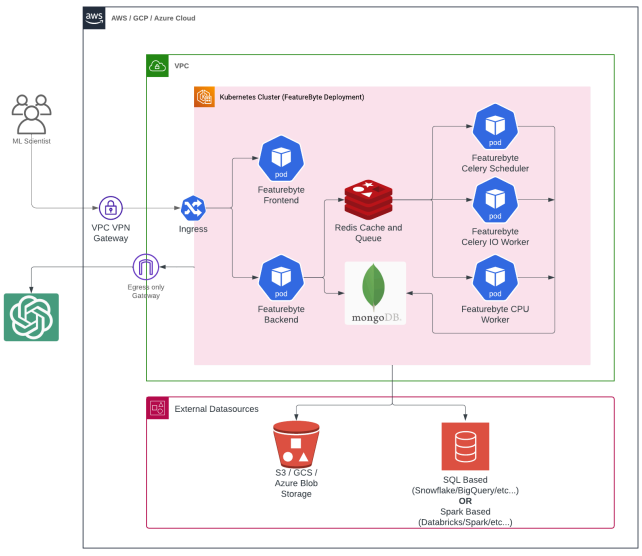
Secure by Design: FeatureByte's Approach to Data Privacy & Security

Introduction

In today's AI-powered world, the importance of data privacy and security is paramount. Enterprises have vast amounts of sensitive information to be processed and analyzed, and protecting that data is essential to customer trust, business operations, and compliance with industry regulations. Data breaches can have severe consequences, including financial loss, damage to reputation, and legal ramifications. Not surprisingly, data privacy and security are top concerns for data leaders. In a global survey of 300+ Chief Data Officers, 42% said that the security and privacy of data was a roadblock to implementing AI solutions.

At FeatureByte, we've built our platform with privacy and security at the core. This approach ensures that customer data remains protected at every step of its journey through advanced encryption, robust access controls, and stringent authentication protocols. By embedding security into the core of our platform, we provide our users with peace of mind, allowing them to focus on leveraging insights from their data without compromising confidentiality or integrity.

In this white paper, we will explore FeatureByte's approach to data privacy and security across five critical dimensions: Customer Data, Authentication Protocols, Data Access Control, Storage Encryption, and Source Code Security & Vulnerability Management.



1. Customer Data

When customers trust FeatureByte with their AI pipelines, our first priority is protecting their data, which is why data never leaves the customer's premises. We believe that customers should have full control over their data, so both the data and control plane of FeatureByte lives in the customer's environment. FeatureByte offers enterprise-grade data security and privacy that allows customers to define access policies, manage user permissions, and monitor usage. Through granular controls and audit trails, customers can ensure compliance with regulatory requirements and mitigate the risk of unauthorized access or data misuse.

Our support mechanisms are designed to operate without directly accessing sensitive information. Instead, we rely on activity logs and diagnostic tools to troubleshoot issues and provide assistance, ensuring that customer data remains confidential and secure. Most issues are resolved by reviewing customer logs from when an error occurred without access to customer data.

Admin accounts are essential for managing the security and configuration of the FeatureByte platform. We enforce strict access controls and authentication mechanisms to prevent unauthorized access to admin privileges. Additionally, access provisioning follows a least privilege principle, ensuring that users only have access to the resources and data necessary for their roles and responsibilities. More on that in section *3: Data Access Control*.

FeatureByte integrates seamlessly with authentication mechanisms, and external access can be managed through firewalls. By leveraging technologies that our customers trust to protect their data, we bolster the overall security of our platform and ensure comprehensive protection for customers' data.

2. Authentication Mechanisms

Authentication is the cornerstone of data security for any platform. Our user authentication workflow is designed to balance security and usability. FeatureByte supports a variety of authentication mechanisms, including Single Sign-On (SSO). These mechanisms ensure that only authorized users can access the platform and that their identities are verified securely.

To facilitate seamless authentication with external identity providers, FeatureByte

supports industry-standard frameworks such as OAuth2 and protocols such as OpenID Connect. This allows users to authenticate using their existing credentials from trusted identity providers, streamlining the login process and enhancing security.

