blancco

Reduce Risk.
Increase Efficiency.
Be Sustainable.™

Security Overview

Blancco Management Portal (BMP)

rev 2023.07

Contents

Introduction

Blancco's Business

We provide organizations with secure, compliant, and automated solutions that accelerate the transition to the circular economy. Blancco operates in three main go to market segments: Enterprise, Mobile and IT Asset Disposition (ITAD). We offer several erasure and diagnostics products to cater for these markets. Our customers use our products to erase or diagnose several types of it assets such as – hard drives, laptops, smartphones, tablets, desktops, servers, usb flash drives, etc.

Scope

This document will discuss various security aspects of BMP. BMP was built from the ground up to be the most secure platform for managing Blancco products. Whether its secure architecture based on an AWS platform, user authentication, data encryption, secure data storage, backup/restore, or logs, all security aspects have been covered in BMP and will be explained in this document.

Blancco Management Portal (BMP)

Easily access and monitor reports, notifications, and certificates at any time with BMP. Organizations can use BMP to manage erasure & diagnostic reports, distribute licenses across global locations, and manage users from one centralized point of control with tamper-proof reports available for auditing as well as Sustainability Dashboards and ESG (environmental, social and governance) calculators helping you to hit your CSR (Corporate Social Responsibility) goals.

Extensive Capabilities:

- Complete cloud-hosted service for erasure & diagnostics operations
- Full compatibility with all Blancco data erasure software
- Easy user management and global distribution of user rights
- Comprehensive reports include details such as device name and model, IMEI code, and storage capacity
- Reports exportable as PDF, XML, and CSV
- Uses AWS (Amazon Web Services) to allow scaling and faster searches of reports
- Back up incoming reports directly to the cloud for future reference
- Full transparency of both diagnostics and erasure processes ensures a gapless audit trail
- Multiple supported languages

Security Focus

Resource Focus

We have a dedicated security team who deal with various aspects of security. Security is not an afterthought but a strong consideration right from design stage to delivery. Every new feature is thoroughly evaluated by the security team.

Product Focus

BMP has been designed from the ground up with security in mind. **Security considerations have been taken into account at various layers of the product:**

1. Infrastructure
   a. We use the best-in-class cloud provider – AWS
   b. We use EC2 instances, firewalls & load balancers
2. Web
   a. HTTPS
   b. SSL/TLS
3. Data
   a. AES 256-bit encryption

Policies, Certifications & Standards

- Blancco strives to use best polices, certification and standards
- We are ISO 27001 and ISO9001 certified across the organization
- We are in the process of going through SOC 2 Type 2 certification for BMP
- Our erasure products have earned several security certifications such as ADISA, etc. Our Certifications

