CASELLE®
Commitment to Community

Caselle Hosted Dashboard

Caselle Cloud Security

Caselle administers the servers for the Caselle Hosted applications. Caselle Cloud security refers to the measures and technologies used to protect data, applications, and infrastructure in cloud computing environments from threats and unauthorized access. This document explains the policies, controls, and practices Caselle will use to ensure the safety and privacy of information stored in the cloud.

In this document, learn why Caselle Cloud security is important, how it works, and how it impacts your experience with Caselle Hosted applications.

Contents

Hosted servers

Caselle administers the servers used to host Caselle Cloud hosted applications.

This service provides you:

- State-of-the-art infrastructure and security using Amazon Web Services (AWS).
- Backup redundancy within and outside of AWS.
- Commitment to the safety and security of your applications and data. Third-party penetration testing is performed routinely.

The topics of security and safety come up frequently when clients consider moving to a cloud-based service. Data security risks are a problem plaguing businesses and communities throughout the U.S. It is one of the primary motivating factors our clients have for moving their applications from a local network installation to a Cloud-hosted environment.

We take protecting your clients' information very seriously. Part of our commitment to be proficient stewards of your data is reflected in our choice of using Microsoft Remote Desktop Services (RDS). This method of access sends screen information to you using an encrypted connection, no application data is passed back and forth directly across the internet. The result is a safe and secure way to access your Cloud-hosted applications from just about anywhere.

Inbound connections to your network are not required. Cloud-hosted applications use the Remote Application (RemoteApp), so users are only allowed to run approved applications. Access to email, internet browsers, and file explorer on the Cloud server have been disabled to further protect your data.

Cybersecurity Letter of Attestation

Caselle contracts the services of LMG Security to perform cybersecurity and network penetration testing on the Cloud environment to ensure its protection from unwanted external sources. The results are found in the Letter of Attestation or log4j Letter of Attestation provided by LMG Security.

Cloud Security FAQs

Q. What measures are taken to secure your data?

A. We use Amazon's AWS Data Centers to host the Cloud infrastructure, followed by the deployment of security firewalls at both the AWS and Cloud server levels. Users go through a whitelisting process to only allow access by our clients and trained Caselle personnel. A robust backup system is in place using both AWS resources and a non-AWS location.

Q. Is testing performed to ensure data and applications are secure?

A. Caselle performs weekly vulnerability tests to detect security changes and contracts with LMG Security, a third-party security company, to perform cybersecurity and network penetration tests on all Cloud systems to verify the strength of our security.

Q. Are operating system (OS) security updates regularly maintained?

A. Cloud systems are on a schedule for routine updates, and critical security patches are expedited when necessary.

Q. How often are backups performed?

A. Backups are performed nightly and kept in multiple U.S. geographic locations both within AWS and outside of AWS. Restoration tests are performed at least annually to ensure a fast recovery if disaster were to strike.

Q. Are Cloud systems monitored for performance and technical issues?

A. All Caselle Cloud systems are monitored twenty-four hours a day, seven days a week using a combination of tools which will alert trained IT personnel when performance thresholds are exceeded, or unusual behavior is detected.