Brightly Security Controls

May 27,2022

Brightly Software
11000 Regency Parkway #400
Cary, NC 27518

Overview

Brightly Software's Information Security program reduce risks to information resources through implementation of controls designed to safeguard the security, availability, and confidentiality of client data. Protecting all proprietary information relating to Brightly Software and our clients is vital to our mission to be the global leader in intelligent asset management solutions.

Brightly Software protects the privacy of client data using a layered defense-in-depth approach to information security. Our cloud platform uses the industry-standard "shared responsibility" model. Built-in security and governance controls prevent unauthorized access to your data – from both Brightly employees and any other parties. Clients create and manage users, load asset data, create workflows, perform data analysis, and export data using application features. Application Role-Based-Access Controls (RBAC) allow client administrators to configure appropriate levels of data access for their internal users.

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 when explicitly authorized by the client. Under the shared responsibility model Brightly Client Services and Technology employees will only access client data as required to perform implementation and support services, to maintain security, and

manage capacity.

All data transmissions over public networks are made using secure, encrypted connections. All client data is encrypted at rest. Brightly applications provide for single sign-on (SSO) integration with any federated identity management supporting SAML v2.0. This allows clients to leverage their existing access control password and Multi-factor Authentication (MFA) policies.

Brightly Software's cloud platform is hosted in multiple secure AWS data centers with sites selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. Physical access to data centers is limited to AWS employees and approved third parties. Access requests are only granted with a valid business justification. They are based on the principles of least privilege and are time-bound. Facility access is removed after the requested time expires.

Brightly Software has architected the hosting of our platform and applications over multiple AWS Availability Zones to achieve high availability and business continuity. AWS Availability Zones are built to be independent and geographically separated from one another. Individual data centers within each availability zone have deployed critical resources to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Governance and Risk

Industry standards such as ISO 27002 and NIST are used as best practices guidelines for Brightly Software' information security program. Brightly Software has developed an Information Security Program based on ISO/IEC 27001 standards. The policies and procedures maintained and monitored in this program address administrative, technical, and physical safeguards appropriate to meet the following objectives:

- Ensure the confidentiality, integrity, and availability of non-public information we store for our clients and employees
- Protect against anticipated threats or hazards to such information
- Ensure Brightly Software follows applicable information security and privacy laws and regulations

We use the Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) program to assess and validate our security practices. In addition, annual HIPAA and PCI Data Security Standards self-

assessments are performed.

Brightly Software complies with the European Union's Global Data Protection Regulation (GDPR). We are registered 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 and Brightly Software's Privacy Shield Statement.

