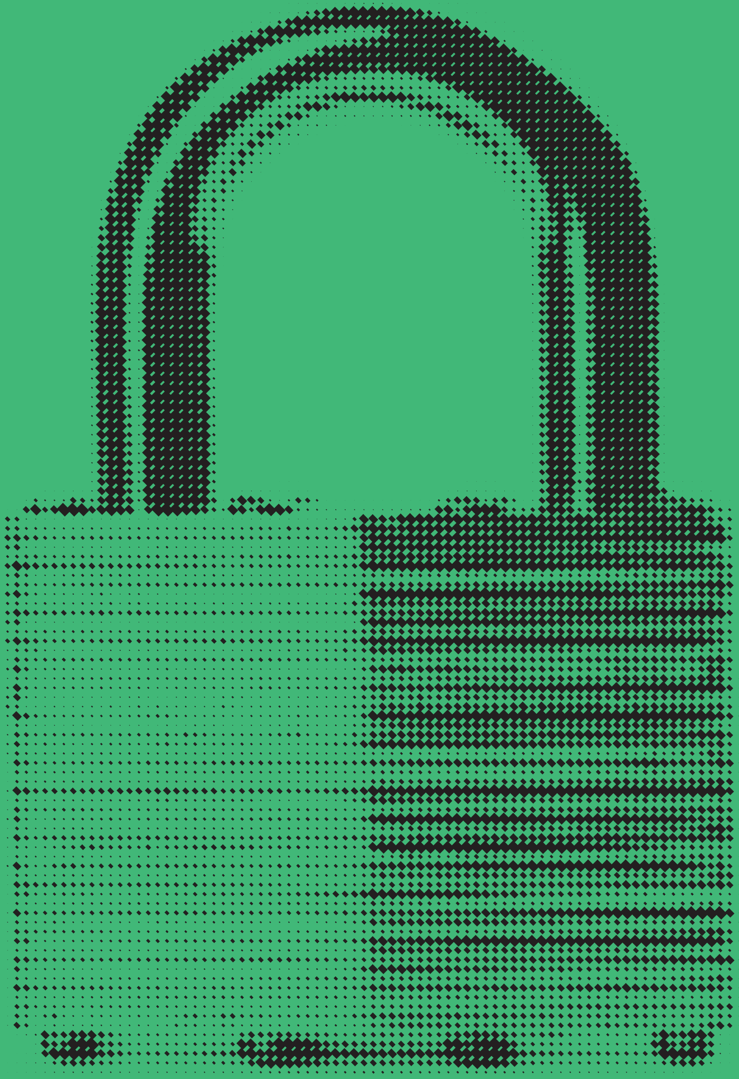
Trust in Every Byte

A Deep Dive into Everlaw's Security Practices



Everlaw

Table of Contents

Introduction

In the rapidly evolving landscape of legal technology, ediscovery platforms have become fundamental to streamlining the litigation process and enhancing the efficiency of legal investigations. The Everlaw platform is a modern cloud-based ediscovery and litigation platform that enables teams to process, manage, review, produce, and present electronically stored information in an efficient, powerful, and cost-effective manner. Storybuilder by Everlaw is a standalone collaborative tool for legal professionals that enables teams to organize documents and build cohesive narratives.

We understand the sensitive nature of the data entrusted to us by our clients. The legal industry demands nothing short of the highest standards of confidentiality and integrity, and our platform is designed to meet these needs head-on. Through our technology, we provide legal professionals with the tools they need to conduct thorough and effective ediscovery, all while maintaining an unwavering commitment to safeguarding their data. Everlaw effortlessly scales with demand, leveraging a secure, cloud-native architecture hosted on Amazon Web Services (AWS). The offering of a cloud-based software as a service (SaaS) solution not only restructures how legal teams manage and analyze data but also embodies stringent security measures, comprehensive compliance adherence, and uncompromising privacy protections.

This white paper outlines Everlaw's approach to security and compliance within the ediscovery sphere. Our aim is to demonstrate not only Everlaw's capabilities as a leader in legal technology but also our dedication to upholding the trust and confidence of our clients in every aspect of our operations. At the heart of our operations, security and compliance are integral to our philosophy, shaping every facet of our business – including product design, development, marketing, sales, and customer service.

Everlaw's Security Philosophy

When it comes to security and compliance, Everlaw takes a holistic approach, embedding it deeply into the core of our company's philosophy. Recognizing the critical nature of hosting sensitive client data on a SaaS ediscovery platform, Everlaw utilizes enterprise-class security protocols and adheres to the highest privacy standards. Our approach ensures that our comprehensive compliance program and strict controls are always in alignment with our clients' needs and expectations.

