Data Security + Brightly: Top 10 FAQs for IT departments

AWS benefits:

- Guaranteed availability
- Predictable total cost of ownership
- Instant elasticity/scalability
- Real-time monitoring
- Regularly delivered/vendor managed
- Data redundancy
- Data durability
- Data security
- Faster deployments

1. What are all inbound and outbound firewall requirements to connect to and use your product?

There are no inbound firewall requirements. All application communication is over http and https ports (80 and 443).

If your organization filters outbound traffic you will need to allow port 80 and 443 traffic access to *.brightlysoftware.com.

2. Where is your application hosted?

Brightly uses multiple availability zones in the AWS US-East-1 region (Northern Virginia).

3. What are the security certifications and policies in place for your data center infrastructure and your organization?

Brightly hosts our SaaS (software as a service) applications in highly secure and available AWS data center infrastructure. AWS regularly achieves third-party validation for thousands of global compliance requirements that are continuously monitored to meet security and compliance standards across all types of businesses. The standards supported by AWS include PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping satisfy compliance requirements for virtually every regulatory agency around the globe.

Brightly’ information security policy framework is based on the ISO/IEC 27001:2013 Information Security Management standards and addresses controls appropriate to insure the confidentiality, integrity, and availability of client data. Our security policies and procedures are based on security best practices such as frequent user security training, regular security patching, defense in depth, and least permissions access. We use the Cloud Security Alliance (CSA) Security Trust Assurance and Risk (START) program to assess and validate our security practices. In addition, annual HIPAA and PCI Data Security Standards assessments are performed. Brightly is registered under the EU-US Privacy Shield framework.

4. Does Brightly always encrypt client data?

All user communication with Brightly applications is via securely encrypted TLS/SSL (TLS v1.2 minimum) communication channels (https). Brightly uses the most current technology for our SSL certificates: 2048 bit key, SHA-2 signature algorithm, and industry standard CA providers. Insecure cipher keys are not used. All services within the AWS infrastructure encrypt data in motion using AWS’s proprietary TLS implementation.

All client data at rest is encrypted using the Advanced Encryption Standard (AES) with 256-bit keys (AES-256). It’s the strongest industry-adopted and government-approved algorithm for encrypting data. We use the AWS Key Management Service (KMS) to ensure that the keys used for data encryption are also protected at rest and have a separate access management system from access to client data. KMS is based on an AWS's fleet of hardware security modules (HSM) which contain security controls to prevent encryption keys form leaving the device in a way that could allow unauthorized access.

5. What are your data privacy policies?

Brightly protects the privacy of client data using a layered defense-in-depth approach to information security. Brightly has adopted security policies and implemented company-wide information security training to protect the privacy of client data. By policy, Brightly employees are prohibited from disclosing information obtained from clients to any other person or entity except in the performance of services for the client and only when the release of the information is authorized by the client.

Brightly' Legal and Information Security teams supports our data privacy management. We keep current on privacy and security laws and regulations to maintain a data privacy program aligned with changing requirements. These high-level policies are reviewed and approved by executive management. In addition to maintaining written policies, Brightly requires annual data privacy awareness training program for all employees.

Brightly' data privacy policy is available online - https://www.brightlysoftware.com/privacy. We will never share, sell, or distribute data that specifically identifies your organization. We may offer services that allow you to view "average" or aggregated data from other clients, but this data will never be specifically identified to you or your organization.

Brightly complies with the European Union's Global Data Protection Regulation (GDPR). Brightly is register under the Privacy Shield Framework. The Privacy Shield Principles lay out a set of requirements governing participating organizations use and treatment of personal data received from the EU and Switzerland. See here for additional information - https://www.privacyshield.gov/US-Businesses

6. What is your general strategy for releasing fixes, patches and enhancements that incorporate best practices and user feedback?

All application updates and releases are included as part of Brightly annual subscription agreement. Clients are not required to provide any support during these updates as Brightly release them via our Software as a Service (SaaS) model.

We release application updates, which include both patches and product enhancements, on a biweekly cadence. Significant enhancements occur roughly quarterly and are communicated in advance to clients. All releases are documented in our online release notes.

Brightly provides a community site - https://community.brightlysoftware.com/s/ . This site provides clients with access to product support – including information on recent release. Clients are also able to submit product fix and enhancement requests through the community portal.

7. What protections do you provided against unauthorized access to data?

In addition to continuous encryption of client data in motion and at rest Brightly implements controls at the infrastructure, product, and procedure levels to further protect data from unauthorized access.

Brightly uses AWS security services for Web Application Firewall (WAF) and AWS Shield Distributed Denial-of-Service (DDoS) protection. AWS WAF protect our web applications and APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. AWS Shield protects against common, most frequently occurring network and transport layer DDoS attacks. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency in the event of a DDoS attack.

AWS Application Load Balancers (ALB) and Virtual Private Clouds (VPC) are used to segment network traffic between internet accessible, internal and database zones. ALB's provide scalability and resiliency by distributing incoming application traffic across multiple targets, such as web servers, across multiple availability zones. A VPC is a logically isolated virtual network within the AWS Cloud.

VPC access control lists and security groups are used to ensure that internal VPC's will only communicate with other approved internal resources.

Antivirus monitoring is a critical component for data protection. Current antivirus solutions are maintained on all endpoints to protect data integrity. Antivirus applications are installed as part of the imaging process for all computers. Antivirus signature updates are deployed daily.

Brightly uses a third party Managed Detection and Response (MDR) service to monitor our AWS environment for potential threats. Our MDR partner provides a dedicated Security Operations Center, staffed with highly skilled and specialized security experts, and 24/7 vigilance. The MDR system ingests events from endpoints, firewalls, load balancers, network flows, and event logs. The ingested data are combined with threat signatures and behavioral analytics to detect dynamic threats quickly across the entire environment. The goal is to provide 24/7/365 monitoring, proactive threat hunting, and coordinated threat response support to stop malicious activity before it can gain a foothold.