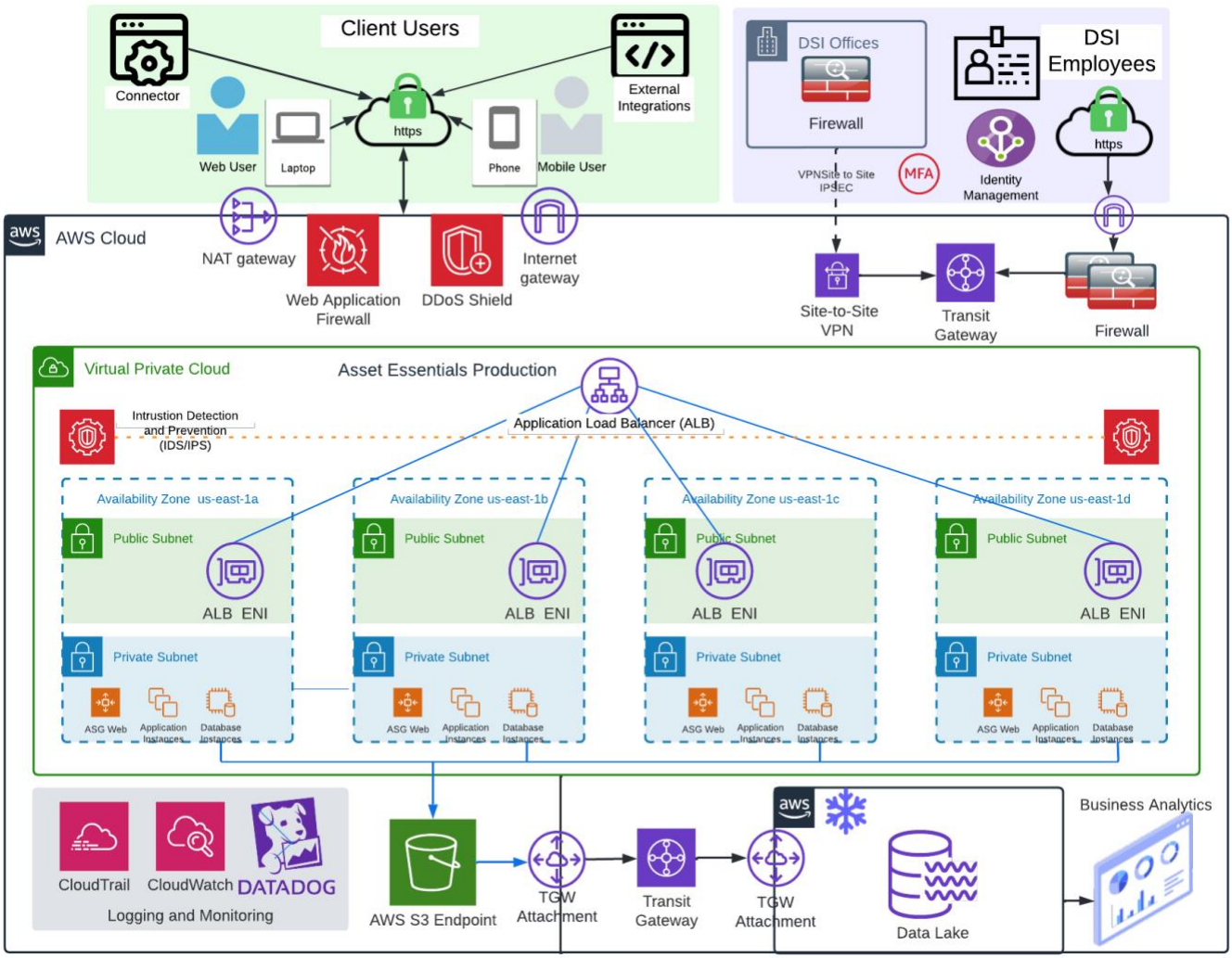
Security Architecture

Brightly Software 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. VPC access control lists are configured to "deny-by-default." All traffic that has not been specifically allowed is blocked.

VPC's are used to segment our cloud platform into an internet-facing DMZ, an application segment, and a database segment.



Intrusion Detection and Response

Brightly Software 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.

Vulnerability Management

Brightly Software uses a risk-based approach to vulnerability management. This approach uses five steps to control vulnerability risks:

1. Identification – Frequent scanning of the entire IT infrastructure – user endpoints, network infrastructure, and servers.
2. Assessment – Includes both traditional CVSS scoring methodology and a calculation of exploit potential.
3. Prioritization – Rank discovered vulnerabilities based both on exploit potential and business system criticality. Protection of systems containing client personal information would always be the highest priority.
4. Remediation – Targeted and actionable tasks against the prioritized list of vulnerabilities.
5. Measurement – Define key metrics and review over time to assess vulnerability management program effectiveness.

Regular authenticated internal and external discovery scans are performed.

Antivirus

Antivirus monitoring is a critical operation for Brightly Software. All workstations and servers must maintain up to date antivirus solutions to protect data integrity. Antivirus applications are installed as part of the imaging process for all computers. The Corporate IT and Infrastructure teams proactively monitor antivirus reports to identify and address issues quickly. Antivirus signature updates are deployed daily and reports are run on a weekly basis to ensure that all computers have current and accessible antivirus agents installed.

Change Management and Patching

Brightly Software follows a documented ITIL-based Change Management process. A Production Change Control Board (PCCB) meets weekly to authorize all Brightly Software changes proposed for production environments. Production environments contain any application, device, or infrastructure that supports Clients or processes that support Clients. Changes subject to PCCB review include:

- Any implementation of new functionality
- Server or network configuration changes
- Any interruption of service

- Any repair of existing functionality
- Any removal of existing functionality

Depending upon the scope of the changes Clients may receive information about changes using all the following methods - phone call, email, or in-application messaging. Online release notes are provided to document application changes.

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

Brightly Software automated release process greatly reduces down time and broken deployments. All Brightly Software updates are scheduled and posted in advance. Brightly Software adds new features and enhancements on a weekly or bi-weekly basis. These enhancements are deployed to our cloud-based solution for our entire client base without the involvement of client IT resources.

Security patches are deployed to all corporate workstations and server systems monthly. Within the server environment patches are first applied to development environments for testing and then deployed to production. High priority patches can be deployed within a day if the security vulnerability is determined to be critical.

Brightly Software 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.