Everlaw’s Security, Privacy, and Compliance Measures

We hold the conviction that security, compliance, and privacy are interconnected facets of a comprehensive program. Everlaw is meticulously designed to protect client data and ensures that when it comes to security, we are doing the right thing and doing it the right way. Built on robust cloud infrastructure and incorporating the latest in cybersecurity best practices, our approach to security addresses the unique challenges faced by the legal and ediscovery sectors.

Inside Everlaw’s Compliance Program

Everlaw’s Compliance Program Framework is strategically structured around seven core elements, guided by established federal guidelines and industry best practices to ensure comprehensive integration of security, privacy, and compliance across all aspects of our operations. We adhere to the strict standards set by pivotal resources such as the United States Sentencing Commission Guidelines Manual, particularly Section 8, which focuses on Effective Compliance and Ethics Programs; the U.S. Justice Manual, Section 9-28.800, dedicated to Corporate Compliance Programs; and the U.S. Department of Justice’s Evaluation of Corporate Compliance Programs.

Enhancing our framework further, we integrate the Cybersecurity & Data Privacy by Design Principles from the Secure Controls Framework. These principles ensure that security and privacy are not afterthoughts but are foundational to our system design and operational processes.

To drive and manage these initiatives, Everlaw has established a dedicated Security Management team. This team is not only responsible for the strategic design and implementation of our security, privacy, and compliance efforts but also oversees the ongoing management of these critical areas. Their work ensures that Everlaw consistently aligns with evolving legal requirements and industry best practices, safeguarding our client data and maintaining trust.

Our approach is more than a compliance checklist; it is a commitment to operational excellence and ethical practice that positions Everlaw at the forefront of legal technology services. Doing the right thing and doing it the right way.

Everlaw's Data Protection Strategy

Our dedication to maintaining the highest standards of data protection and privacy is integral to every facet of our operations. Anchored by our expert Privacy team, we focus relentlessly on securing the integrity and confidentiality of the data entrusted to us.

Proactive Data Management

Tasked with overseeing our comprehensive data inventories and impact assessments, our Privacy team plays a crucial role in our security infrastructure. These ongoing activities are essential for promptly identifying and mitigating any risks to data handling. Regular updates to our data inventories ensure that we have current and accurate records of data flows and storage specifics, allowing us to quickly address any potential gaps in our data protections.

Dynamic Risk Assessments

Our commitment to dynamic improvement involves continuous risk assessments that scrutinize the effectiveness of our data protection measures. By regularly adapting our strategies, we keep pace with evolving legal and regulatory demands, ensuring that our data handling procedures safeguard client information against emerging threats.

Certifications and Compliance

Everlaw holds a SOC 2 Type 2 certification, a testament to our rigorous privacy standards. This certification not only underscores our dedication to robust data protection practices but also reinforces the trust our clients place in us.

Transparency in Data Policies

Our Privacy Policy is crafted for transparency, outlining in clear terms how Everlaw collects, uses, stores, and discloses personal information. This policy ensures that our clients and users are well-informed of our data management practices and their rights regarding personal data, fostering an environment of trust and openness.

Enterprise Risk Management

Everlaw has implemented the Three Lines of Defense governance model to enhance its internal control systems. This model promotes effective and transparent management of compliance obligations and risk by defining clear accountabilities throughout the organization. Our risk assessment and management strategy is vital for governance in all departments. It follows the guidelines from the NIST Risk Management Guide for Information Technology Systems, NIST SP 800-30. The Security Management team is responsible for organizing regular risk assessment meetings with the risk management committee, ensuring the risk register is meticulously maintained and updated, and continuously monitoring the effectiveness of risk response strategies and their implementation.

Policies & Procedures

Our policies and procedures are designed to enforce strict standards of security, privacy, and compliance across all aspects of our operations. These documents not only guide our daily activities but also ensure that every member of our team understands and implements our core values and legal obligations in their work. Everlaw meticulously documents, disseminates, and updates internal policies and procedures that effectively reinforce ethical norms and compliance, fostering a culture deeply rooted in integrity. They also serve to address the compliance, security, and privacy risks identified by the company via the risk assessment process described above. Everlaw's Policies and Procedures address information security, business policies and practices, and federal- and government-specific compliance requirements.

