# Security Guide

## EMC CloudBoost

Release number 2.0

## EMC CloudBoost Security Guide

P/N 302-002-470
REV. 1

February, 2016

EMC® CloudBoost™ enables long term storage provisioning in the cloud for backups made with EMC NetWorker®, EMC Avamar®, and Veritas NetBackup™. This guide provides details about the security related aspects of CloudBoost 2.0.



EMC²

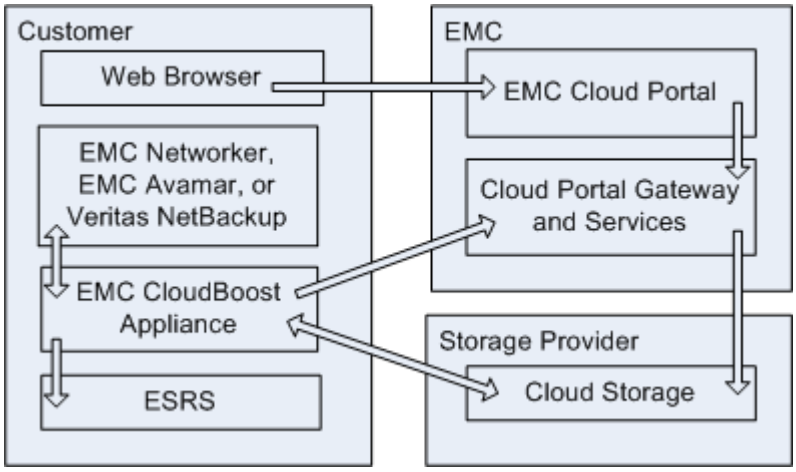
# CloudBoost Architecture

EMC CloudBoost is either a physical or a virtual appliance along with other components that enable long term storage in the cloud of backups made with EMC NetWorker, EMC Avamar, or Veritas NetBackup.

**Table 1** CloudBoost Components

| Component | Description |
|---|---|
| CloudBoost appliance | Onsite physical or virtual appliance that indexes, deduplicates, compresses, encrypts, and manages data transfer to and from the cloud. The optional data cache stores the data that is most recently written to or read data from the cloud. |
| CloudBoost client | Application that helps with data transfer between the CloudBoost appliance and the backup application. The CloudBoost appliance includes the client, but some backup applications require the client to be separately installed on the server for the backup application. |
| EMC Cloud Portal | Web-based portal providing a single interface for managing CloudBoost and other EMC services and products. |
| Cloud storage provider | S3 compatible object storage for data sent from the CloudBoost appliance. Several public and private cloud storage providers are supported. |
| EMC Secure Remote Services (ESRS) | Virtual appliance that enables two-way remote communication with EMC to monitor system health and to communicate events, alerts, status, and health to EMC Customer Support proactively. No user data is transferred. |

**Figure 1** EMC CloudBoost Security Architecture




# Data Protection

CloudBoost protects data by encrypting it when it is received. Data remains encrypted within the CloudBoost environment until it is restored. When restored, the data is decrypted as it leaves the CloudBoost environment and is returned to your application. While data is being transferred between the CloudBoost appliance and the cloud storage

provider, it is encrypted a second time. Communications between CloudBoost components is also encrypted.

Storage providers add their own measures to protect data. For more information, contact the provider.

## Data at Rest Protection

At rest data is encrypted using 256-bit AES encryption in CBC mode. For integrations where the CloudBoost client is installed on the server of the backup application, data is encrypted by the client before it is sent to the CloudBoost appliance. For integrations that use the client on the CloudBoost appliance (such as EMC NetWorker), data is encrypted on the appliance. Data remains encrypted as it is sent to or retrieved from the cloud storage provider. Data is not decrypted until it is returned from the CloudBoost environment to the integrated backup application as part of a restore operation.

CloudBoost manages the data encryption keys. The keys are securely saved in a keystore on the appliance. The keystore is encrypted and backed up to the cloud storage provider, where it can be recovered as needed.

## Data in Transit Protection

The CloudBoost appliance and the cloud storage provider use SSL and TLS to encrypt data being transferred between them. This encryption is in addition to the encryption that occurred when the data was received from the integrated backup application.

All communications between the CloudBoost components is also encrypted with SSL and TLS. For information on the ports that must be opened, see CloudBoost Ports on page 4.

## Cloud Storage Provider

Data is stored with a supported S3 cloud storage provider. The data is encrypted before being sent to the provider and remains encrypted in the provider data center. The provider does not know the encryption key and cannot decrypt the data. Each provider also takes additional measures to protect the data. For more information, contact the provider.

## Data Removal Practices

CloudBoost places the application data in the CloudBoost appliance and the cloud storage provider data center. As the data is being transferred to the cloud storage provider, it is stored on the appliance. After the data is transferred, the data is deleted from the appliance. If the appliance cache feature is enabled, the data remains on the appliance for quicker restores until the appliance must make room for new data transfers, at which time it is deleted.