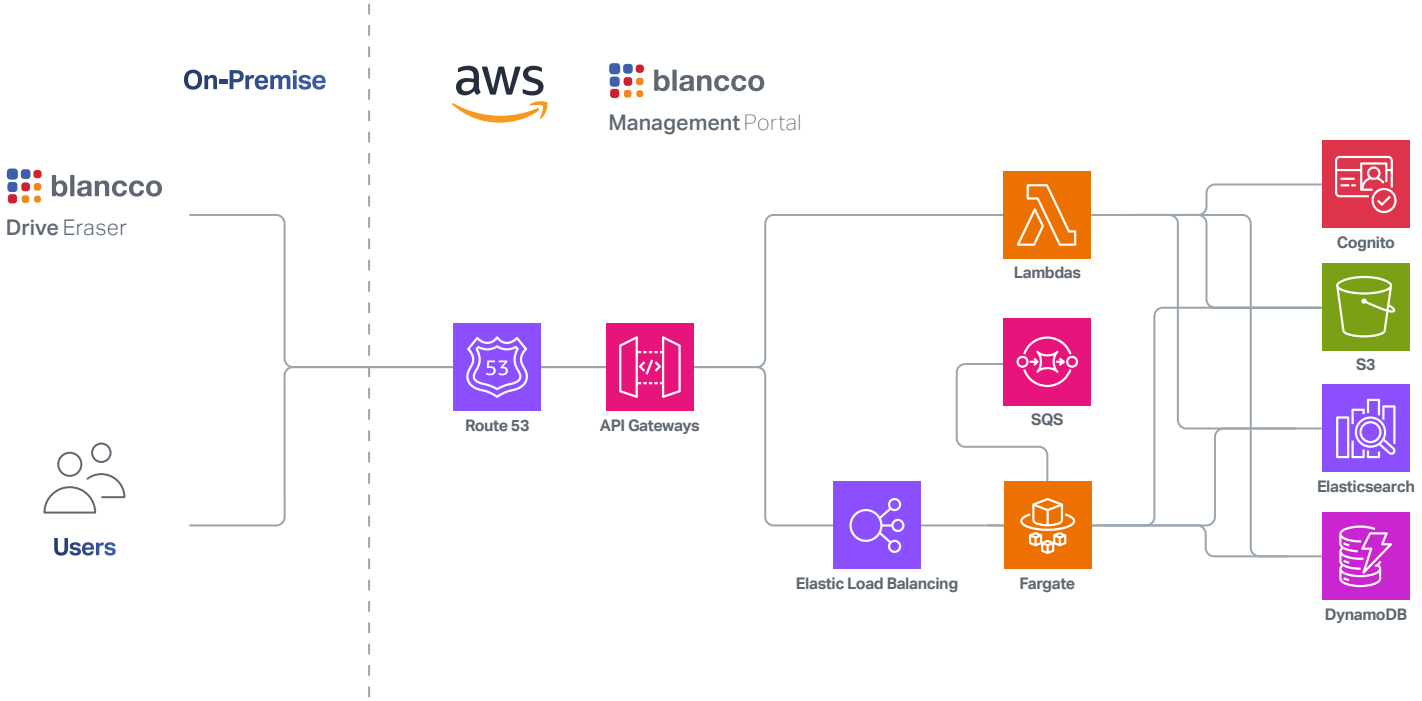
Product Architecture

BMP is a cloud application based on Amazon Web Services (AWS) infrastructure.
The diagram below shows the high-level architecture and components used:

BMP is deployed in a standard AWS region (EU/IRE). Optional region choices are available at additional cost.

Infrastructure includes the following layers:

1. Routing
2. Access Layer
3. Computer Layer
4. Storage Layer



As depicted in the diagrams above, BMP uses a layered architecture based on AWS technologies.

The following programming languages and data storage environments are used:

1. Python
2. Java
3. DynamoDB
4. AWS S3
5. Elastic Search

Personal Information / CPI

The BMP holds erasure & diagnostics report data such as asset identifiers, make, model, device types, erasure standards used, erasure result, diagnostics tests performed, diagnostics results, etc.

The customer (known as tenant in BMP), will have a unique sandboxed account. Each account has at least one Manager User and other type of Users. User basic data such as Name and Email are stored for user login and role management purposes. Data is encrypted at rest. No other personal information will be stored.

Blancco follows industry leading security practices. In the unfortunate event of a data breach, we will immediately inform the affected customers, provide mitigations in the short term and permanent solutions as soon as possible.

Identity & Access Management

BMP in a multi-tenant system hosting various customers.

The Key Features Of Access Management:

- Every customer has their own isolated environment which is accessible only by them or Blancco personnel if needed.
- An individual user account is required to use the system.
- Every user account is identified by a unique verified email address and belongs to a single tenant.
- Every user has a role which defines their authorities within tenant.
- User actions are logged for review purposes.

Default Roles:

1. **Manager User:** Has to be present for every Tenant and will have all privileges that a tenant can have.
2. **Basic User:** Has view privileges but cannot delete content – users / reports.
3. **Auditor:** Has limited view privileges only.

In the future, BMP will have custom role capabilities and will allow tenants to define their own roles. More information will be provided on that when available.

Password Rules:

BMP user login password requires:

- minimum 10 characters
- at least 1 upper letter
- at least 1 lower letter
- at least 1 number and
- at least 1 symbol

User Creation API

BMP offers an API to create users under a tenant. Login to your BMP account to see a complete guide on how this API works.

Single Sign On

BMP will support single sign on later this year. We will be adding support for SAML and OAuth 2.0.

Blancco Access To Tenant Data

Blancco strictly restricts the access to production customer data to the following users:

The Key Features Of Access Management:

- **Sales operations:** to onboard a customer to BMP, assign licenses and create manager user.
- **Support:** a few supports personal will have access to BMP to provide support such as troubleshooting, create/modify users on behalf of customers, reset passwords etc.
- The Blancco development team and other Blancco personnel do not have access to BMP production data.

Audit Log Management

All relevant user actions are logged in audit log. Audit logs leave a traceable trail (timestamps) detailing who did what and when. Audit logs are capture for all users including managers and administrators. Audit logs do not expire and are accessible to a restricted group of Blancco staff. Audit logs can be requested by contacting Blancco Support in the event of a security incident.