Availability & Business Continuity

Everlaw consistently maintains an annual uptime exceeding 99.95%, inclusive of scheduled maintenance. Our meticulous business continuity and disaster recovery plans are developed using insights from regular risk assessments, vulnerability scans, and threat analyses, along with third-party and vendor risk evaluations. These plans and our incident response procedures are rigorously tested at least once a year, playing a crucial role in refining our continuous risk assessment and management strategies.

Personnel Security

All employees and select suppliers undergo comprehensive background checks prior to the first day of working at Everlaw, including criminal history and employment verification in accordance with local laws. Everlaw also verifies work eligibility for all employees by collecting I-9 documents and running E-Verify checks. Additionally, all Everlaw employees, upon joining the company and/or during their employment period, as well as certain service providers, are required to sign nondisclosure and confidentiality agreements. Everlaw requires employees to affirm their acknowledgment and agreement to follow Everlaw's Code of Conduct, Employee Handbook, and all Policies and Procedures on an annual basis.

Incident Response

The importance of a robust incident response capability cannot be overstated. An effective incident response strategy is critical to mitigate the impact of security breaches and cyberattacks swiftly and efficiently. We prioritize a structured and rigorous incident response process to manage and recover from incidents with minimal disruption to our services and to maintain trust with our clients and stakeholders. Our incident response framework is designed to detect, respond to, and recover from cybersecurity incidents promptly.

Everlaw adheres to the NIST SP 800-61 guidelines for incident management, establishing clear escalation paths and defined steps for breach notification. Our incident reporting and response procedures are supported by a suite of advanced security technologies that ensure comprehensive threat monitoring and management. These procedures are designed to handle a variety of scenarios, including insider threats and software vulnerabilities, and are rigorously tested annually to confirm their effectiveness. Our team participates in ongoing training and industry initiatives to stay at the forefront of cybersecurity practices, ensuring a proactive stance in incident management. All incidents are logged in a secure tracking system, which is audited annually to maintain our high standards of security and accountability. By preparing for, rapidly addressing, and thoroughly recovering from any security incident, we safeguard our operations, protect our clients' data, and preserve the integrity of our services.

Corporate IT Security

Everlaw enforces uncompromising security measures, anchored by mandatory full-disk encryption across all employee computers utilizing the advanced 256-bit AES encryption algorithm. This protocol ensures the secure handling of both customer and personal data. Our layered security approach includes role-based access controls, multi-factor authentication (MFA), and precise account management procedures, underpinned by a robust information security policy that mandates antivirus software and strong password protocols aligned with NIST best practices.

To safeguard mobile access, Everlaw strictly controls device permissions through a comprehensive bring-your-own-device (BYOD) policy, ensuring all devices meet our security standards before accessing our network. This policy includes protocols for securely erasing Everlaw data in the event of device loss or theft. Consistent application of multi-factor authentication further secures access across mobile platforms.

Our Security Management team diligently monitors compliance, ensuring all employees adhere to our clean desk and BYOD policies while maintaining ironclad device security configurations in collaboration with the Everlaw IT team. This proactive security governance helps maintain the high trust our clients place in our ability to safeguard sensitive legal data.

Training & Awareness

We recognize that the foundation of robust security and privacy practices lies in continuous education and awareness. Our comprehensive training program is designed to empower every employee – from newcomers to seasoned professionals – with the knowledge and tools they need to uphold our high standards of data protection, compliance, and ethical conduct.

Onboarding and Continuous Education

Every new member of the Everlaw team begins their journey with us by participating in an in-depth orientation session focused on security, compliance, and data privacy. This foundational training ensures that from day one, our employees are aligned with our core values and understand their critical role in protecting client information.

Annual Live Training Sessions

Security and privacy are dynamic fields, and staying ahead requires an ongoing commitment. That's why we host annual live training sessions for all staff, regardless of their tenure. These interactive sessions are designed to engage employees in a meaningful dialogue about real-world security challenges and best practices. By simulating scenarios and discussing recent case studies, we foster a hands-on understanding of how to apply security principles in everyday activities.

Role-Specific Training

Recognizing that different roles entail different risks and responsibilities, Everlaw provides tailored training that's specific to the functional roles of our team members. Updated annually, this role-specific training ensures that each employee's knowledge is current and relevant to their specific duties, enhancing our collective ability to safeguard sensitive information effectively.

