Brim Security Whitepaper

Last updated: 18 August 2025

Executive Summary

At Brim, we understand that your data is crucial to your business. Our platform combines enterprise-grade security with innovative AI solutions to protect your information while helping your business grow. This whitepaper explains our comprehensive security measures in clear, straightforward terms.

Key Security Highlights:

- **Enterprise Security**: SOC 2 certification and ISO 27001 (expected December 2025 and January 2026)
- **Data Protection**: Advanced encryption for all data
- **Reliability**: 99.99% uptime guarantee
- **Quick Response**: Under 12-minute incident response time
- **Regular Updates**: Security patches within 24 hours

Table of Contents

Brim Security Whitepaper

Last updated: 18 August 2025

1. Introduction

At Brim, security is at the heart of everything we do. We protect your data using multiple layers of security while making our platform user-friendly and easy to access. We believe that security is essential for success in today's digital landscape. This whitepaper outlines our security measures and the steps we take to ensure your data is safe and protected.

Key Security Principles
We follow industry-best practices to protect your data:

- **Zero Trust**: We verify everyone, every time.
- **Defence in Depth**: Multiple layers of protection.
- **Least Privilege**: Access is restricted to what is absolutely necessary.
- **Security by Design**: Security is integrated into every part of the system.
- **Continuous Monitoring**: We always watch for potential threats and vulnerabilities.

2. Security Standards and Certifications

We maintain the highest security standards in the industry to ensure that your data is fully protected. Brim complies with a range of globally recognised certifications, and we are committed to ensuring that we meet or exceed these standards at all times.

Current Certifications:

- **GDPR**: We comply with European privacy regulations and have implemented robust measures to protect personal data.
- **SOC 2**: We are in the process of becoming SOC 2 certified, with full certification expected by **December 2025**.
- **ISO 27001**: We are in the process of becoming ISO 27001 certified, with full certification expected by **January 2026**.
- **CCPA**: We are working towards full compliance with the California Consumer Privacy Act (CCPA), with full compliance expected by **December 2025**.

Certification Timeline

- **GDPR**: Fully compliant
- **SOC 2**: Expected completion in **December 2025**
- **ISO 27001**: Expected completion in **January 2026**
- **CCPA**: Full compliance expected by **December 2025**

3. Understanding Brim's Security

Brim's platform is designed to provide businesses with AI-powered solutions, while also ensuring that your data is safe. We have designed our architecture with security in mind, following best practices and robust protection measures to ensure your data remains private and secure.

Security Architecture
Our security measures cover every level of our system, from edge security to data protection. The key components include:

- **Edge Security**: We use advanced firewall protection and DDoS mitigation to prevent attacks before they can reach the platform.
- **Application Security**: Secure development practices, regular security testing, and vulnerability scanning ensure that our applications remain secure.
- **Data Security**: We protect your data using **AES-256 encryption** for data at rest and **TLS 1.2+ encryption** for data in transit. Secure key management ensures that sensitive data is encrypted and protected from unauthorised access.

4. Partner Security Management

At Brim, we carefully choose our partners to ensure they meet the same high security standards we follow. Our partners are required to comply with relevant certifications, including **ISO 27001** and **SOC 2 Type II**. We perform regular security assessments and maintain strict confidentiality agreements to ensure that your data remains secure, even when shared with third parties.

5. Business Continuity

We understand that business continuity is critical. If something goes wrong, we ensure that you can quickly recover with minimal disruption.

Key Continuity Measures:

- **Backups**: We conduct daily automated backups, retaining data for **30 days**.
- **Disaster Recovery**: We have a **Recovery Time Objective (RTO)** of **4 hours** and a **Recovery Point Objective (RPO)** of **15 minutes**.
- **Uptime Guarantee**: We guarantee **99.99% system availability**, ensuring that the platform is always accessible when you need it.

6. Information Security Measures

Brim's platform employs multiple layers of security to safeguard your data. These layers are designed to provide comprehensive protection across all aspects of the platform, from encryption to access management.

Key Security Controls:

- **Data Encryption**: We use **AES-256** encryption for data at rest and **TLS 1.2+** for data in transit.
- **Access Management**: We require **multi-factor authentication** and employ **role-based access control** to ensure that only authorised users can access sensitive data.

