BrightSign®

# TECHNICAL NOTES

## BrightSign Network Security Statement

BrightSign, LLC. 16795 Lark Ave., Suite 200 Los Gatos, CA 95032
408-852-9263 | www.brightsign.biz

# INTRODUCTION

For a cloud-based content management and distribution network, database security and server reliability should be of the highest prioirty. The BrightSign Network has been built with these principles in mind. This document provides a general overview of security and recovery architecture for the BrightSign Network. Note that some specific information may be withheld for security purposes.

## Physical Security

All BrightSign Network servers are hosted using Amazon Web Services (AWS). Amazon strictly controls physical access to its platform infrastructure using military-grade perimeter control, as well as state-of-the art surveillance and intrusion-detection systems.

Access to the Amazon data centers is limited only to Amazon employees with legitimate business needs, and each grant of access is revoked once an individual's business need expires, even if the individual is still an employee of Amazon. All physical and electronic access to data centers by employees is logged and routinely audited.

## Virtual Data Center Security

All communication with the BrightSign Network is mediated by two pairs of gateway servers. All calls to BrightSign Network domains are directed to these gateways. Each gateway communicates with a specific set of BrightSign Network nodes, and each pair of gateways is assigned traffic from a geographically distinct part of the globe.

Nodes located within the security group (i.e. behind the gateways) can communicate directly with each other because they have a list of internal IP addresses; however, these addresses are not communicated outside of the security group.

### DDoS Protection

The gateway servers protect internal nodes from being overloaded in case of a distributed denial of service (DDoS) attack. Furthermore, there are backup gateway servers that are running “warm” 24 hours a day and can immediately come online if one or more gateway becomes overloaded with connections.

Each gateway also has process code for the other gateways installed on it, so all gateways can be rotated to different routings or geographical assignments in event of an attack.

### General Disaster Recovery

Each BrightSign Network server node has a backup server that can take over in case of unscheduled downtime. The database server for the BrightSign Network has both a mirror and a backup that frequently update to prevent data loss in event the production database goes offline.

All active server nodes are monitored by scripts that notify BrightSign IT personnel less than a minute after a problem arises with a node.

### Protection Against Intrusion Attacks

Quarterly scans are carried out to check for hacking and intrusion attempts. All server operating systems are also protected with industry-standard virus detection software.

All BrightSign Network account passwords are hashed and salted. Once a password is generated, it is impossible for even BrightSign IT personnel to obtain the password from the BSN database. Furthermore, only a very limited subset of individuals at BrightSign have the credentials for root access to the BSN database.

## Application and Communications Security

The BrightSign Network interacts with digital signage environments by communicating with BrightSign devices, BrightAuthor software, and the BSN API (i.e. the browser-based BSN WebUI).

### Devices

The BrightSign Network and BrightSign devices communicate with each other using HTTPS, rather than HTTP. The BrightSign Network requires a device to authenticate itself with a hashed and salted phrase before it can download content.