Data that is transferred to a cloud storage provider remains with the provider until you no longer want that data stored in the cloud. How quickly the data is removed depends on the provider. Each provider has its own data removal policies. Contact the specific provider for its policies.

If CloudBoost integration with a backup application is abruptly stopped without proper removal (example: an application server fails), the application data remains stored with the cloud storage provider. If the appliance cache feature is enabled, cached data remains on the appliance until the space is needed for newer data transfers to the cloud storage provider.

If you stop using CloudBoost, any data on the appliance remains encrypted on the appliance. Data that is stored with a cloud storage provider remains encrypted and cannot be decrypted without CloudBoost. The time the data remains stored with the provider depends on their policies and the status of the account with the provider.

# Infrastructure Security

CloudBoost includes features to protect the infrastructure. To prevent unauthorized access to CloudBoost, the proper account credentials are required. To address vulnerabilities, updates are made available as needed. Updates can be applied without interruption to the availability of CloudBoost. To help with network management, specific ports are used for specific CloudBoost activities.

## CloudBoost Access Control

Access control prevents unauthorized users from getting to the data and CloudBoost components. Access to CloudBoost is controlled through accounts and passwords.

- EMC Cloud Portal - You access the Portal by logging in with a web browser using your Cloud Portal credentials. The Portal allows you to perform administrative tasks, such as specifying cloud storage providers, managing and configuring the CloudBoost appliance, and starting the installation of appliance software updates.
- CloudBoost appliance - When you deploy the CloudBoost appliance, you choose a password for the appliance administrator account. This password allows you to log in to the appliance to provide the appliance with its registration code during initial deployment. You can also log in to perform certain administrative and support tasks at the command line interface. The CloudBoost appliance account is not the same as the Cloud Portal account.

## CloudBoost Updates and Malware Protection

EMC provides updates to the EMC Cloud Portal, CloudBoost appliance, and CloudBoost clients as new features are available and issues are addressed. EMC continuously and seamlessly updates the Portal. The CloudBoost administrator is responsible for updating the appliance and the CloudBoost clients, when the clients are installed on an integrated backup application server.

The CloudBoost appliance does not protect against malware attacks, nor does it try to recognize and prevent data that is related to or affected by malware from being sent to the cloud storage provider. To ensure the integrity of data, appropriate anti-malware software should be used.

## CloudBoost Ports

CloudBoost requires several ports to be open for proper communications between components.

**Note**

Although the following table shows communications "From" one component "To" another, communications generally also occurs in the opposite direction.

**Table 2** Firewall port requirements

| From | To | TCP Port | Description |
|---|---|---|---|
| Administrator workstation | Storage node on the CloudBoost appliance | 22 | SSH for maintenance and troubleshooting |
| Storage node on the CloudBoost appliance | Cloud storage (public or private) | 443 | HTTPS to access object store (if supported) |
| Storage node on the CloudBoost appliance | EMC Cloud Portal | 443 | HTTPS to EMC Cloud Portal and Cloud Portal Services/APIs |
| Storage node on the CloudBoost appliance | ubuntu mirrors | 443 | /mirrors.kernel.org/ |
| CloudBoost client | Storage node on the CloudBoost appliance | 443 | When Avamar is deployed with CloudBoost, this is necessary for the CloudBoost appliance on the Avamar staging server. |
| CloudBoost client | Storage node on the CloudBoost appliance | 443 | When Veritas NetBackup is deployed with CloudBoost, this is necessary when the CloudBoost client is on the Windows media server. |
| Administrator workstation | Storage node on the CloudBoost appliance | 4444 | HTTPS to EMC Cloud Portal/API |
| NetWorker server | Storage node on the CloudBoost appliance | 7800-7900 | Various NetWorker services |
| NetWorker server | Storage node on the CloudBoost appliance | 7937 | NetWorker client service daemon (nsrexecd) |
| NetWorker server | Storage node on the CloudBoost appliance | 7938 | NetWorker port mapper |
| Storage node on the CloudBoost appliance | site cache servers | 8443 | Incoming HTTPS port for all data read and write traffic |
| Storage node on the CloudBoost appliance | ESRS gateway | 9443 | Communication from CloudBoost appliance to the EMC Secure Remote Services gateway |

## Security Settings

CloudBoost includes settings that control security related aspects of the product.

- Remote appliance administration - By default, remote access to the CloudBoost appliance is disabled. You can enable remote access to the appliance, perhaps when troubleshooting and for support purposes.
- Proxy server - You can specify the use of a proxy server.

# Privacy Policy

EMC wants to help you protect your information. To do this, EMC operates on several policies regarding your information.

- Your information is your information, not our information.
- We never sell your information to anyone, nor do we sell information about you.
- We never share your information with anyone unless you explicitly tell us to.
- We never sift through your information to create a profile of you for targeted advertising.

Published February, 2016