Ongoing Awareness Campaigns

Our Security Management team leads the charge in keeping security and privacy at the forefront of everyone's mind throughout the year. Through a mix of email bulletins, visually engaging posters strategically placed around the workplace, and regular presentations, we keep the conversation about security ongoing. Supplemental materials, such as quick-reference guides and FAQs, are also provided to reinforce daily best practices.

Beyond security and privacy, Everlaw's training program encompasses critical aspects of regulatory and compliance education. This ensures that all employees are well-versed in the legal and regulatory frameworks that affect our business and our clients. Regular updates on new regulations and compliance requirements through the use of email, posters, presentations, and other supplemental materials are key parts of our commitment to operational excellence and legal adherence.

Third-Party Risk Management

Recognizing the critical role of external vendors and suppliers in our operations, Everlaw implements a stringent third-party risk management program. This program initiates a thorough security and privacy assessment for each potential third party to ensure their practices align with our rigorous security requirements.

Comprehensive Evaluation Process

Prior to any contractual engagement, our evaluation process involves not only the Security Engineering team but also the Governance Risk and Compliance team, the Operations team, and the Finance team. This cross-departmental approach ensures that all potential vendors and suppliers meet Everlaw's high standards in security, operational integrity, and financial stability.

Ongoing Oversight and Collaboration

Once onboarded, third-party relationships are continually monitored. Our teams perform regular reviews and audits on critical vendors to ensure ongoing compliance with Everlaw's privacy and security standards. This vigilance helps manage and mitigate risks associated with external collaborations, safeguarding our operations and data across all touchpoints.

Independent Assessments & Certifications

To validate the effectiveness of our internal controls and practices, we engage in rigorous annual independent audits conducted by reputable third-party firms.

Our audit regimen encompasses an array of internationally recognized standards, ensuring comprehensive coverage across all critical aspects of our operations. Customers interested in reviewing our security credentials can obtain the latest certification documentation by reaching out to their Customer Success representative.

SECURITY ACHIEVEMENTS AND CERTIFICATIONS

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations

Information Security Management System
ISO 27001
Certified

Information Security Management
ISO 27017
Certified

CYBER ESSENTIALS
CERTIFIED PLUS

AUTHORIZED
StateRAMP

FedRAMP
NIST 800-53

As you consider our security practices, detailed in this white paper, we encourage you to visit Everlaw's Data Security and Compliance page.

SOC 2 TYPE 2

To request a copy of Everlaw's SOC 2 report, contact your Customer Success representative.

SOC 3

Download Everlaw's SOC 3 report here.

ISO 27001:2022

Download Everlaw's ISO/IEC 27001 certificate here.

ISO 27017:2015

See Everlaw's ISO/IEC 27017:2015 certificate here.

CYBER ESSENTIALS PLUS

You can view our certification details on the NCSC.gov.uk site.

FEDRAMP

Everlaw has achieved FedRAMP Moderate Authorization for Everlaw's federal cloud. The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. federal government program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud products and services.

Government customers can learn more about our FedRAMP authorization here. You may also request Everlaw's FedRAMP package through the FedRAMP Program Management Office using its package request form.

PRIVACY FRAMEWORKS

GDPR

HIPAA

CCPA

STATERAMP

Everlaw has achieved StateRAMP Moderate Authorization. This authorization ensures Everlaw's security and risk standards meet the critical needs of state government agencies who can securely implement Everlaw's platform to manage litigation, investigations, public records requests, and collaboration.

Click here to see Everlaw's StateRAMP listing and learn more about the program.

Everlaw is trusted by the DOJ, all 50 state attorneys general, Fortune 500 companies, and Am Law 100 firms because we set the bar in cloud security.

Access Management

We employ a sophisticated role-based security model to govern access within our production network, ensuring that sensitive data and system operations are shielded from unauthorized access.

Principle of Least Privilege

Access to our production environments is rigorously controlled through the principle of least privilege. This means each team member is granted the minimum level of access necessary to perform their job functions effectively. We extend this careful approach to all areas, ensuring that security is never compromised.

Authentication

Multi-factor authentication is mandatory for accessing the AWS console and the administrative areas of the Everlaw platform, providing an added layer of security that helps thwart unauthorized access attempts.

Controlled Access Based on User Roles

Access to our platforms, including critical production environments, is strictly role-based. This ensures that every access request aligns with the user's defined job responsibilities. All access requests undergo a rigorous review process, initially by the user's manager and subsequently by other relevant parties, such as our Legal team, when necessary. This multi-tiered review guarantees that access is appropriate and justified.