Many organizations adopt Single Sign-On to secure access to digital services with better efficiency and security. This is achieved by delegating authentication to identity providers that manage user identities. By redirecting to an Identity Provider (IDP) using OAuth2 and OpenID Connect, FeatureByte can integrate seamlessly with a wide range of popular IDPs, including Google, Microsoft, and Okta. This allows organizations to easily integrate FeatureByte services alongside existing ones without compromising security or ease-of-access.

3. Data Access Control

Role-Based Access Control (RBAC) is a fundamental security principle that governs access to resources based on users' roles and permissions. FeatureByte employs RBAC to granularly manage access to data and features within the platform, ensuring that users only have access to the resources necessary for their roles and responsibilities.

Two types of roles are built into the FeatureByte platform: Admin and User. We understand that organizations have a wide range of roles and access needs, so Admins have the ability to set up custom roles within the FeatureByte environment to provision granular levels of permission.

At every step, we are committed to leveraging the systems and processes that our customers already use and trust, and RBAC is no exception.

When users connect FeatureByte to a data platform, such as Snowflake or Databricks, FeatureByte requires individual users to provide their access token; delegating access rights to the data platform's admin. Our platform is designed to prevent bypassing or circumventing access restrictions, ensuring that data access is granted only to authorized users and applications with the necessary permissions and credentials.

4. Storage Encryption

FeatureByte provides customers with the flexibility to bring their own encryption (BYOE) standards, allowing

them to encrypt data using their preferred encryption algorithms, key management practices, and cryptographic parameters. This ensures that customers maintain full control over the encryption process and can tailor security measures to meet their specific requirements.

Customers also have the autonomy to designate the encryption standards for all persistent storage resources, including Amazon S3 buckets, Google Cloud Storage, and Kubernetes Persistent Volume Claims (PVCs). This allows customers to enforce data encryption policies consistent with their organizational security policies and regulatory requirements, regardless of the underlying storage infrastructure.

FeatureByte employs strong encryption mechanisms to protect sensitive tokens, credentials, and cryptographic keys used for authentication, access control, and data encryption. These tokens are encrypted using randomized keys specific to each deployment, ensuring that sensitive information remains confidential and protected from unauthorized access or misuse.

5. Source Code Security & Vulnerability Management

FeatureByte conducts regular vulnerability scans of its source code repositories, leveraging automated static code analysis tools, software composition analysis (SCA) techniques, and manual code reviews to identify and remediate security vulnerabilities and coding errors early in the development lifecycle.

Container images used in FeatureByte deployments undergo rigorous vulnerability scanning and image integrity checks, leveraging vulnerability databases, security advisories, and threat intelligence feeds to identify and mitigate known vulnerabilities, configuration weaknesses, and software supply chain risks before deployment.

We employ dependency scanning tools and software composition analysis (SCA) techniques to identify and remediate known vulnerabilities, licensing issues, and third-party software risks within software dependencies, libraries, frameworks, and external components. By continuously monitoring and updating dependencies, we ensure that only secure and compliant software components are integrated into the platform.

FeatureByte seamlessly integrates container scanning into the deployment workflow using AWS Inspector, a fully managed security assessment service that automates the discovery, prioritization, and remediation of security vulnerabilities, configuration drifts, and compliance violations in containerized environments hosted on AWS.

To ensure that no vulnerabilities exist, FeatureByte undergoes annual penetration testing and security assessments conducted by independent third-party security firms. These tests evaluate the effectiveness of our security controls, identify potential vulnerabilities and attack vectors, and validate the platform's resilience against real-world threats and sophisticated cyber attacks.

Conclusion

Today, every company is a data company, and their data must be protected with the utmost care. FeatureByte remains committed to upholding the highest standards of data privacy and security with a comprehensive suite of security features, robust access controls, and advanced encryption techniques in place to safeguard customer data against unauthorized access, data breaches, and cyber threats.

We are dedicated to continuously enhancing our security posture and staying ahead of emerging threats, evolving regulatory requirements, and industry best practices to ensure the ongoing protection, compliance, and integrity of customer data.

For organizations seeking more information on our data privacy and security features, detailed documentation is available on our website.

We built FeatureByte with data privacy and security in mind. It is our goal to empower organizations to harness the full potential of their data while ensuring that sensitive information remains confidential, secure, and compliant with regulatory requirements. As threats evolve and security challenges become increasingly complex, we remain committed to partnering with our customers to address their unique security needs and deliver innovative solutions that enable them to thrive in a rapidly changing digital landscape.