BEDROCK SECURITY

Confidently Embrace Data Sprawl with a Strong Data Security Program

A Bedrock Security Whitepaper

www.bedrock.security

Enabling business to grow safely in the era of cloud and GenAI

Executive Summary

To keep up with both competition and market demands, businesses are rapidly adopting cloud and GenAI services, which is causing an explosive growth in data. Data is growing at an unprecedented rate, outpacing the ability of security resources to analyze and protect it. To keep up with the volume, variety, and velocity of this data, businesses need to evolve their data security programs. They must ensure visibility into these vast data volumes and secure them without hindering business operations.

Legacy Solutions Don't Solve Today's Challenges

Despite exponential data explosion, security resources remain linear — security teams cannot and should not need to grow based purely on the volume of data. The global data creation is predicted to reach 175 zettabytes (ZB) by 2025, according to IDC. This is demonstrated in a [1]survey that revealed an organization deals with 63 percent growth in data volume per month, on average, with 12 percent of respondents reporting 100 percent growth. At the same time, organizations face growing cyber threats targeting that data.

Security teams already handle wide and varied information technology and security needs, and the legacy security tools currently in place were not designed to analyze and protect the modern enterprises' use of data. Attacks are occurring more frequently, and the attack surface is growing along with the data. As a result of these challenges, there are more regulations[2] regarding data security, with shorter response times mandated for companies impacted by a cyber event. Response is limited due to lack of resources, including cybersecurity talent[3].

[1] Ibrahim Surani (2020) *The Impact of Data Growth on Enterprises.* Dataversity https://www.dataversity.net/the-impact-of-data-growth-on-enterprises/

[2] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure https://www.sec.gov/files/rules/final/2023/33-11216.pdf

[3] Amanda Steinman (2023) ISC2 Reveals Growth in Global Cybersecurity Workforce, But Record-Breaking Gap of 4 Million Cybersecurity Professionals Looms https://www.isc2.org/Insights/2023/10/ISC2-Reveals-Workforce-Growth-But-Record-Breaking-Gap-4-Million-Cybersecurity-Professionals

Delays in identifying and classifying data results in more visibility gaps and longer mean time to recovery, repair, respond, or resolve (MTTR).

Security teams must identify and classify data quickly to ensure that the data is being accessed per policy, there is no overly permissioned access or exposure of that data, and that data is hardened as best as possible — all while ensuring continuous assessment of security and compliance issues that violate policy. Delays and inconsistent data access causes friction between security and other lines of business, resulting in individual teams fighting for resources, seeking prioritization for their data needs, and needing access to more security expertise. Meeting these growing data needs is challenging and significantly slows down the security team's ability to respond to cyber threats and other pressing security issues.

> "Generative AI poses a unique data challenge because once data goes into a model, it's challenging to control the output. Enterprises need assurances that GenAI models are compliant and secure, and that they will not divulge sensitive information."
>
> **Suha Can, CISO, Grammarly**

Legacy data security solutions, including Data Security Posture Management (DSPM), fall short of meeting modern business needs. They lack the necessary architecture for accuracy, scale, and speed, and depend on inaccurate rules-based data classification. Security teams waste hours updating rules to capture all pattern variations, a futile task as dynamic data usage disrupts static rules.