Special Measures for System Administrators

The ability to create or modify user access accounts and privileges in the production environment is restricted to a limited number of qualified system administrators. This control is crucial in maintaining the integrity and security of our systems.

Logging and Audit Compliance

Every request for access is logged, and comprehensive audit trails are maintained. This not only helps in tracking and managing access but also supports our compliance initiatives. We also conduct quarterly access reviews for all privileged users to ensure ongoing compliance and address any potential security gaps promptly.

Change Management

Changes to both infrastructure and software are developed and tested in a separate development or test environment before implementation. The Everlaw Configuration Management Policy dictates that all changes must be documented and approved by the Configuration Change Review Group (CCRG). The CCRG consists of cross-functional experts and ensures that all changes to the Everlaw platform meet our strict standards for quality and security.

Security Impact Analyses

Changes with potential security implications are subject to a security impact analysis. This analysis is crucial in identifying potential risks and determining necessary mitigating actions to maintain our platform's integrity and security.

Emergency Changes

For urgent modifications, Everlaw employs a formalized emergency change management process that maintains rigorous review and approval standards but operates at an accelerated pace. This ensures that even in urgent situations, changes are implemented without compromising security or performance. All necessary approvals are obtained and documented before any emergency change is initiated.

Consistency Across Networks and Applications

Our change management procedures apply uniformly across the board – from network device adjustments to application development. Every change is logged, analyzed for security implications, and must receive formal approval before implementation.

Documentation and Accessibility

Change management policies and procedures are comprehensively documented and reviewed annually to adapt to new challenges and regulatory requirements. These documents are readily accessible to all Everlaw employees, stored in a shared folder and on the company intranet, ensuring that our team is always informed and compliant with the latest standards and practices.

Physical Security

A comprehensive security program extends beyond digital assets to include the physical premises. We implement rigorous physical security measures to ensure that access to our corporate offices is carefully controlled and constantly monitored.

Controlled Access

Access to our facilities is limited to specifically authorized personnel whose job functions necessitate it. Our visitor management process is designed to balance security with accessibility. All visitors are required to sign in upon arrival and must be accompanied by an Everlaw employee throughout their visit to ensure we maintain a secure environment while facilitating necessary external interactions. Once access to our facility is no longer required, due to changes in employment status or job function, we promptly revoke access.

Data Center Security

Everlaw's operations are securely hosted on AWS cloud servers, leveraging advanced infrastructure to provide robust data protection and high availability. Our services span multiple global jurisdictions to ensure localized compliance and optimal performance. Specifically, we operate in the following AWS cloud hosting regions:

/ United States: U.S. East and West Regions

/ Canada: Central Region

/ Australia: Asia Pacific, Sydney Region

/ United Kingdom: London Region

/ European Union: Frankfurt Region

AWS Security Credentials

AWS has achieved SOC 1, SOC 2, and SOC 3 certifications, along with ISO 27001 and FIPS validations. These certifications testify to AWS's commitment to maintaining high security and privacy standards, aligning with numerous legal and security frameworks globally.

EVERLAW'S GOVCLOUD OFFERING

Everlaw's Federal Cloud offering is hosted exclusively on AWS GovCloud. This specialized hosting environment is designed to meet the stringent requirements of U.S. federal agencies, including AWS's FedRAMP authorization and operations exclusively managed by U.S. citizens on U.S. soil.

For further information about AWS's security measures, practices, and compliance certifications, please refer to their detailed documentation on security practices and security compliance.

Secure Architecture

Everlaw's cloud infrastructure utilizes Amazon Web Services to host our application, all customer data (or case materials), and backups with optimal security. This setup ensures the safeguarding of sensitive information and system operations.

Network Isolation with Amazon Virtual Private Cloud (VPC)

Everlaw enforces a secure environment within our AWS-hosted framework. By deploying Amazon VPCs, Everlaw's services operate within separate, secure virtual networks. These networks are isolated from other external traffic, with connectivity managed precisely through advanced firewall configurations.

Management Subnet

Each VPC contains a management subnet that provides the Everlaw environment with security and management functionality. This includes logging and monitoring, vulnerability scanning, and other management tools. Access to this environment is strictly restricted to Everlaw personnel only, using encrypted channels and MFA.

Secure Cloud Practices

We ensure endpoint protection in hosting environments, including antivirus systems that are regularly updated following critical security patches or releases, consistent with Everlaw's server change control policies.

