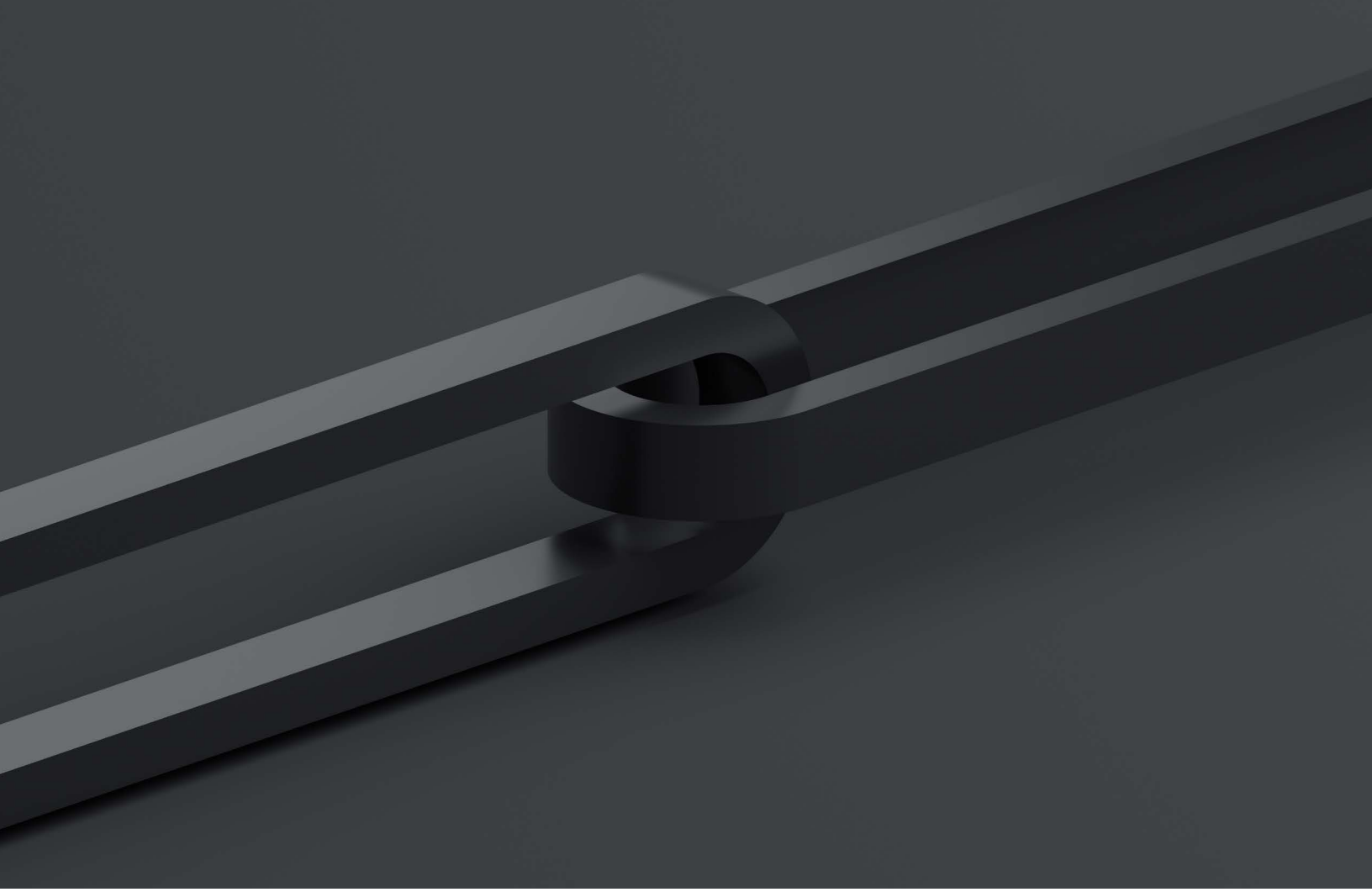
everlaw

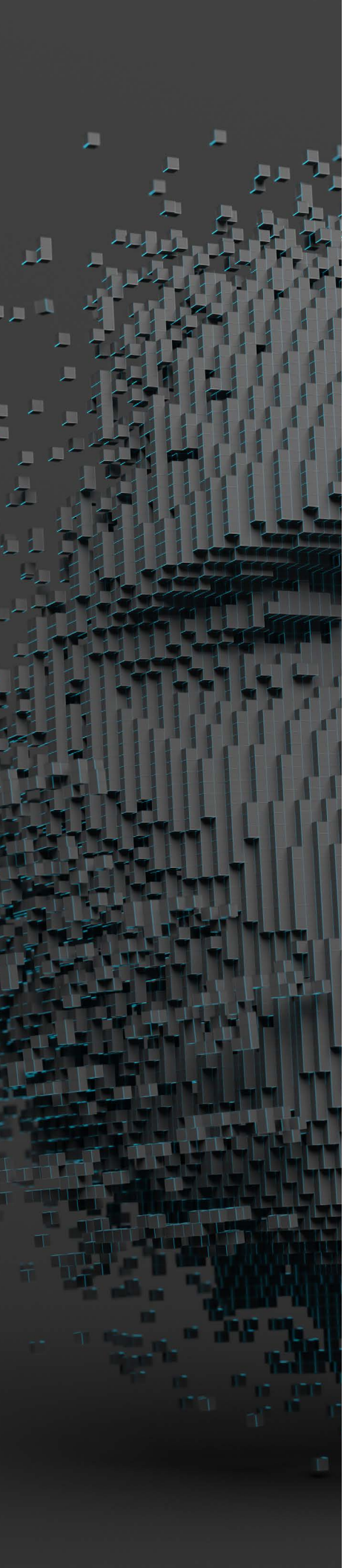
Cybersecurity in the World of Ediscovery

Tips and Considerations for Legal Organizations



Over the years, the legal industry has slowly shifted to remote-based collaboration, as organizations have found themselves working with legal teams in various locations. Global events have expedited this transition — it's now common to practice law remotely, and, as a result, cloud-based tools are becoming crucial to conducting business as usual. While many legal professionals already use cloud-based ediscovery tools, the broad adoption of remote collaboration has made them an absolute necessity.