Physical Security

Physical security issues can range from vandalism to theft. Brightly Software's cloud platform and client data are hosted in locked down, limited access AWS data centers.

AWS data center locations are selected to mitigate environmental risks, such as flooding, extreme weather events, and earthquakes. Data center are designed to anticipate and tolerate failures while still maintaining service levels. Core services are designed to an N+1 standard. This allows Brightly Software applications to leverage multiple independent data centers within an AWS availability zone for redundancy and continued operation in the event of individual data center failures.

Only pre-authorized personnel are allowed in the data centers, which are secured by sophisticated biometric security systems. Data center facilities are staffed and monitored 24x7x365. AWS provides physical data center access only to approved employees and third parties. All employees who need data center access must first apply for access and provide a valid business justification.

Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification.

These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

Access to all Brightly Software office locations is controlled by access badges which are immediately deactivated upon employee termination or being reported as lost. All facility visitors must be signed in by Brightly personnel and escorted while in our office locations.

Physical access to AWS data centers and Brightly offices is logged, monitored, and retained. Information gained from logical and physical monitoring systems is reviewed to enhance security on an as-needed basis.

Physical access points to AWS data center server rooms are recorded by Closed Circuit Television Camera (CCTV). Physical access is controlled at ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms if the door is forced or held open.

Business Continuity and Availability

Data Center Redundancy

Your data is not useful if it is not accessible. Brightly Software understands this, and we have designed our solutions for high performance and availability. Brightly applications are hosted in state-of-the-art virtualized infrastructures. High availability and automatic scalability are provided by leveraging our AWS hosted infrastructure and using load balancing and clustering technologies.

Brightly Software's cloud platform is hosted in multiple secure AWS data centers with sites selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. Brightly Software has architected the hosting of our platform and applications over multiple AWS Availability Zones to achieve high availability and business continuity.

AWS Availability Zones are built to be independent and geographically separated from one

another. Individual data centers within each availability zone have deployed critical resources to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AWS has identified critical system components required to maintain system availability and recover service in the event of outage. Critical system components are backed up across multiple, isolated Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected, allowing Brightly to architect our applications to take advantage of automatic fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design.

All AWS data centers use the following operational support systems:

Power - Data centers are equipped with a back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

Climate and Temperature – Control climate mechanisms maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages.

Fire Detection and Suppression – Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

Leakage Detection - Data centers monitor to detect the presence of water. If water is detected, mechanisms are in place to remove water to prevent any additional water damage.

Cloud Platform Redundancy

Brightly cloud platform services are maintained on a highly redundant system. We use the AWS Well-Architected Reliability Framework to implement best practices for reliability, high availability, and fault tolerance. Each tier of the application leverages AWS auto-scaling groups, load-balanced server farms and active / passive configurations to provide high availability and fault tolerance.

The Brightly Software cloud platform is partitioned across multiple fault-isolated AWS Availability Zones (each made up of multiple discrete data centers). Applications load balancers, web server farms and active / passive database clusters are used to take full advantage of the resilience

provided by the AWS Availability Zones.

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. Backups stored in AWS are encrypted. All data storage is in the continental United States. Testing of backup integrity is performed weekly.

Data Ownership

Per section 1.3 of Brightly Software's Master Subscription Agreement Brightly Software acknowledges and agrees that the Client retains all ownership right, title, and interest in and to Client data, including all Intellectual Property Rights.

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. API's are also available for automation of data exports. Brightly Client Services can assist clients in obtaining extracts of their data.

Brightly Software Helpful Links

Brightly Software community site - https://community.brightlysoftware.com/s/

Privacy Policy - https://www.brightlysoftware.com/privacy

Master Subscription Agreement - https://www.brightlysoftware.com/sites/default/files/file/2022-03/Brightly%20Subscription%20Agreement__revMar2022.pdf

Data Processing Addendum - https://www.brightlysoftware.com/sites/default/files/file/2022-03/Brightly%20Data%20Processing%20Addendum%20for%20Subscribers_revMar2022.pdf

Professional Services Addendum - https://www.brightlysoftware.com/sites/default/files/file/2022-03/Brightly%20Professional%20Services%20Addendum_revMar2022.pdf

Privacy Shield Statement – https://www.brightlysoftware.com/sites/default/files/file/2022-05/Brightly%20Privacy%20Shield%20-%20May%205%202022.pdf

Subprocessor Listing - https://www.brightlysoftware.com/sites/default/files/file/2022-03/Brightly%20Privacy_SubProcessors_revMar2022.pdf