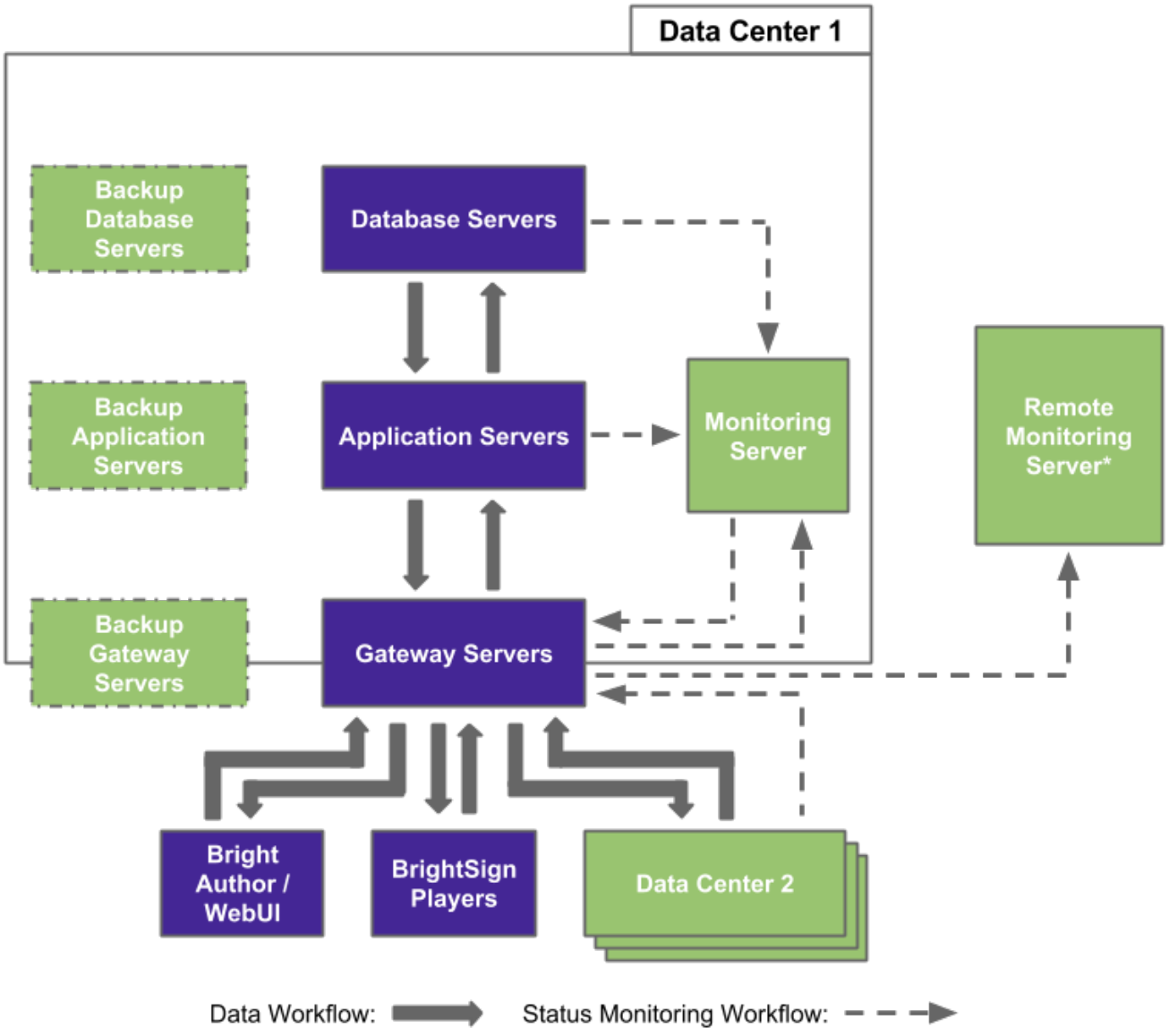
### BrightAuthor

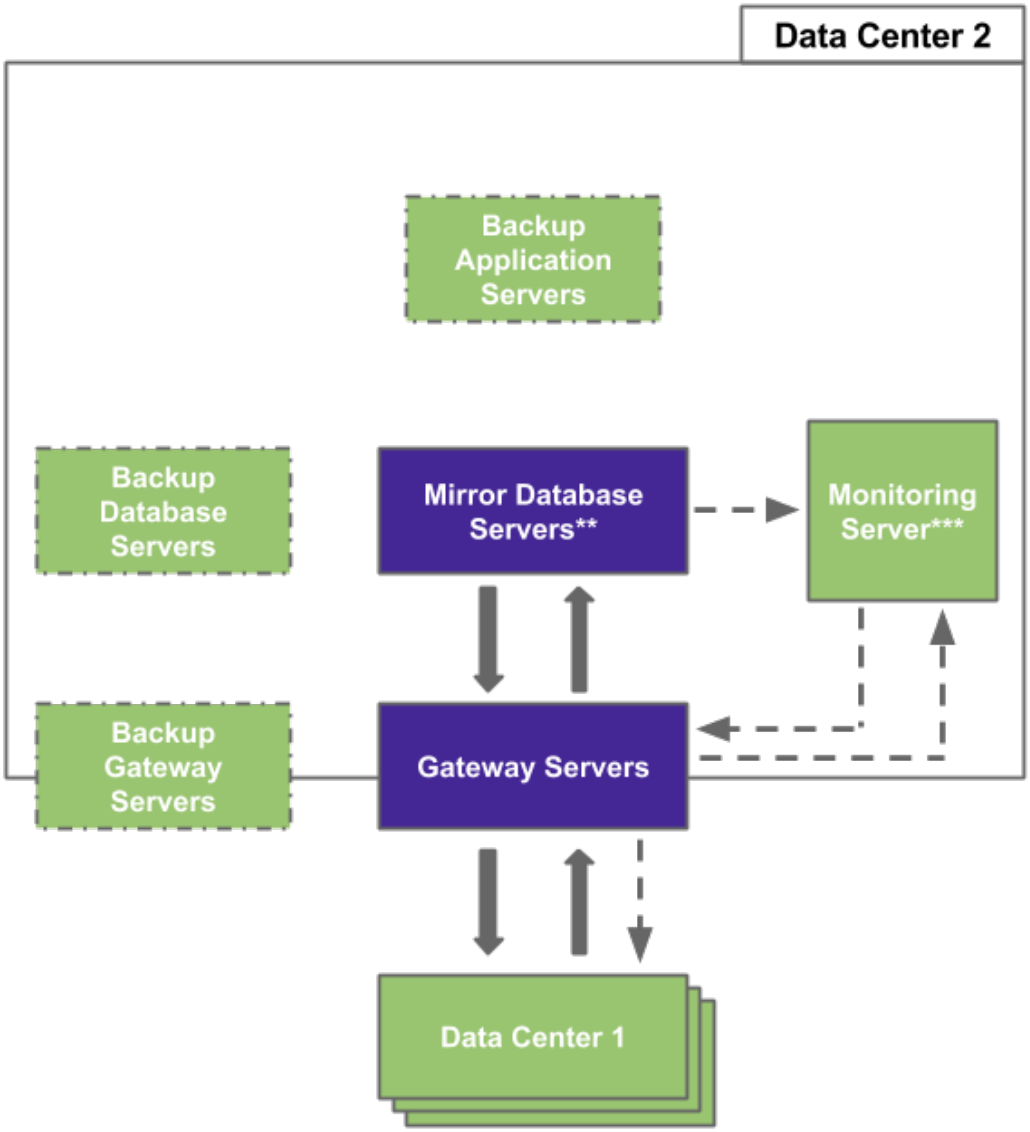
BrightAuthor requires BSN account authentication before affecting changes on the BrightSign Network. All communication between BrightAuthor and the BrightSign Network is carried out using HTTPS.

### BSN API

Every API call requires account authentication before affecting changes on the BrightSign Network or returning content from the database.

## Data Center Operation Block Diagram






**Notes**

* During normal operations, the Remote Monitoring Server only receives updates from the Monitoring Server within Data Center 1. If the Remote Monitoring Server is no longer receiving updates from the Monitoring Server, it will switch to receiving information directly from each Gateway, Application, and Database node.

** The Database Servers in Data Center 2 constantly mirror the Database Servers in Data Center 1.

*** The Monitoring Server in Data Center 2 reports to the Monitoring Server in Data Center 1.