How Filevine Approaches Security

WHITEPAPER

Filevine

Partners in safegaurding legal data

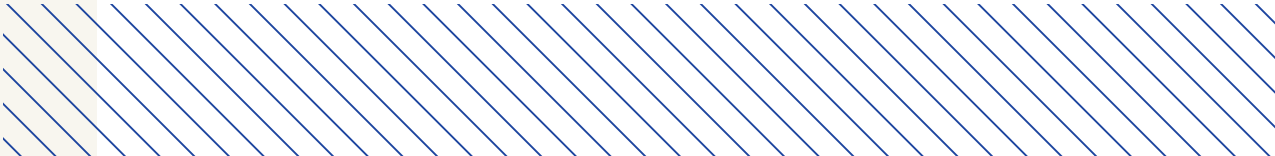
Filevine is dedicated to helping you comply with your ethical duty to protect your clients' information. Our team of experienced security professionals is dedicated to protecting your information so you can better serve your clients and manage your practice with confidence.

As cyber threats proliferate, data security has become a growing concern for legal professionals. ABA Model Rule 1.6 charges all lawyers with the responsibility to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." The ABA Standing Committee on Ethics and Professional Responsibility has further stated that lawyers must "understand technologies that are being used to deliver legal services to their clients [and] use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer."

With this in mind, this paper aims to describe some of the sophisticated security controls Filevine uses to protect your information. This document is not intended to address Filevine's total security landscape. Instead, it explores some of the greatest security threats legal professionals face today, and describes several powerful techniques we employ to safeguard your data.

One of the most effective ways to safeguard data is to have security experts who are familiar with the threats facing the legal vertical and experienced in protecting law firms and their highly confidential data. The Filevine security team has both, and the team has recognized security certifications in many disciplines. These certifications include:

CISSP, GSLC, GCPM, GLEG, GWAPT, GAWN, CIPP/US, GPEN, GSOC, CISA, ITIL v3 Foundations Certification, G2700, GISP, Security+ and Testout Security Pro.



Filevine also provides ongoing security training to its workforce to keep pace with the evolving cyber threats and has implemented best-in-class security technology to protect your data from the emerging risks against your practice. These risks include, but are not limited to the following:

Risk #1: Ransomware

One of the most common cyber attacks currently facing lawyers is ransomware. These attacks often begin with a phony email (or phish) which fools a firm employee into opening an infected Word document or other attachment which then launches a malicious program infecting the computer. With access to one computer, the attack can spread throughout the network by exploiting vulnerabilities in older versions of Server Message Block (SMB), which provides access to local files, network file shares, printers, and backups. This attack allows a cybercriminal to encrypt the entire system so users cannot access the computers and demand a ransom to restore access to the users.

Ransomware attacks against lawyers are on the rise, targeting firms of all sizes and geographic locations. This often results in the loss of all access to records and client data—sometimes permanently. Firm operations often screech to a halt, sometimes for months, as managers scramble to recover their data. In the meantime, bad press and client dissatisfaction grows.

HOW FILEVINE HELPS PROTECT YOU

Built on AWS's Trusted Platform

Filevine is a legal operating core built on AWS—which is considered to be one of the most reliable, highly available, and secure global infrastructures available. This is the same platform used by government intelligence agencies, the Department of Defense, and some of the world's largest businesses and financial institutions (for example: Dow Jones, Capital One, GE, Johnson & Johnson, NASA, Disney, Netflix, BBC, Adobe, Turner Broadcasting, Facebook, Twitter, and millions of others). Filevine leverages AWS's FIPS 199 "Moderate" level IaaS and PaaS platforms to ensure that your data is always available and protected.

Filevine believes in defense-in-depth, leveraging HA systems, solid backup practices, and best-in-class of class computing practices to provide solid protection from ransomware events and other disasters. Defense-in-depth means that Filevine does not rely on a single control or even two to protect a security risk area. Typically, three or more security controls are designed to protect each aspect of the security program protecting the Filevine platform.

Redundant Data Backup

Filevine automatically conducts daily backups of your data. These backups are redundant and cross multiple availability zones and data centers. To provide an added layer of security, backup data is encrypted using AES 256 to protect it at rest. Even in a dire situation, should a firm employee introduce malware into your system, your data in the Filevine system should not be impacted. We regularly test the ability to restore these backups to ensure prompt recovery of your data in the event of a disaster.

Disaster Recovery and High Availability (HA)

A fire, flood, or ransomware event can damage files and servers or lead to lost productivity and billables. Filevine ensures that no matter what happens to your physical office, as long as you can get an internet connection, you can immediately access your Filevine files and operate your practice remotely. Our Disaster Recovery Plan ensures that the Filevine platform has redundant switching, routing, and power for the supporting infrastructure systems to keep the platform up and to keep you productive. These investments make Filevine a central part of your firm's Disaster Recovery and Business Continuity Plans. No business continuity plan would be complete without HA systems.