Audit log example: login

Example of events captured in logs:

1. Action: User Login
2. Tenant ID: alphanumeric
3. Username: abc@email.com
4. IP: XX.XX.X.XXX

Audit log example: report viewing

1. **Data:**
   a. **Report ID:** alphanumeric
2. **Tenant ID:** alphanumeric
3. **IP:** XX.XX.X.XXX
4. **Action:** View Erasure Report
5. **Username:** abc@email.com

Backup And Recovery

BMP data is being backed up and replicated on a separate AWS account on their respective regions. Backed up data can be retrieved and restored to a live system if needed.

This is integrated into the Blancco Business Continuity Plan (BCP) plan, and which is separated from the corporate database. Annual disaster recovery testing is conducted to ensure backup & recovery is functioning as expected.

Main details:

- Recovery Point Objective (RPO): 1 hr
- Recovery Time Objective (RTO): 4 hrs
- Backup encryption: AES-256
- Backup expiration: TBD

Uptime:

BMP uptime is 100% since the measurement started in June 2023. We will be adding a 3rd party tool for monitoring uptime shortly.

Change Control Management

Any changes of the system go through the normal development lifecycle. New features or bug fixes are reviewed, designed, developed and verified by the product team before any changes are deployed to production. Different isolated environments are used to ensure proper development and quality of changes. Quality gates with manual approvals are used to manage transitions of changes between environments.

Any changes in the system are verified and approved by the:

- Product Manager
- Technical lead
- Quality lead

The builds and deployments of the product are automated with CI/CD pipelines and deployment of updates do not require human intervention after manual approval of changes. Cloud Operations of this product is a shared responsibility of the Infrastructure and the Development team. The infrastructure team are responsible for providing the account and monitoring whereas the Development Team are responsible for deployment and management.

Cloud Security & Monitoring

Application logs and audit logs are stored in AWS CloudWatch. Logs and additional metrics are used to monitor system behaviour.
Additionally, the following security aspects are monitored:

Concept	Status	Implementation
DDoS protection	**OK**	AWS Shield
Disaster recovery	**OK**	
High Availability (HA)	**OK**	Micro service architecture with load balancing is in use. At least two (2) of each service instances are always available.
Intrusion Detection and Prevention (IDS/IPS)	**OK**	AWS GuardDuty
Vulnerability management	**OK**	AWS Inspector

Encryption

- Data is encrypted both in rest and in flight.
- HTTPS communication with the system is enforced with TLS v1.3.
- AES-256 encryption is used with data persistence.

Firewall

Application Load Balancer configuration

By default, load balancers do not allow any unmapped communication to pass through.

AWS Shield

AWS shield provides protection against Distributed Denial of Service (DDoS) attacks.

Infrastructure Security

All data is processed within isolated private networks. Data persistence and communication utilize encryption.

Intrusion Detection / Prevention

Amazon GuardDuty is used as a cloud Intrusion Detection service.

Vulnerability Management

Vulnerabilities are monitored with:

- Amazon Inspector for vulnerability management
- Amazon GuardDuty for threat detection / malware (cloud centric IDS)
- Automatic security scans
- Manual penetration testing

Patch Management

All the security related findings are categorised as Critical/High/Medium/Low and are immediately assessed by the development team. Any critical identified vulnerabilities are addressed without delay and pushed through change control with the highest priority.

Risk Management

All the associated risks are updated to the Risk Register and followed up on the monthly risk register review.

Application Programming Interface (API)

The Support section in BMP has a guide that explains the API's general concepts, describes all the endpoints, and provides technical documentation at the end.

Available endpoints are as follows:

- Export report
- Export reports (GET)
- Export reports (POST)
- Create users (POST)

Incident Response And Support

Blancco uses a service desk ticketing system to capture and respond to customer issues. These issues are further assigned to the R&D Team. Issues are immediately assessed by the R&D Team and depending upon the severity of the issue (Blocker, Critical, High, Medium, Low), a fix is planned and released.

Use our Support Portal to report incidents regarding BMP issues, availability, security or general questions: **support.blancco.com**

Customers are encouraged to submit any vulnerabilities found to Blancco using incident management **guidelines**.

If a support ticket is created, the outcome will be one of two scenarios:

- ☑ Support engages IT
- ☑ Support engages Development