Blitz Information Security

(470) 747-9992

750 B Street Suite 3300,
San Diego CA, 92101

www.blitzrocks.com

Security Overview

Blitz was designed and implemented following security best practices. Our data is encrypted and stored in a highly secure location. Our users are authenticated prior to accessing Blitz and our algorithms validate that they have permissions to see the data they are requesting. All data is transferred through secure channels and we conduct periodic testing to validate that our system remains secure.

We strive to keep up to date with Microsoft's documented best practices for cloud applications and apply them as much as possible to Blitz's design, implementation, and operations.

Data Center Security

Microsoft datacenters employ controls at the perimeter, building, and computer room with increasing security at each level, utilizing a combination of technology and traditional physical measures.

- Security starts at the perimeter with camera monitoring, security officers, physical barriers and fencing.
- At the building, seismic bracing and extensive environmental protections protect the physical structure and integrated alarms, cameras, and access controls (including two-factor authentication via biometrics and smart cards) govern access. The systems are monitored 24x7 from the operations center.
- Similar access controls are used at the computer room, which also has redundant power.

Password Requirements

For application access, our passwords requirements are the following:

- Minimum length: 8 characters
- Required numerical characters: 1
- Required lower case characters: 1
- Required upper case characters: 0
- Required special characters: 0

SOC Levels

Microsoft Azure offers the following SOC compliance:

Compliance: We conform to global standards

Azure meets a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards like Australia IRAP, UK G-Cloud, and Singapore MTCS.

Rigorous third-party audits, such as by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate. As part of our commitment to transparency, you can verify our implementation of many security controls by requesting audit results from the certifying third parties.

(470) 747-9992

750 B Street Suite 3300,
San Diego CA, 92101

www.blitzrocks.com

When Microsoft verifies that our services meet compliance standards and demonstrates how we achieve compliance, that makes it easier for customers to secure compliance for the infrastructure and applications they run in Azure.
Source: https://azure.microsoft.com/en-us/support/trust-center/

SOC 1, 2, and 3 Reports

Microsoft has achieved SOC 1 Type 2, SOC 2 Type 2, and SOC 3 reports. In general, the availability of SOC 1 and SOC 2 reports is restricted to customers who have signed nondisclosure agreements with Microsoft; the SOC 3 report is publicly available.
Source: https://www.microsoft.com/en-us/trustcenter/compliance/soc

MongoDB Atlas meets the following standards:

Does MongoDB Atlas meet compliance standards that test for data safety, privacy, or security?

Service Organization Control (SOC) Reports are independent third-party examination reports that demonstrate how the MongoDB Atlas service achieves key compliance controls and objectives. The purpose of these reports is to help you and your auditors understand the controls established to support operations and compliance.

A Type 1 SOC 2 Report: Security was completed on May 31st, 2017.

MongoDB, Inc. is also certified under the EU-US Privacy Shield. View the certification here. MongoDB Atlas infrastructure runs on top of Amazon Web Services, Microsoft Azure, and Google Cloud Platform; each cloud provider undergoes its own series of independent third-party audits on a regular basis.

Learn more about cloud compliance on Microsoft Azure

Learn more about MongoDB Cloud Services Compliance.

Source: https://www.mongodb.com/cloud/atlas/faq

Network Security

Given that our solution is completely hosted in the cloud, it leverages all Microsoft Azure's high-level network security practices to defend itself from attacks. Official documentation on this topic can be found here: https://docs.microsoft.com/en-us/azure/best-practices-network-security.

Regarding the design of Blitz itself, our focus on using Platform-as-a-service components and the fact that these are all fully managed by our providers mean that there are less things that we need to concern ourselves with. E.g. Azure App Services by design only exposes ports 80 and

443 for HTTP and HTTPS traffic, respectively, and we only use HTTPS throughout the application.

Any resources that we require and that need to be managed by us (e.g. a VM to run load/stress tests) are deployed in (Azure's) virtual networks, which we setup completely independently for each environment and leveraging Azure's Network Security Groups, so only the traffic that we deem necessary can make it into (or out of) those networks.

Data encryption and protection

Data stored in Blitz is automatically encrypted. The following summary provides more details about the security strategy followed by MongoDB Atlas.

MongoDB Atlas is security hardened by default.

Each MongoDB Atlas group is provisioned into its own VPC, thus isolating your data and underlying systems from other MongoDB Atlas users. Network encryption and access control are configured by default, and IP whitelists allow you to specify a specific range of IP addresses against which access will be granted. All security-specific updates to the operating system and database of the underlying instances are automatically applied by MongoDB engineers.

For deployments running in Azure and GCP, storage volumes are automatically encrypted.

Read the MongoDB Atlas Security Controls white paper for more information about MongoDB Atlas security and data security.

Penetration Testing

We conduct quarterly penetration tests using OWASP approved tools to validate the security of our application, with a focus on OWASP's Top 10. Results of our tests can be provided upon request.

