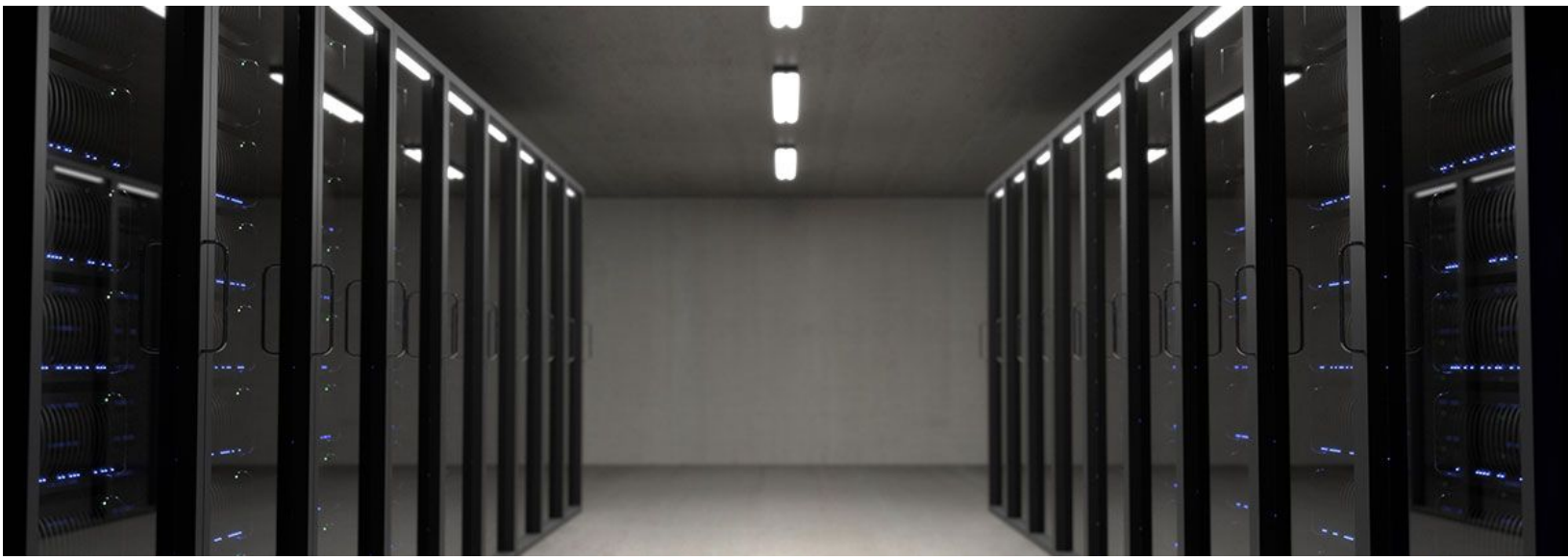
Cicayda eDiscovery

DATA AND CLOUD SYSTEM SECURITY OVERVIEW



Security First

At Cicayda, data and system security is always a concern for our engineering team. Our system architecture is aimed at not only providing our customers with the best experience and workflow, but also preventing data breaches and their potential risks and liabilities.

Below we have outlined how Cicayda ensures the security and integrity of our customers' data through best practices in several critical areas.

AMAZON WEB SERVICES AND CLOUD COMPUTING

Cicayda utilizes Amazon Web Services as a scalable cloud computing platform to deliver our web applications to you the end user. The AWS infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services. The AWS global infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards. Protecting this infrastructure is AWS's number one priority, and AWS provides several reports from third-party auditors who have verified its compliance with a variety of computer security standards and regulations that can be found at http://aws.amazon.com/compliance.

Physical Security

Cicayda data centers in the United States are located within a private cloud at Amazon's AWS distributed infrastructure. The AWS infrastructure used by Cicayda is designed and managed to meet security best practices along with a host of the most well-known IT security standards

These Include :

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FEDRAMP
- DOD CSM Levels 1–5
- PCI DSS Level 1
- ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

ENVIRONMENT

AWS carefully chooses facility location to mitigate the risk of flooding, extreme weather, and earthquakes.

SITE PERIMETER

AWS has security guards, fencing, and video surveillance guarding site perimeters. Personnel are only allowed on site after applying for access and providing a valid business reason. Once on site, their access is restricted to pre-approved areas.

INFRASTRUCTURE

AWS also limits access to their HVAC, backup power, and fire suppression systems. These systems are regularly checked as part of normal operations.

DATA

There is another layer of security checks prior to accessing AWS servers. Server rooms require multi-factor authorization, and servers warn employees of any attempts to remove data. Storage devices are decommissioned using the techniques outlined in NIST 800-88. In addition, AWS is audited by third party auditors on more than 2,600 requirements throughout the year.

Should an accident or disaster occur, Cicayda is prepared for immediate data recovery to maintain service. Cicayda maintains redundant data centers throughout Amazon's AWS infrastructure. Our primary data center includes live database servers and file storage as well as immediate backups. If the primary data center suffers a catastrophic failure or a loss of external connectivity, users may experience minimal downtime while web servers are activated at the secondary data center to restore access there.

Technical Safeguards

Cicayda employs a security advisor with extensive experience in communications intelligence, network security, digital media exploitation, cyber threat intelligence, indications and warning, and information warfare who is responsible for implementing security policies and procedures.

Only full-time Cicayda project managers and engineers who have undergone background checks, completed Cicayda engineering security or operations security training, and are subject to confidentiality agreements with Cicayda have access to client data.

DATA ENCRYPTION

Cicayda customers send data to us via secure FTP, HTTPS or on an encrypted hard drive. All ingested data is protected using SHA-256 key exchange, AES-256 encryption, and TLS, SSH, and SCP for transfers. Thus, customer data is protected both in transit and on disk at our Cicayda data centers.

ACCESS CONTROL

Every endpoint of our platform checks to ensure the user has access to the requested data.

AUDIT CONTROL

Every request sent to our platform is scrubbed of sensitive data and logged.

TRANSMISSION SECURITY

Cicayda only transmits data over TLS encrypted connections. This include data sent to clients and data sent to AWS services.

NETWORK SECURITY

All Cicayda servers are behind a firewall that only permits web traffic to application servers and SSH traffic for developer maintenance.