Due to the increased dependence on these tools, security concerns have become top-of-mind for legal professionals. The collaborative nature of the litigation and discovery process inherently makes protecting sensitive and privileged data a top priority. And with new legislation, compliance with data privacy regulations and security certificates has become even more necessary. In short, security is more of a pressing issue now than ever before, especially in the legal world where protecting client information is sacrosanct.



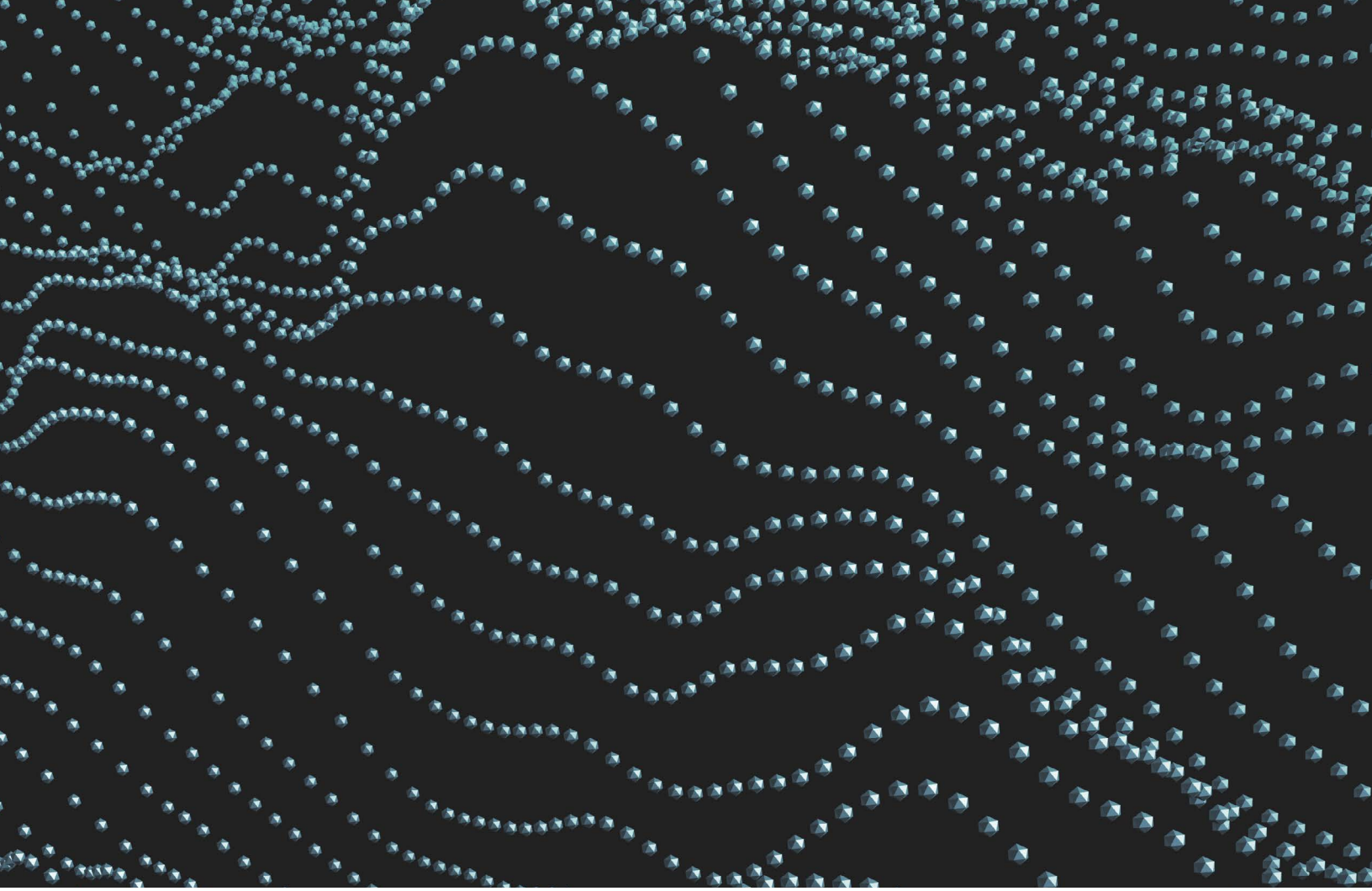
Why is Cybersecurity Important?