In addition to our own penetration testing, Microsoft constantly tests the whole Azure platform with things such as:

- Port scanning and remediation.
- Perimeter vulnerability scanning.
- Network level DDOS (Distributed Denial of Service) detection & prevention.
- A proactive strategy called **Assume Breach**, where internal teams simulate real-world attacks at the network, platform, and application layers, and separate teams identify and remediate any vulnerabilities found.

Blitz Security Audits

The information security policy is a key component of **Blitz** overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

Objectives

The objectives of **Blitz** Information Security Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

Policy Framework

Management of Security

- At board level, responsibility for Information Security resides with the IT & Support Manager
- Blitz's Cloud Services Delivery Manager is responsible for implementing, monitoring, documenting and communicating security requirements for the organization.

Asset Security and Protection

- Prior to create, disable or modify information system accounts including privileged and vendor accounts the IT & Support Manager must authorize it.
- Passwords to access Blitz networks, applications and for the user accounts must be complex and are changed every 45 days.
- Multi Factor Authentication is required to access Blitz cloud related applications.
- Remote access to Blitz's network is restricted only through Virtual Private Network.
- Blitz has different network segments, flow control policies and restricts the transfer of sensitive information within its network to protect sensitive data
- The information is protected by using encryption in Blitz's desktops, laptops, serves and data processed, stored or managed via cloud services.
- Blitz has commercial grade boundary protection tools such as firewalls.
- Security patches are applied in a monthly basis within 30 days as they become available.
- All new products are tested and assessed for privacy security issues.

Contracts of Employment

- All contracts of employment contain a confidentiality clause that must be acknowledged and signed by the new employees.

Access Controls

- Blitz has access control devices for the restricted areas containing information systems or stored data.

Application Access Control

- Access to the data, system utilities, program source libraries, information systems including on mobile devices is defined based on business requirements and their roles and users in the organization and their ecosystem (employees & partners).

Information Risk Assessment

- Information Security risks is managed on a formal basis. An Incident Report is created and reviewed at regular intervals; action plans should be put in place to effectively manage those risks. These reviews will serve to identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

Information security events and weaknesses

- All information security events and suspected weaknesses are reported to the Cloud Services Delivery Manager. All information security events are investigated to establish their cause and impacts with a view to avoiding similar events.

Classification of Sensitive Information.

Sensitive information is classified in two different levels:

I. Restricted

- Social security number
- Bank account number
- Driver's license number
- Phone numbers
- Personal home address.
- Passport information.

Sharing of Restricted information within the company may be permissible if necessary to meet the Company's legitimate business needs. Any sharing of Restricted information within the Company must comply with Company policies.

II. Confidential

Company Information is classified as Confidential if it falls outside the Restricted classification but is not intended to be shared freely within or outside the Company due to its sensitive nature and/or contractual or legal obligations. Examples of Confidential Information include all non-restricted information contained in personnel files, misconduct, improvement action plans, compensation reviews, 360 evaluations, internal financial data, certification records, client information.

Any sharing of Confidential information within the Company must comply with the Company policies.

Protection from Malicious Software

- Antivirus applications are implemented, updates are released to all devices within 24 hours.
- Antimalware application is configured to continuously scan or to perform periodic scans of the information systems, including files from external sources.

User media

- Removable media of all types that contain software or data from external sources, or that have been used on external equipment, are restricted from being used in Blitz's equipment.
- Users breaching this requirement may be subject to disciplinary action.

Monitoring System Access and Use

An audit trail of system access and data use by staff is performed on a yearly basis. Blitz has in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right monitor activity where it suspects that there has been a breach of policy.

System Change Control

- Changes to information systems, applications or networks shall be reviewed and approved by the IT & Support Manager.

Intellectual Property Rights

- All information products are properly licensed.
- All employees are expected to co-operate fully with this policy. Users shall not install software on the organization's property without permission from the IT & Support Manager.
- Users breaching this requirement may be subject to disciplinary action.

Azure and Mongo DB Security Audits

Additional to our periodic reviews, we also benefit by the security audits performed by our software providers:

Microsoft Azure

SOC Levels

Microsoft Azure offers the following SOC compliance:

Compliance: We conform to global standards

Azure meets a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards like Australia IRAP, UK G-Cloud, and Singapore MTCS.

Rigorous **third-party audits**, such as by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate. As part of our commitment to transparency, you can verify our implementation of many security controls by requesting audit results from the certifying third parties.

When Microsoft verifies that our services meet compliance standards and demonstrates how we achieve compliance, that makes it easier for customers to secure compliance for the infrastructure and applications they run in Azure.
Source: https://azure.microsoft.com/en-us/support/trust-center/

SOC 1, 2, and 3 Reports

Microsoft has achieved SOC 1 Type 2, SOC 2 Type 2, and SOC 3 reports. In general, the availability of SOC 1 and SOC 2 reports is restricted to customers who have signed nondisclosure agreements with Microsoft; the SOC 3 report is publicly available.
Source: https://www.microsoft.com/en-us/trustcenter/compliance/soc

Mongo DB Atlas

MongoDB Atlas meets the following standards:

Does MongoDB Atlas meet compliance standards that test for data safety, privacy, or security?