Synchronizing Network Time

Network Time Protocol (NTP) is essential for maintaining accurate and synchronized time across computer systems, which is crucial for security mechanisms, logging, and time-sensitive applications. Accurate timekeeping enables precise event correlation, supports authentication protocols, and ensures reliable logging for incident response and forensic investigations. In our systems, we use the systemd-timesyncd service for time synchronization, utilizing NTP servers provided by NIST, as detailed at NIST Internet Time Service. This practice is critical for maintaining consistency in transaction timestamps, data logs, and other time-sensitive operations that customers perform on our platform. This approach not only helps in protecting our infrastructure from potential security threats that could exploit detailed configuration data but also ensures that every client interaction remains consistent and reliable.

Data Security Enhancements

Everlaw employs private subnets that use private IP addresses to handle internal operations securely, while managing all public internet traffic through carefully configured AWS security groups. This strategic control helps maintain the integrity and confidentiality of data interactions.

Encrypted Communications

All communications between Everlaw clients and our platform, as well as exchanges with third-party applications, are protected via HTTPS using transport layer security (TLS). This encryption ensures that all data transmitted remains secure and private.

Encryption at Rest

To protect data at rest, Everlaw uses AWS's default encryption service, which employs the advanced AES-256 encryption standard. This feature automatically encrypts all data stored on disk, including at the database level, enhancing the security measures against potential data breaches.

Application Security

Everlaw is committed to safeguarding customer data through effective security practices embedded throughout our development lifecycle. Our Secure Development Lifecycle (SDLC) emphasizes the importance of security from the ground up, integrating key practices to minimize vulnerabilities and enhance software reliability.

Focused Developer Training and Review Processes

An essential element of our SDLC is the ongoing professional development of our development team. To equip them for the evolving landscape of cybersecurity threats, we provide continuous training focused on emerging challenges, with a particular emphasis on the vulnerabilities outlined in the OWASP Top 10 security risks.

To integrate security seamlessly into our development process, we conduct thorough design and code reviews, employing advanced tools such as dynamic application security testing, software composition analysis, and static application security testing. These methodologies are critical in ensuring that every phase of software development adheres to the highest standards of data protection and maintains the structural integrity of our systems.

Error Management and Data-Handling Techniques

Our development process incorporates error handling, comprehensive logging, and a file integrity manager to track and mitigate potential issues swiftly. Input validation and strong encryption protocols are systematically employed to secure data at all points of interaction, thereby preventing common vulnerabilities such as improper data handling and leakage.

Continuous Security Training and Penetration Testing

Our engineers undergo annual secure code training, focusing on the most current security risks, common threat agents, and effective security controls. This training ensures that our team is proficient in identifying and addressing potential security issues during development. Moreover, Everlaw engages third-party security experts to conduct thorough penetration tests on our web applications at least once a year. These tests are essential for identifying vulnerabilities that might not be detected during internal reviews, allowing us to rectify them proactively.

Security Monitoring & Rapid Response

Our team of security and site reliability engineers play a crucial role in actively monitoring our system configurations and any deviations from expected activity. This continuous scrutiny helps us ensure that Everlaw's infrastructure remains secure and that our clients' data is protected against both current and future cyber threats. Our dedicated on-call team is equipped to handle specific alerts, ensuring immediate action is taken when necessary. To maintain a vigilant watch over our systems, we employ a robust suite of security measures:

- **Vulnerability scanning:** We systematically scan our systems to identify and address vulnerabilities before they can be exploited.
- **Intrusion detection and prevention systems:** These critical tools help detect and prevent unauthorized access, providing an additional layer of security.
- **Real-time alerts:** By subscribing to authoritative sources like US-CERT, we stay updated with the latest security advisories and threat intelligence, enabling us to react swiftly to emerging threats.

Everlaw's monitoring strategy incorporates both open-source and commercial tools, including host intrusion detection software, to comprehensively assess our network integrity. Additionally, we leverage the detailed security logs generated by AWS firewalls, which allow us to monitor and investigate any suspicious activities effectively.

Data Security

All customer data, both in transit and at rest, is encrypted. We employ hybrid encryption methods to protect data consistently across all interfaces and storage systems, to align with the standards specified in NIST Special Publication 800-53.

Encryption in Transit

Everlaw secures application data transmissions using HTTPS, ensuring that all customer data is encrypted while in transit. We utilize TLS version 1.2 or higher to safeguard HTTPS communications comprehensively.