Furthermore, our HA computing environment spans multiple availability zones with local system redundancy, to ensure that should any part of the system fail—such as operating systems, web services, databases or file storage—there is a redundant system ready to pick up the load.

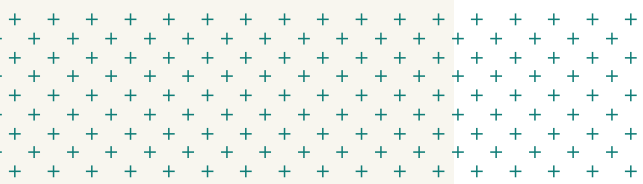
Up-to-Date Server Software

Filevine keeps its servers patched with the latest security updates to protect against new and emerging security threats. We regularly refresh our server infrastructure through automated deployments to ensure pristine, fully patched, and secured server images are deployed into production.

Physical Data Security

Filevine leverages AWS data centers to ensure they are secure, offsite locations with redundant power supply and cooling systems. This provides added stability and redundancy to keep the Filevine systems online, accessible, and secure. Physical access points to server rooms are recorded by closed-circuit television cameras and access is monitored and controlled by professional security staff.

Physical access to Filevine office locations is provided via electronically managed security systems and access devices. Filevine facilities are locked at all times and access is only granted with the authorized security application from previously authorized devices, ensuring that only Filevine personnel or approved visitors enter the building(s).



Risk #2: Password and Identity Theft

The Verizon 2019 Data Breach Investigation Report[1] found that 80% of hacking- related breaches are due to compromised, weak, and reused passwords. These data breaches can result in tremendous financial and social costs to firms and individuals. When large data breaches occur, the criminal underground often hoards these breached usernames and passwords in large databases spanning many years and many successful attacks. Using this historical information, and human tendencies to reuse passwords we have memorized, cybercriminals can often discover trends or patterns over time, allowing them to sometimes guess passwords for other cloud systems.

HOW FILEVINE HELPS PROTECT YOU

Identity and Access Management (IAM)

Filevine has invested heavily in a best-in-class IAM system to manage multiple security controls related to passwords. These security layers ensure Filevine employee's passwords and access are protected with multiple controls and sophisticated protection. These layers include but are not limited to role-based access controls (RBAC), enforcement of strong passwords, two-factor authentication (2FA), password session time-outs, and account expiration for frequent, unsuccessful login attempts. These access controls give Filevine employees and customers greater control over who has access to information.

Role-Based Access Control

This allows Filevine administrators and firm administrators to easily manage access to their confidential information. Access is granted or restricted based on predefined job roles inside the organization. If an individual changes roles, their access changes as well. This makes it easier to authenticate, authorize, and audit access to systems and case data. Firms can also delegate or provide limited access to clients or outside counsel without compromising security.

Strong Passwords

When you create a Filevine user account or update your account's passwords, Filevine requires a complex password of at least eight (8) characters and at least one (1) non-letter character. All passwords are salted and one-way hashed in storage. Filevine administrative accounts have even stronger password requirements to ensure access to the Filevine platform is secure.

Two-Factor Authentication (2FA)

Filevine administrative accounts utilize 2FA to provide an additional level of authentication, dramatically reducing the risk of hacking and data theft. 2FA is a combination of something you know, such as a password, and something you have, such as a soft token, hard token or some other one-time password (OTP)

technology such as Google authenticator. Due to this extra level of security for Filevine users, it's much less likely that the theft of a device or password will result in unauthorized access to data. Filevine has further enhanced the platform by enabling this same 2FA feature for Filevine's customers so their users are equally protected from password re-use or theft.

Failed Login Attempts
When Filevine user accounts reach an unacceptable threshold for failed login attempts, the accounts are automatically locked and a time escalation algorithm kicks in to prevent additional failed attempts to access the account. This practice reduces the likelihood of unauthorized access by someone who has identified a valid username but is attempting to brute force or guess the password.

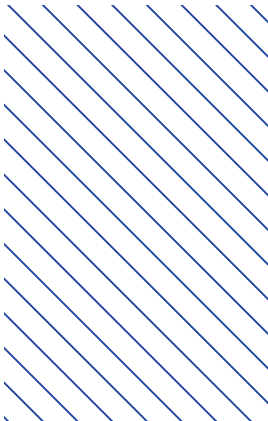
Risk #3: Website Security

The VDIR report for 2019 shows that web application attacks are among the most common attacks for almost every kind of business reviewed in the report(1). Many SaaS platforms, websites and web applications are targeted by hackers in an attempt to gain unauthorized access to large quantities of sensitive information. To prevent these attacks from being successful, Filevine has continued to follow a defense-in- depth approach to protect this important information. This approach includes writing secure code, testing the code, protecting the code from attack, internal testing, and hiring external security experts to make sure we didn't miss anything.