Service Organization Control (SOC) Reports are independent third-party examination reports that demonstrate how the MongoDB Atlas service achieves key compliance controls and objectives. The purpose of these reports is to help you and your auditors understand the controls established to support operations and compliance.

A Type 1 SOC 2 Report: Security was completed on May 31st, 2017.

(470) 747-9992
750 B Street Suite 3300,
San Diego CA, 92101
www.blitzrocks.com

MongoDB, Inc. is also certified under the EU-US Privacy Shield. View the certification here. MongoDB Atlas infrastructure runs on top of Amazon Web Services, Microsoft Azure, and Google Cloud Platform; each cloud provider undergoes its own series of independent **third-party audits** on a regular basis.

Learn more about cloud compliance on Microsoft Azure

Learn more about MongoDB Cloud Services Compliance.

Source: https://www.mongodb.com/cloud/atlas/faq

(470) 747-9992

750 B Street Suite 3300,
San Diego CA, 92101

www.blitzrocks.com

Single Sign-On Requirements

Blitz integrates with Azure AD to authenticate and manage users for our enterprise customers. Other Single Sign-On providers are supported based on customer requirements. The following diagrams illustrate how Blitz could work with Azure B2C and Ping Identity:

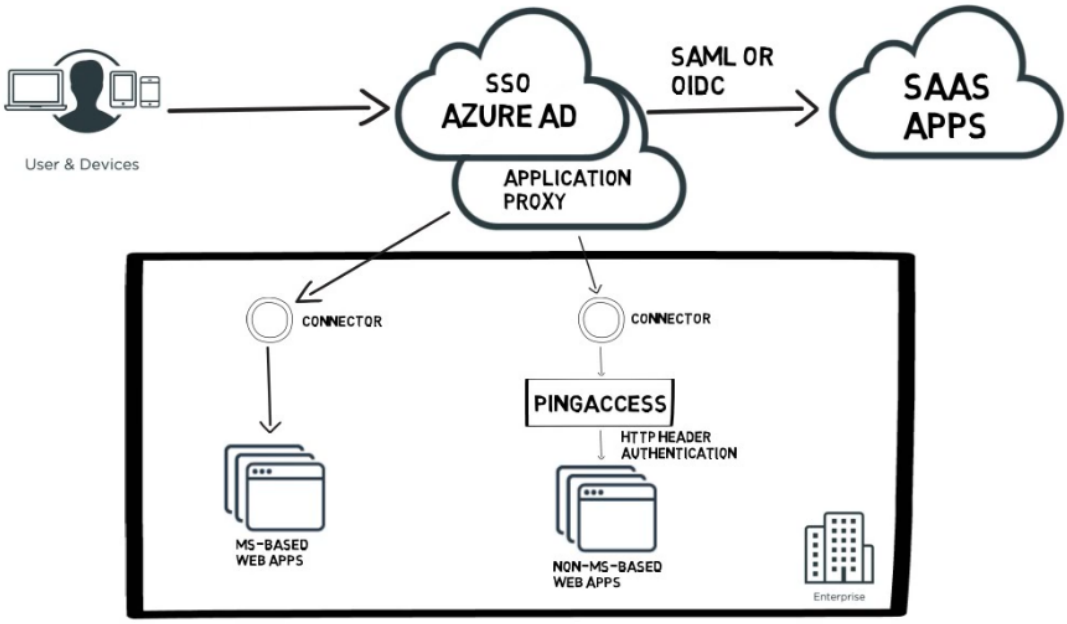
PingAccess

PingAccess is a solution result of the partnership between Microsoft and Ping Identity that integrates Azure AD and PingAccess. This solution allows the authentication to Azure AD and have SSO access for non-Microsoft based legacy on-premises applications without the need of VPN.

How does it work

PingAccess on-premises needs to be installed, Azure AD application proxy configured and then the applications can be integrated.

When a user accesses an on-premises application, PingAccess reaches out to Azure AD, gets an OpenID Connect (OIDC) token and translates it to the appropriate proprietary header that is expected to grant or deny access.



Azure AD B2C

Azure AD B2C is a cloud identity management service that allows to connect to any customer. Enables to customize and control how customers with external users sign up, sign in and manage their profiles when using our applications.

How it works

Customers can access our applications using their existing social accounts, personal emails or local accounts.

Basically, there are 3 steps needed in the B2C tenant:

1. Register application
2. Authenticate users
3. Grant access

Blitz can be configured to support this framework.

(470) 747-9992

750 B Street Suite 3300,
San Diego CA, 92101

www.blitzrocks.com