Additionally, our email systems employ opportunistic TLS encryption to secure email exchanges, enhancing the privacy and integrity of communications.

Encryption at Rest

For data at rest, Everlaw leverages AWS's AES-256 encryption to secure data stored on disks. We extend this protection to snapshots and backups, ensuring that all stored data is encrypted with AES-256, thus securing inactive data on any device or network from unauthorized access.

Integrating Data Protection and Privacy

In alignment with our SDLC, Everlaw integrates data protection and privacy from the initial design phase of each feature and product. By embedding organizational and technical safeguards early, we ensure that personal data is processed only for its intended purpose. Our adherence to detailed information security policies and procedures guarantees the security, availability, processing integrity, and confidentiality of customer data at every step.

Through these uncompromising encryption practices and proactive design strategies, Everlaw remains committed to the highest level of data security, ensuring that our clients' information is protected against evolving cyber threats.

Data Backup & Deletion

Everlaw backs up client data every three hours and stores the data in private S3 buckets for storage. Everlaw platform users with delete permissions in database settings can delete documents from the database. Once case materials have been marked for deletion, we store the data in our backup environment for 120 days. Per our terms of service, we keep certain administrative data that is anonymized to help improve our service. Under no circumstances will we keep case materials or other attachments.

Utilizing AWS Storage Solutions

To optimize data storage and security, Everlaw leverages AWS storage classes, designed to store data across multiple availability zones within the designated AWS geographic region. These availability zones are strategically set up to be physically separate and isolated, yet interconnected with low latency, high throughput, and highly redundant networking. This infrastructure setup ensures that client data is securely stored and remains accessible without the risk of significant downtime or data loss.

Product Security Features for the Everlaw Platform

We are dedicated to providing robust security features within our platform to enhance user experience and data protection. Here's an overview of some key security functionalities that ensure our customers can manage and safeguard their legal data effectively:

Single Sign-On (SSO)

Everlaw supports single sign-on through the SAML 2.0 protocol, allowing users to access our platform using their organization's existing LDAP or other SSO systems. This integration simplifies the login process and enhances security by reducing the number of passwords users need to manage.

Multi-Factor Authentication

To further secure customer accounts, Everlaw offers multi-factor authentication at no additional cost. This security measure can be enforced across the organization, requiring users to provide a second form of verification – such as a code sent to their email or mobile device – when logging in, thereby significantly enhancing account security.

Granular Permissions

Everlaw enables precise control over access rights within the platform, which is critical for maintaining the security and efficiency of data reviews. Administrators can set detailed permissions, allowing users access only to the tools, data, and work products necessary for their specific roles and responsibilities.

User Analytics and Monitoring

Our comprehensive analytics tools provide administrators with insights into both live and historical user activity within their projects. Everlaw's User Activity logs all user activity including login, logoff, and unsuccessful login attempts, enabling proactive oversight and security management.

Secure In-Platform Sharing

Everlaw's in-platform messaging system allows for secure, direct communication and document sharing among users. This feature eliminates the need for downloading and sharing sensitive documents through less secure channels like email, enhancing both usability and security.

Flexible Sharing Options

Everlaw also facilitates secure collaboration with third-party experts or co-counsel by allowing users to create, organize, and share specific document subsets within a secure project environment. This capability ensures that external parties have access only to the necessary documents, reducing the risk of broader data exposure.

Location Approval Lists (IP Range Blocking)

Recognizing the security challenges of remote work, Everlaw allows project administrators to restrict access based on IP address and geographic location. This feature is particularly useful for organizations looking to tighten security protocols and ensure that only authorized users can access project data from approved locations.

Intelligent Innovation: Generative AI at Everlaw

All the work we do is guided by our generative AI principles, which focus on control, confidence, and transparency. These key principles guide us to deliver responsible generative AI to our customers. We believe this new generation of AI will be transformative over the long term, rather than a flash in the pan. Thus, we are more interested in being the best at generative AI than being the first. So while we have multiple teams working on our generative AI features, they are working under the guidance of these principles and collaborating with our customers to ensure we are delivering features consistent with our long-term philosophy of acting with integrity and discipline: doing the right thing and doing it the right way.

Transparency, Privacy, and Security

Consistent with our strong security culture, if we use any third-party AI tool, our Legal and Security teams will evaluate the specific system's operational approach, the data that will be processed, and the safeguards that are in place to protect the data and then review the governing legal terms to align with our commitments to our customers. We will only select third-party AI tools with capabilities to disallow them or others from training models on our customers' data. We will notify our customers about the third-party tools we are using. We'll also ensure that our security obligations, such as FedRAMP, are met before offering any such tool to customers that rely on those obligations.