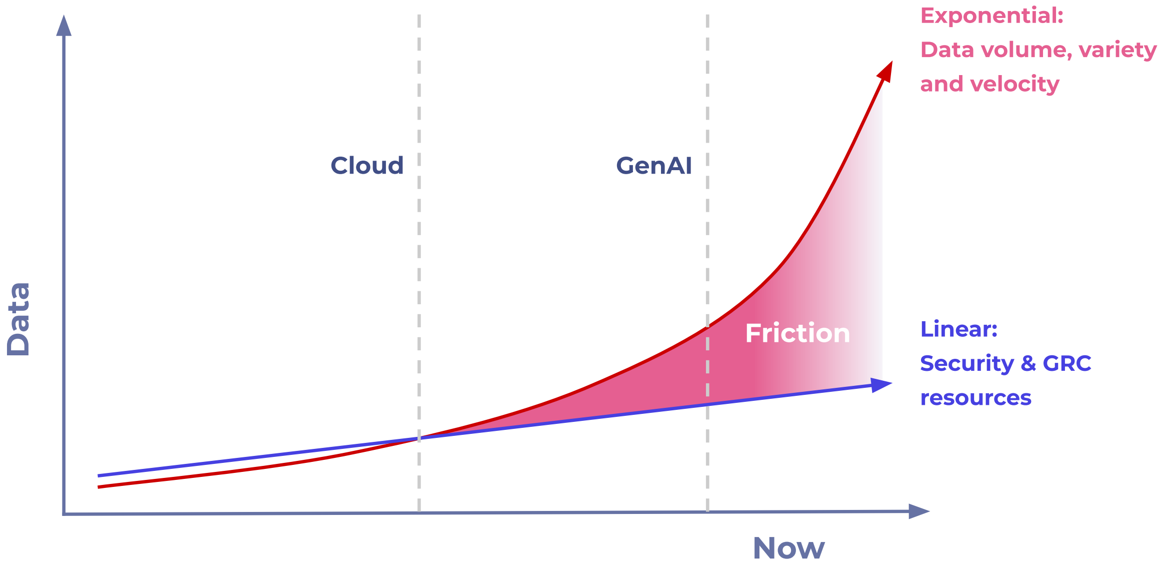
Introducing Frictionless Data Security

The key to enabling the business to use data safely is to make security resources exponential instead by making data security frictionless. By continuously discovering, managing, and protecting an organization's most sensitive data, Bedrock Security provides significant benefits at every level:

- **Organizational level:** The Chief Information Security Officer (CISO) no longer slows down business goals or inherits additional risk as the lines of business (LOB) and board of directors (BOD) seek to put data to use.

- **Security team level:** Internal security teams, including the security operations center (SOC); governance, risk, and compliance (GRC) team, and engineering team all can now work together seamlessly by simplifying data access and protection.
- **Individual level:** Individual SOC team members have fewer tickets and lower MTTR, GRC teams need fewer meetings and have less friction with the lines of business, and engineering teams have less overload and face less complexity because data security is simple and seamless.

This approach transforms data challenges into business opportunities. The technology that enables this solution must be built with artificial intelligence (AI) reasoning deployed on a highly efficient architecture.



How to Create a Robust Frictionless Data Security Program

Most organizations start with a basic foundation and then build from there. Understanding which stage an organization is in and how to get to the next level of maturity is vital to building a robust data security program. Data security programs must be designed for today's exponential data growth and data usage without causing unnecessary friction.

STAGE 1: BUILD A STRONG DATA SECURITY FOUNDATION

Many tools prioritize visibility but fail to deliver accurate information. This results in frustration on the part of those relying on the data and increased risk for the organization as a whole. Bedrock Security uses AI reasoning to go beyond fixed patterns to automatically provide a clear picture of risk. Accurate, prioritized risk assessment is key — everything else is built on knowing and understanding an organization's unique data.

The Bedrock platform provides accurate risk assessment by ensuring that organizations have both visibility into the data and a clear understanding of where and how the data could move. It does this by identifying data type, location, and access information, then classifying and categorizing data based on that information. This categorization, which discovers data and its business context without relying on rules, ensures the high accuracy needed for a strong data security foundation; Bedrock's AI Reasoning Engine (AIR) achieves this with accuracy and automation.

Bedrock also shows identity entitlement access to data, displaying who can access data and the context of that access. This is also important in terms of data movement shown as data maps/flows — where the data exists and where it can flow or move may impact who or what has access. Using all this information, an organization can not only assess risk, but also ensure that it is prepared to remediate risk if necessary. This comprehensive and accurate risk assessment and remediation reduces friction within the organization as the security team does not need to find the data owner upfront to do this discovery and classification. It also reduces friction by getting the classification on both known and discovered data, making it easier to identify the data owner and get an accurate picture of compliance status.

> "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: BUILD CONTINUOUS DATA SECURITY

Once an organization has accurate risk assessment and remediation, it's time to build more advanced data security. Through adaptive sampling, detection, and remediation capabilities, the Bedrock platform minimizes response times and enhances accuracy despite the constantly changing nature of data and cyber threats.

A core requirement for data security at this stage is to keep up with changing data, different access needs, and modern adversaries with constantly evolving tactics. Staying up to date with large volumes of data requires rapid data detection and response (DDR), so Bedrock includes built in alerts to prevent security and compliance violations from impacting the organization. Bedrock also allows organizations to implement a policy to detect such violations, ensuring that any potential issues are resolved quickly. The platform includes the remediation steps needed to resolve any violations and includes integration to ensure the SOC and any security orchestration, automation, and response (SOAR) solutions are always up to date on any issues. This provides the continuous capability to reduce mean time to detect/respond (MTTD/R).

