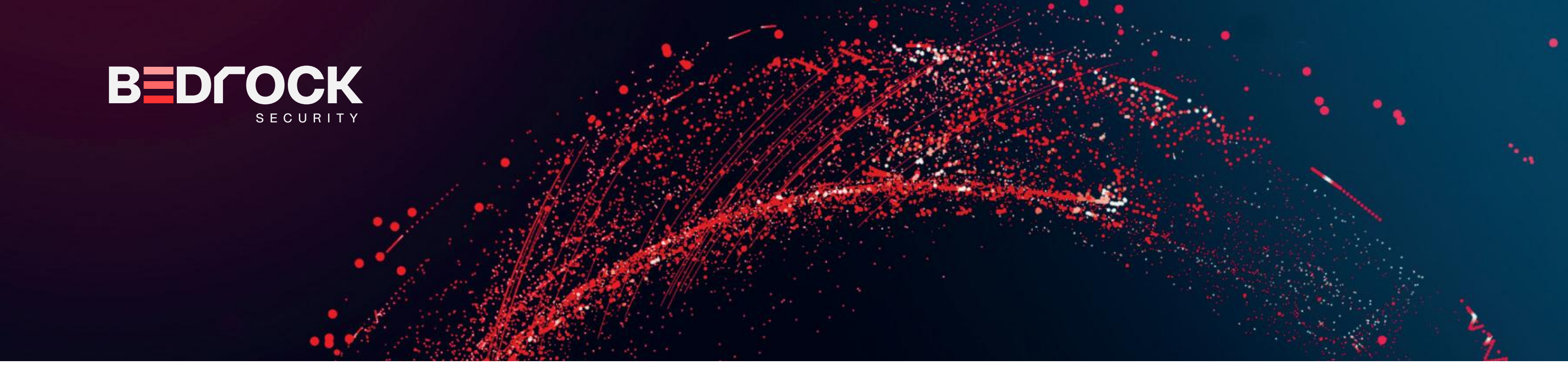
### Risk & Compliance Monitoring

Bedrock detects hundreds of violations of recommended best practices, including misconfigurations, postural violations, and overly broad permissions, as well as violations of the controls of common compliance frameworks.

Bedrock's Trust Boundary is a patented, adaptive policy technology that allows you to quickly highlight what data is important and the system takes care of the rest. The policy engine enables custom policies, drawing upon Bedrock's dynamic data categorization and classification. For GenAI, Trust Boundaries can be created to protect source and derivative works from sensitive information, core IP, or copyrighted materials.

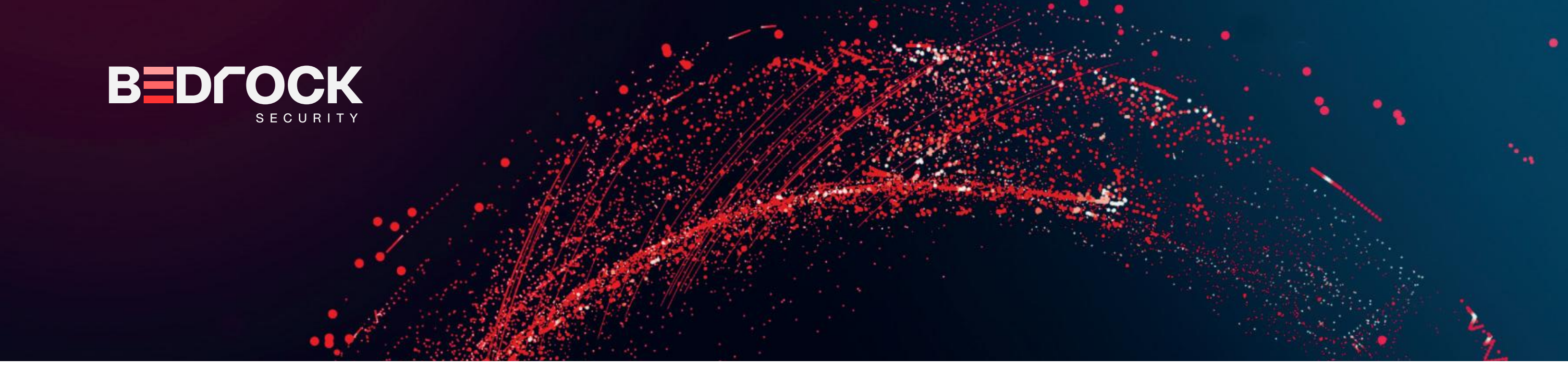
### Use Case Roles

Bedrock reduces friction by ensuring different groups can work together to seamlessly protect your data. Security teams can benefit from DDR alerts and least privilege capability - with SIEM/SOAR integrated routing for SOC and threat hunting teams. Compliance teams can leverage out-of-the-box compliance assessment and reporting, as well as, create new policies for assurance and audit. And governance teams can create more accurate data maps and data access governance policies based on user, data type, data source, and other factors.