- **Security Monitoring**: Our 24/7 monitoring systems provide real-time threat detection and alert our security team to potential risks.
- **Data Storage Minimisation:** We follow a strict data minimisation approach. We only store data when absolutely necessary, and our standard practice is to avoid retaining personal data whenever possible. Typically, data is stored by our customers, not by Brim. For most of our operations, we store only metadata—such as logs or usage data—not the actual content or personal data, ensuring minimal data retention. This approach helps reduce exposure and enhances privacy protection.

7. Access Control Systems

We implement strict access controls to ensure that only authorised individuals can access sensitive information.

Key Features:

- **Multi-Factor Authentication (MFA)**: This adds an extra layer of protection to user accounts.
- **Role-Based Access Control (RBAC)**: Users are granted access only to the data they need to do their job, ensuring the principle of least privilege is followed.

8. Risk Management

At Brim, we actively identify and mitigate security risks before they become threats. We use a combination of regular testing, vulnerability management, and continuous monitoring to ensure our platform remains secure.

Key Risk Management Practices:

- **Regular Testing**: We perform regular security scans, regular penetration tests, and annual security audits to identify vulnerabilities.
- **Vulnerability Management**: We rapidly patch vulnerabilities and continuously update our systems to address emerging threats.

9. Security Operations

Our security team is always on alert to detect and respond to potential threats. We ensure that any security incidents are quickly identified and addressed using AWS (Amazon Web Services) and GCP's (Google Cloud Platform) global leading security capabilities. These platforms provide us with industry-leading tools and infrastructure that ensure the highest level of protection and scalability for your data.

Key Security Operations:

- **Real-time Monitoring**: Leveraging AWS and GCP's extensive monitoring systems, we continuously scan the platform 24/7 for any signs of malicious activity. Both platforms offer advanced threat detection and anomaly monitoring to help us respond quickly.
- **Incident Response**: In the event of a security issue, we utilise AWS and GCP's global incident response capabilities, which provide immediate, automated alerts and support to help our dedicated incident response team act quickly and minimise any potential impact on your business.

10. Staff Security Programme

Security awareness is crucial to maintaining a secure environment. Brim's staff security programme leverages both **AWS** and **GCP**'s training and security services to help us stay ahead of emerging threats.

Staff Security Training:

- **Initial Security Orientation**: All employees receive training on our security policies and procedures, supported by **AWS** and **GCP**'s best practice guidelines.
- **Ongoing Security Training**: Regular updates, phishing simulations, and security awareness programmes help keep our team sharp and aware of evolving threats, using the latest tools and threat intelligence provided by AWS and GCP.

11. Security Metrics

We track key performance indicators (KPIs) to measure the effectiveness of our security efforts, ensuring we meet our security goals with the help of AWS and GCP's global capabilities for security monitoring and data analytics.

Key Metrics:

- **System Uptime**: **99.99%** (target) – Achieved with **AWS** and **GCP**'s globally distributed infrastructure, ensuring high availability.
- **Incident Response Time**: **<15 minutes** (current average: **12 minutes**) – Supported by **AWS** and **GCP**'s automated incident response systems.
- **Security Patch Implementation**: **<24 hours** (current average: **18 hours**) – Using **AWS** and **GCP**'s tools, patches are implemented swiftly across our systems.

12. Industry Solutions

We provide specialised security solutions tailored to different industries, ensuring we meet the unique requirements of each sector. By leveraging **AWS** and **GCP**'s industry-leading tools, we can offer robust, scalable, and compliant solutions for businesses in financial services, healthcare, and technology.

- **Financial Services**: Enhanced encryption, extended audit logging, and custom compliance reports, all supported by **AWS** and **GCP**'s secure infrastructure.
- **Healthcare**: HIPAA compliance, patient data protection, and enhanced access controls, with **AWS** and **GCP**'s secure and compliant cloud services.
- **Technology**: API security, cloud protection, and DevSecOps integration, built on **AWS** and **GCP**'s secure, flexible cloud platforms.

13. Common Questions

How do you keep our data safe?
We use multiple security layers, including strong encryption, access controls, continuous monitoring, and regular testing, to ensure your data is secure.

Can others see our data?
No. Your data is private and only accessible by authorised users based on the roles and permissions you've set.

What happens if there's a problem?
We have a rapid response plan in place. In the event of an issue, we will notify you immediately, deploy our response team, and provide regular updates as we resolve the problem.

14. Contact Information

If you have any security-related questions or concerns, please don't hesitate to reach out to us.
Website: www.joinbrim.ai
Security Contact: security@joinbrim.ai