Control

Customers will be able to opt in or out of using our generative AI tools. If they choose to use these tools, any interactions with generative AI should be clearly indicated to the user.

Confidence

Generative AIs can provide immense value, but they can also make mistakes. We want to ensure that users can develop confidence in their results. To that end, where possible, we will take the following actions:

/ Tailor generative AI features to specific use cases that we believe perform reliably.

/ Require the AI to cite specific, immediately verifiable passages of text from users' evidence as justification for its responses.

If that is not possible, ensure that users have clear access to any evidence provided as context to the AI, so that they may perform a more comprehensive validation if they so choose.

How does Everlaw^AI Assistant work?

Everlaw^AI Assistant combines LLMs developed by OpenAI with the data inside Everlaw's purpose-built platform. Everlaw^AI Assistant provides a native AI experience that is relevant to your teams and your litigation and investigation use cases, all in a way that respects the privacy of your data. To learn more about Everlaw^AI Assistant, visit our Everlaw^AI Assistant product overview.

Privacy First: How Everlaw Protects Your Confidential Data

To the extent any case materials you submit to Everlaw^AI Assistant are subject to any applicable privacy law, the terms of the Data Processing Addendum, or the data processing addendum that is applicable to your account apply. In addition, your data is subject to the same confidentiality requirements as stated in your agreement with Everlaw.

Best Practices for Using the Everlaw^AI Assistant

Large language models (LLMs) are systems trained on a huge corpora of text. Based on this training, these models are adept at predicting the next word given a sequence of preceding words. This is the core capability of LLMs.

While some compelling functionality can be built from this core capability, it is important to remember that LLMs are probabilistic language machines with no notion of things like truthfulness, accuracy, or intent. LLMs are trained to produce fluid text, not accurate responses. When using any feature backed by an LLM, it is important to remember that these systems can and do produce inaccurate, false, and/or misleading statements, even when additional guardrails have been put in place.

When using Everlaw^AI Assistant features, we encourage you to exercise your own judgment and expertise to validate responses. Human validation is particularly important when you are using the system to create factual claims about people or events, or work product you intend to share with others. We require Everlaw^AI Assistant to cite specific, immediately verifiable passages of text from users' evidence to make human review and validation intuitive. For more information, check out our Knowledge Base.

Data Security with Everlaw^{AI} Assistant: Staying Within Everlaw

When you use EverlawAI Assistant, each data request is sent to our AI service provider individually, over an SSL-encrypted service, to process and send back to Everlaw. The data you submit and the responses you receive via EverlawAI Assistant are not used to fine-tune or improve our AI service provider's models or service or shared between customers. Our AI service provider does not store the data you submit or the responses you receive.

Currently, as of the date this paper was published, our AI service provider only has servers in the United States. Everlaw supports our customers' compliance with the GDPR and the CCPA. We will process and transmit data for EverlawAI Assistant in accordance with our Data Processing Addendum and your individual agreement with Everlaw.

Everlaw believes that with the right implementation, the benefits of this technology for legal professionals will be significant. Everlaw aims to be the legal industry's most trusted AI platform, and we'll work every day to earn that trust.

Conclusion

Everlaw remains unyieldingly dedicated to safeguarding our clients' sensitive information with advanced, proactive security measures. Everlaw's commitment extends beyond mere compliance with industry standards. We strive for excellence in every facet of our security protocols to anticipate future challenges and evolve our defenses proactively.

As we continue to enhance our security practices, Everlaw's focus remains on maintaining the trust and confidence of our clients. We are not just protecting data; we are preserving the integrity of legal processes and the privacy of the individuals they affect. Moving forward, Everlaw will relentlessly improve and innovate, ensuring that our security measures are as dynamic and resilient as the legal professionals we serve.

About Everlaw

Everlaw helps legal teams navigate the complex ediscovery landscape to chart a straighter path to the truth. Trusted by Fortune 100 corporate counsel, 93 of the Am Law 200, and all 50 state attorneys general, Everlaw's advanced technology empowers organizations to tackle the most pressing technological challenges—and transform their approach to discovery and litigation in the process.

Contact us

US
2101 Webster St.
Suite 1500
Oakland, CA 94612
844.everlaw

UK
32-38 Scrutton Street
London, EC2A 4RQ
0800.068.9249

everlaw.com