## Bedrock vs Legacy Solutions

| SUBSECTION | DSPM & LEGACY SOLUTIONS | BEDROCK |
|---|---|---|
| Time-to-Value | Significant time for initial setup. Additional tools or steps required for policy enforcement, remediation, or forensics. Ongoing rules tuning for each datastore, data type, and as data changes and threats evolve. | Ready to run in minutes with all key elements in one platform, integrating seamlessly with existing workflows for accelerated ROI. AIR accelerates time-to-value by learning data and business context automatically. |
| Deployment | Some DSPMs operate in a model where enterprise data is visible to their employees, and have more complicated, heavyweight deployments. | The Outpost model ensures Bedrock never sees your data and one-click deployment via a CloudFormation template makes onboarding quick. |
| Visibility | Limited ability to detail entitlements, leading to possible gaps. | Shows datastores, principals, services, and how they relate to each other. Traverses the full entitlement permission structure to understand exactly what access has been granted and uses access activity to determine actual usage. |
| Data Categorization | Limited classification abilities due to reliance on rules and complex RegEx's, generally restricted to regulatory-based types. Less extensive customization options. Data lineage either not offered or with limited capabilities. | Classifies using regulatory categories (e.g., PII, PCI), broad topics (e.g., HR data), and document type (e.g., W4 form). Allows customers to create custom data types and classifications based on their internal data - no rules or RegEx's required. Performs data lineage analysis to detect instances of data being copied (even partially) from one datastore to another. |
| Risk | Limited categorization abilities make impact analysis less useful. Most do not have "blast radius" visualization. | Ranks each datastore, principal, or service by its potential impact if compromised, enabling easy prioritization. Provides visual "blast radius" analysis that details the impact of an account takeover or other breach. Detects overprovisioned principals with more access to data that they need and provides minimization workflow. |
| Detection & Response | Limited or no ability to create custom policies or Trust Boundaries. None or generic remediations that are often not relevant to the detected problem. | Offers a wide array of pre-configured Issues pinpointing typical misconfigurations, departures from optimal practices, and breaches of standard compliance protocols. Empowers users to craft personalized policies like Trust Boundaries, outlining the permissible locations for sensitive data. Simplifies the remediation process for identified issues by presenting a concise selection of relevant options to minimize or alleviate risk. |



## Bedrock vs Legacy Solutions

| SUBSECTION | DSPM & LEGACY SOLUTIONS | BEDROCK |
|---|---|---|
| Reporting | Varies. | Ability to export reports and schedule regular reports to keep track of key internal metrics. Dashboards that provide a high-level view of data security posture at a glance. |
| Integrations | Integrations with SIEMs, ticketing solutions, and SSO/identity providers. | Integrations with SIEMs, ticketing solutions, and SSO/identity providers. |
| Scale | Generally takes much longer to scan and onboard data, with substantial infrastructure cost, due to brute force data scanning. | Fastest time-to-value and lowest OpEx in DSPM through leveraging Adaptive Sampling, removing the tradeoff between accuracy and cost. |
| GenAI Assurance | Limited. | Fingerprinting to identify datasets involved in model trainng or RAG databases. Creates a Data Bill of Materials (DBOM) for a full understanding of data being used for GenAI model training / fine tuning and RAG. Trust Boundaries for GenAI ensures protected data does not get used for training. |

## About Bedrock Security:

Bedrock Security, the frictionless data security company, is revolutionizing data security in the cloud and GenAI era with its leading data security platform powered by the industry's only AI Reasoning Engine (AIR). Bedrock delivers the speed, scale, and precision demanded by modern enterprises to embrace the explosive growth of data without introducing risk. Headquartered in the San Francisco Bay Area and backed by Greylock, the company is led by industry veterans in cloud, GenAI and cybersecurity. To learn more, visit https://www.bedrock.security/.