

DATAGENIX

ClaimScape Security Infrastructure

Keeping Your Data Protected

ClaimScape managed hosting combines dedicated client infrastructure with controlled application access and a replicated database environment.

Built on Amazon Web Services (AWS), the hosting architecture protects client data while supporting the availability required for ongoing healthcare administration.

Client Data Has Its Own Place in the Environment

Protecting healthcare administration data starts with how the hosting environment is structured. ClaimScape uses dedicated database and server infrastructure rather than shared tenancy, keeping each client environment separate within AWS.

Dedicated Infrastructure

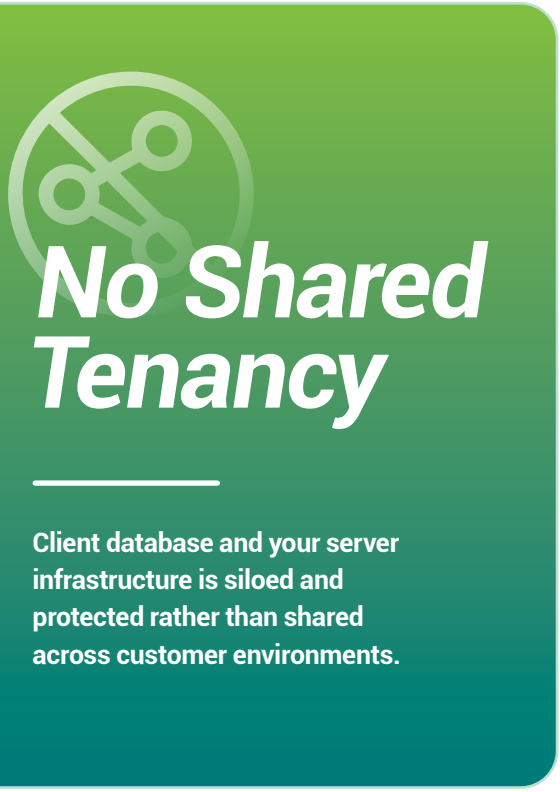
Each client environment uses dedicated server and database infrastructure. Customer data is placed in private subnets that are isolated from public inbound access.

Encryption is enforced while data is stored and while it moves across internal or external connections.

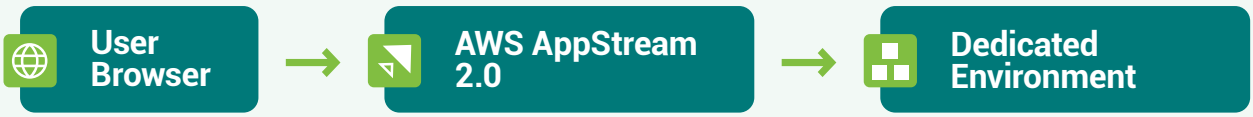
Application Access Without Direct Exposure

AWS AppStream 2.0 streams ClaimScape through an HTTPS connection, allowing users to launch the application from a browser without requiring a VPN or remote desktop connection.

AppStream protects streamed pixels and end-user inputs with end-to-end AES-256 encryption. User sessions are non-persistent, so they are disposed of when no longer in use rather than retained for a future session.



Users interact with ClaimScape through a secure streamed session while the hosted application remains within AWS.



Access Controls Extend Beyond the User Session

ClaimScape applications use two-factor authentication with a one-time passcode sent by phone or email. SAML 2.0 federation integration is also available for organizations that need to connect ClaimScape with their existing identity environment.

The Database Is Replicated Before a Disruption Occurs

ClaimScape uses Amazon Relational Database Service (RDS) with a Multi-AZ configuration. The production database is synchronously replicated to a standby database in a separate Availability Zone at another physical data center.

If the primary database becomes unavailable, Amazon RDS is configured to fail over automatically to the standby environment.



Separate Availability Zones maintain an active database and synchronized standby environment.

Backups Provide Additional Recovery Options

Daily EC2 backups protect the hosted server environment. Continuous point-in-time database recovery provides another way to restore data from an earlier point when needed, while daily database snapshots and backups are retained for 90 days.

Infrastructure Is Monitored Around the Clock

AWS CloudWatch monitors EC2 infrastructure 24/7 and generates alerts when issues are detected. Automated recovery is configured for EC2 host-level failures, reducing reliance on manual intervention when an infrastructure problem occurs.

Built for Continuity

The standby database is maintained in a separate Availability Zone and kept synchronized with the production environment before a failover occurs.

Capacity Adjusts as Usage Changes

Server infrastructure can be scaled as additional capacity is required.

AWS Layer 7 load balancing distributes application traffic across available resources, while dynamic backend scaling supports AppStream user sessions as demand changes.

The Hosting Architecture Supports Technical Review

An IT or security review often requires more detail than a general statement about data protection. Reviewers may need to understand how client resources are separated from other environments and how access to AWS infrastructure is controlled.

ClaimScape managed hosting is structured around defined controls and a documented AWS architecture, giving organizations a technical environment they can evaluate as part of security reviews and ongoing IT oversight.

Access Is Controlled Beyond the Login

User authentication is one layer of protection. Within AWS, least-privilege security group configurations restrict access to resources, while administrative RDP access to EC2 instances is limited.

Public HTTPS endpoints require TLS 1.2 or higher. AWS Web Application Firewall protects web applications, while AWS Shield provides protection against distributed denial-of-service attacks.

Activity Is Logged and Infrastructure Is Monitored

Application- and system-level events are logged within the environment, providing a record of activity at both levels.

AWS CloudWatch monitors EC2 infrastructure around the clock and generates alerts when operating conditions require attention.

A Stronger Foundation

Together with the dedicated infrastructure, data protection, and recovery measures built into ClaimScape managed hosting, these controls provide organizations with substantive information to evaluate during security reviews and ongoing IT oversight.

Book a Demo

Request More Information