Brightly products build in numerous security controls, including role-based permissions and secure software development practices. Role-based permissions allow the configuration of granular access controls to grant scope of data access and functional capabilities based on specific user roles. Brightly uses a Secure Software Development Life Cycle (S-SDLC) framework that defines how we build our applications from inception to decommissioning. Application security considerations are an active component of planning and requirements. Regular vulnerability scanning and application dynamic and static testing are part of the S-SDLC.

Brightly uses separate environments for development, quality assurance testing and production. Production environments are separated logically from non-production environments to avoid unauthorized access or changes to production data. Brightly software development policies specify that production data containing personal data is restricted from non-production environments for testing or other purposes.

Client data is segmented from other clients using separate databases instances located on the multi-tenant database server infrastructure. Additional logical data segmentation is provided using unique Client ID numbers.

Brightly is committed to protecting the security of its customers' information and we take all reasonable precautions to protect it from unauthorized access, modification, or disclosure. Our documented and management approved incident management response policy documents the process used in responding to an actual or suspect data breach. It specifies members of the incident response team and steps to be followed for incident identification, containment, eradication, and recovery. Brightly has identified the relevant law enforcement and regulatory authorities we may need to contact in the event of a security incident. The policy also provides for prompt notification of clients impacted by an incident.

8. What precautions do you have in place for business continuity and disaster recovery?

Brightly has implemented disaster recovery and business continuity plans to ensure our customers experience consistent delivery of their crucial online services. Plans and procedures are documented for backups, data recovery and disaster recovery.

Full database backups and transaction log backups are performed automatically on Production servers for all databases. Database backups are taken nightly, and transaction logs are taken every 15 minutes. Backup processes are actively monitored for failures. The Product Delivery team is notified of failures and steps are taken to resolve. Stored backups are electronically transmitted over secure encrypted channels to AWS S3 storage daily. After 30 days in Amazon S3 storage backups are moved to Amazon Glacier storage for long-term archiving. Daily backups are archived and maintained for a minimum of one year. Monthly backups are archived and maintained for a minimum of seven years. Backups stored in AWS are encrypted. All AWS storage is in the continental United States.

Multiple AWS Availability Zones (AZ) within our AWS Region are used to provide for recovery capability. AWS Availability Zones (AZ) are isolated data center locations within an AWS region. Each AZ is backed by multiple physical data centers. While a single availability zone can span multiple data centers, no two zones share a data center. Each AZ in a region has redundant and separate power, networking, and connectivity to reduce the likelihood of two zones failing simultaneously.

Our application redundancy strategy leverages AWS auto scale groups in conjunction with multiple availability zones. The configuration is based on architectural and industry best standards to provide the continuous service in the event of a failure. Web and application servers are in an active/active configuration. Web traffic is load balanced between all web servers by an AWS Application Load Balancer (ALB). The failure of any web server or availability zone is detected by the ALB. The ALB disables the failed server and web traffic is automatically rerouted to the remaining server nodes.

Each tier of the application has multiple servers in either an active/active or active/passive configuration based on architectural needs and industry standards. Infrastructure-as-Code (IaC) technology allows for the rapid scaling or deployment of infrastructure to meet emergency needs.

High availability for data in the local AWS AZ is provided by using database servers in an active/passive configuration in concert with AWS Elastic Block Storage (EBS). Database requests are routed to the active database server. In the event of a failure on the active database server, the passive server is automatically brought online and takes over active database responsibilities. EBS volumes are replicated within the local AZ.

Brightly' main facility is in Cary, North Carolina. Located near Research Triangle Park, Cary has excellent access to transportation facilities and emergency services. The office is located within the same power grid as a regional medical center. In the event of a power outage, restoration of service to this grid is a utility priority. Brightly has additional office locations in the United States, Canada, the UK, Australia, and India. Our business can operate at capacity if any office location is lost. Fully remote business operation for an extended period (such as during a pandemic) is also possible if access to all office locations is impaired.

9. Do clients retain full rights and control of their data?

Per section 2.2 (b) of Brightly standard Terms of Service (https://www.brightlysoftware.com/terms) Brightly acknowledges and agrees that the Client retains all ownership right, title, and interest in and to Client data, including all Intellectual Property Rights. The data you place in our applications belongs to you. We will never share, sell, or distribute data that specifically identifies your organization. We may offer services that allow you to view "average" or aggregated data from other clients, but this data will never be specifically identified to you or your organization.

Clients can self-service exports of their data through the application by using an export utility or running detailed system reports and then exporting the report. Exports can be saved in PDF, Excel or csv formats.

10. Does your web-based interface support authentication, including standards-based single sign-on?

Brightly encourages clients to use the single sign-on (SSO) feature provided with the application. This allows users to log in to the application based on the client's already established password policy. Our SSO supports any SAML 2.0 compatible identity service (like Microsoft's Azure AD or Active Directory Federation Services).

About Brightly Software

Brightly, the global leader in intelligent asset management solutions, enables organizations to transform the performance of their assets. Brightly's sophisticated cloud-based platform leverages more than 20 years of data to deliver predictive insights that help users through the key phases of the entire asset lifecycle. More than 12,000 clients of every size worldwide depend on Brightly's complete suite of intuitive software – including CMMS, EAM, Strategic Asset Management, IoT Remote Monitoring, Sustainability and Community Engagement. Paired with award-winning training, support and consulting services, Brightly helps light the way to a bright future with smarter assets and sustainable communities. For more information, visit brightlysoftware.com