HOW FILEVINE HELPS PROTECT YOU

Secure Software Development Lifecycle (SDLC)
Filevine follows a secure SDLC methodology aligned with the OWASP Top 10(2). The OWASP Top 10 are the most common security flaws that hackers try to exploit to gain unauthorized access to the site. Filevine developers attend annual training on OWASP Top 10 practices and development code architects perform peer code reviews on code before it goes into production. DAST and SAST tools are also used to reduce the likelihood of security defects making their way into production.

Penetration Testing
Filevine utilizes industry-recognized security experts to annually test the Filevine platform to ensure our websites, web applications, APIs, and related services are safe and secure. We hire different White Hat hackers every year to ensure we are getting a fresh approach to testing the platform and to ensure the platform is robust and secure.



In Transit Data Encryption

Filevine encrypts all data traffic using TLS 1.2 encryption, allowing for data to flow securely between your browser and the Filevine platform. Because all data goes through at-rest using AES 256 encryption, if in the unlikely event that a data center was compromised, any data acquired would be unreadable.

Server-Side Verification

All data is validated server-side to ensure that data coming from the customer will not allow unauthorized access or the injection of harmful data.

Secured Database

Your most critical information, such as your client database, should not be accessible to anyone on the internet. Filevine only allows access to critical resources to a whitelist of Filevine's web servers. This means that when a user sends a request to the web server to access client data, the web server then sends that request to the database server. If the computer that originally sent the request is not from that whitelist, the database server will reject it. This provides an additional layer of security for the client data.

Restricted Access to Production Data

Unauthorized and unnecessary access to your data is prevented with Filevine. We operate under the principle of least privilege and restrict access to data in the production environment to a small number of administrators only.

Secure Document Download

Each time an authorized Filevine user requests to download a document from Filevine, the system will check that user's permissions to ensure that they are authorized to download that specific document. After confirming, Filevine generates a unique, one-time-use URL for each download. This unique URL is only accessible for 60 minutes to ensure that documents are not shared with unauthorized users.

Filevine also allows customers to grant permissions to their guest users so they can download documents. Filevine users can also determine how long download links will be valid.

Secure Document Upload

Filevine utilizes the web standard CORS (cross-origin resource sharing) to ensure uploads originate only from Filevine and cannot be uploaded from other browsers or web pages. All files are encrypted "in transit" with TLS 1.2. Once the data is received, we encrypt it with AES 256 for "at rest" storage.

Operational Security

Filevine maintains a Business Continuity plan and a Data Security Incident Response Plan, among other policies and procedures. Our team of data security,

compliance, and legal professionals are working diligently to obtain SOC2 certification, an effort that is on target for completion in Q4 2020.

Security Policies and Procedures
Filevine has created a detailed set of information security policies and procedures to govern the secure operations of the Filevine platform. These security policies include Access Controls, Database Security, Incident Response, Incident Management, Encryption, Remote Access, and numerous other control areas.

With these investments to address three of the most common cybersecurity risk areas for our customers, Filevine is well-positioned as a leader in the case management platform vertical, delivering a robust, secure and compliant legal core platform to our clients.

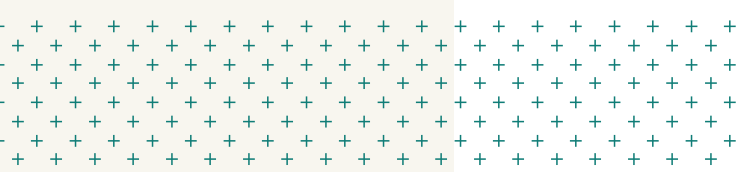
Security Certifications

Certified Information Systems Security Professional (CISSP) GIAC Security Leadership Certification (GSLC)
GIAC Certified Project Manager (GCPM)
GIAC Legal Issues in Information Technology & Security (GLEG)
GIAC Web Application Penetration Tester (GWAPT)
GIAC Assessing and Auditing Wireless Networks (GAWN)
Certified Information Privacy Professional (CIPP/US)
GIAC Certified Penetration Tester (GPEN)
GIAC Securing Oracle Certified (GSOC)
ITIL v3 Foundations Certification
Certified Information Systems Auditor (CISA)
GIAC Certified ISO-27000 Specialist (G2700)
GIAC Information Security Professional (GISP)
Security+
Testout Security Pro

References

1. https://enterprise.verizon.com/resources/reports/dbir/
2. https://owasp.org/www-project-top-ten/

If you have questions about security, or the other ways that Filevine can help your practice, give us a call or email us at info@filevine.com.



filevine.com