casepoint

BROCHURE

Security Brief | Superior Security. Trusted Protection.

Securing Client Data is Our Top Priority

We understand that securing sensitive data is paramount. The need for data integrity and defensibility is extremely high for corporations, government agencies, law firms, and service providers. We remain committed to the highest levels of security at the company, data center, web application, and database levels. Our policies, procedures, and company culture are all focused on keeping your data safe and protected around the clock, with continuous monitoring and the highest standards of security at each level.

Security Overview

Casepoint has established comprehensive security measures at all levels—organizational, architectural, and operational—to ensure that all data, applications, and infrastructure remain protected and secure. Casepoint has designed, developed, documented, approved, and implemented an Information Security Management Program (ISMP) that addresses industry-best practices around security and privacy. Our ISMP includes administrative, technical, and physical safeguards to protect data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. Our ISMP is also comprehensively documented with corresponding manuals for our security procedures and other policies.

Built on Trust

Casepoint's legal technology solutions meet rigorous security, privacy, and compliance standards.

Industry-standard Security Certifications

FedRAMP

SOC 1

SOC 2

SOC 3

ISO 27001:2013

ISO 9001:2015

NIST 800-53

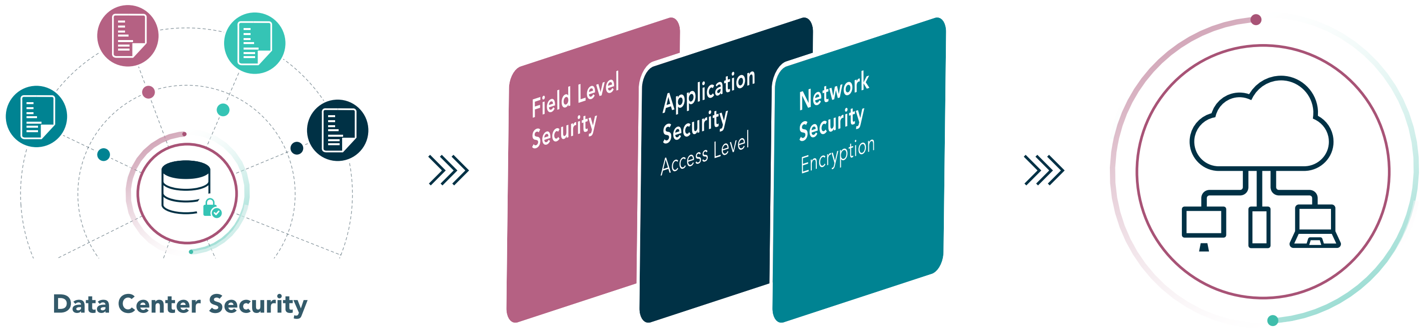
NIST 800-171

HIPAA

PCI DSS

We Stand by It

Casepoint provides a level of security you can trust. Our clients demand strict security standards that we have provided with flying colors. Our commitment to high standards of security pertains to every single level. Don't expect anything less from your legal technology provider.



Data Center Security
Physical Security

Organizational Security

At Casepoint, **security is the responsibility of each and every employee.** We ensure that all Casepoint employees are apprised of security best practices. Our Security Team is comprised of a group of top executives that design and drive our security programs. They ensure that our security awareness and policies are maintained across our organization.

Architectural Security

- **Data Encryption:** Our team of experts has defined policies for **all granular controls of access such as Network access control, OS access control, application access control, VPN access policy, and end-user encryption key protection policy.** All media drives are encrypted with military-grade encryptions.
- **Single Sign-on:** **Casepoint supports single sign-on (SSO)** using SAML protocol. Users can log in using their organization's LDAP or other SSO system.
- **Multi-factor Authentication (MFA):** **Casepoint offers multi-factor authentication to all customer accounts.** Multi-factor authentication increases your account's security by verifying with a second method, such as your email or mobile device.

Operational Security

- **Physical Security:** There are several levels of physical security controls in place to protect information assets in our offices and facilities where information assets are stored and/or processed. **All physical access to the data centers is highly restricted and stringently regulated.**
- **Network Security:** We have established detailed operating policies, procedures, and processes designed to help manage the overall quality and integrity of the organization environment. We've also implemented **proactive security procedures like network intrusion prevention systems (IPS).**
- **Application Security:** Casepoint's management-approved ISMS Manual provides policies and procedures for the development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities. **Our team of experts has established software development and release management processes to control the implementation of major changes.**