> "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**

To achieve continuous data security, Bedrock is built on serverless architecture with dynamic policy enforcement, all designed for modern cloud environments. AIR uses Adaptive Sampling to crawl and assess massive quantities of data to understand data in a way that is both accurate and time and cost efficient. And to simplify policy enforcement in these complex environments, Bedrock allows organizations to set Trust Boundaries, which are effectively adaptive data perimeters, to make it simple for security teams to put policies in place and enforce them automatically.

STAGE 3: DATA SECURITY SURFACE MINIMIZATION

The final stage of data security layers on top of the foundation built in the previous two stages. With accurate risk assessment and remediation in place, combined with continuous data security, it's time to build on the foundation to minimize the data security surface and enable frictionless risk management.

As organizations build increasingly robust data security programs, it's best practice to seek to minimize the data attack surface proactively to reduce risk further. Bedrock enables this by identifying opportunities to reduce entitlement access to data (for example, adopting the principle of least privilege), minimize stale data (that is, find and remove unused or ghost data), harden data (for example, by masking data), and identify and protect core intellectual property (IP). Bedrock's AIR provides risk impact analysis and recommendations with AI-enabled fingerprinting and threat graphs, including identities and data context.

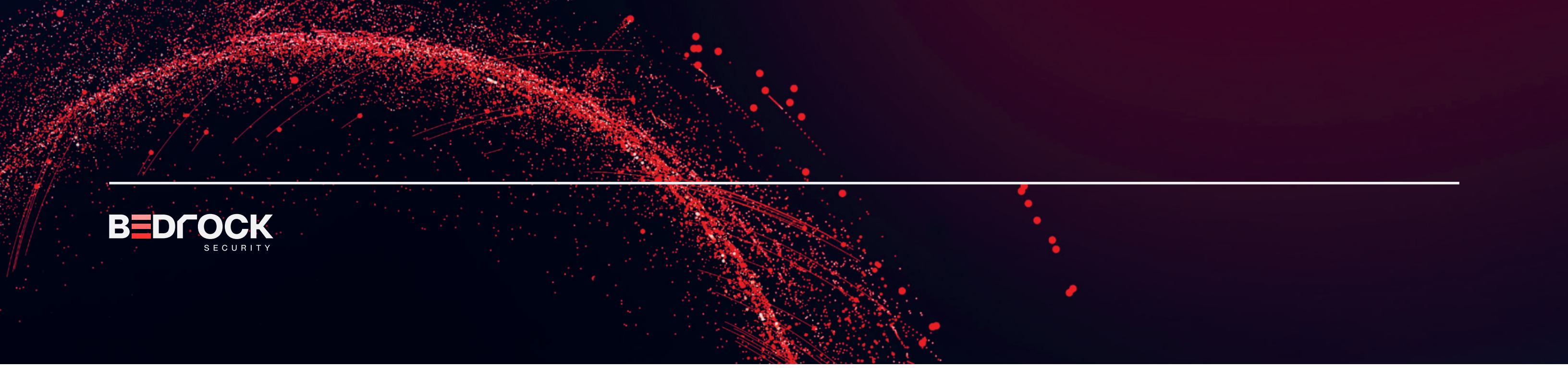
This approach removes any remaining friction between the CISO and lines of business, ensuring that data supports corporate goals, particularly in terms of protecting and tracking usage of the company's core IP.

Frictionless Data Security Today Is Business Success Tomorrow

Managing and securing data at scale is business-critical in the cloud and AI era. Legacy data security approaches, including DSPMs, are inadequate for dynamically and cost efficiently understanding and protecting data in cloud and AI environments. Organizations must adopt data security measures that seamlessly integrate with operations to enable more effective risk management and remediation. Bedrock Security developed AIR to deliver rapid, accurate risk assessment and response in a unified platform that allows an organization to understand all its data and business context, even as data volumes grow year over year. Built on serverless architecture, the Bedrock platform provides the scale and speed needed with the lowest operating expenditure (OpEx) to enable continuous security.

> “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**

Bedrock’s AIR increases accuracy by providing data visibility and mapping, helping organizations reduce their attack surface. And because the Bedrock platform is built on highly performant and efficient architecture, AIR can reduce MTTD/R, leading to lower risk for the organization. Bedrock enables organizations to build a holistic data security foundation that empowers organizations to embrace data sprawl without increasing risk.



About Bedrock Security:

Founded in 2021, Bedrock Security, the frictionless data security company, is headquartered in San Francisco and backed by Greylock Partners. The company is dedicated to revolutionizing data security in the cloud and AI era, leveraging advanced AI Reasoning to provide a comprehensive and frictionless approach. Bedrock Security's dynamic team, led by seasoned experts, is committed to delivering more than just security; they empower organizations to navigate the complexities of cybersecurity and harness the power of their data for sustained success.