As cloud-based platforms have become more advanced, so have hackers' abilities to circumnavigate security measures. Over a period of six months, seven law firms were victims of cybersecurity breaches from hacker groups Maze and REvil. These security attacks highlighted a stark change in how hackers have customarily operated.

In early 2020, Maze began targeting law firms, threatening to release client data if the law firms didn't pay their ransom demands. Things escalated quickly in February when Maze released documents from Texas-based law firm Baker Wotring. The data in question included the Health Insurance Portability and Accountability Act (HIPAA) consent forms and pain diaries from personal injury court cases. Maze's tactics were unique: whereas other hacker groups typically threatened to block data access, Maze simply exposed a few documents to prove they had successfully hacked into these firms' databases.

Not to be outdone, REvil hacked Grubman Shire Meiselas & Sacks, a New York-based entertainment law firm, and threatened to expose client information from the likes of Madonna, Bruce Springsteen, U2, Nicki Minaj, and more. These legal documents contained everything from email addresses, phone numbers, and personal correspondence to nondisclosure agreements, contracts, and other wide-ranging information.

Previously, hackers would typically focus their attention on an individual lawyer via traditional methods, such as phishing and social engineering. However, modern hacker groups have developed more sophisticated methods (e.g., using remote access backdoors to hijack administrative controls and access client information) to hold legal organizations hostage.



These attacks demonstrate how much risk is involved when law firms are handling troves of privileged information. In the same vein, law firms can take security measures to ensure their clients' data is always secure. By using software that helps with data encryption, law firms can mitigate the headaches associated with hacker attacks.

In addition to protecting their data from malicious threats, legal organizations have found themselves facing an influx of new legislation from global governments, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and HIPAA. Lack of compliance with these regulations can result in severe financial penalties and unquantifiable loss of professional credibility. For example, penalties for not complying with the GDPR can be as high as €20 million (fees and punishment depending on several variables), and HIPAA penalty violations can be as high $50,000 (law firms can rack up a maximum of $1.5 million in fees per calendar year).

Cybersecurity Best Practices While Working Remotely

According to Ruth Hill Bro, co-chair of the American Bar Association's Cybersecurity Task Force, law firm employees working from home are appealing targets for cyber breaches. The global pandemic and new work environments have given hackers and scammers even more opportunities for data breaching. Ediscovery experts are encouraging law firms to perform risk assessments and complete all legal work on secure servers, using multi-factor authentication to access sensitive information.

While working from home, legal professionals may be accessing or transmitting confidential information concerning the firm and its clients.

As the Maze and REvil hacks demonstrated, a lack of security measures can lead to potential hacks and releases of private data.

Although there is no one-size-fits-all approach for maintaining cybersecurity while practicing law from home, below are some quick and easy ways legal professionals can protect their data from threats.

Ensure that devices have employer-provided security software with the latest manufacturer updates before accessing any remote systems. Additionally, when downloading sensitive data, be prepared to provide additional credentials to gain access.

Stay home — don't work from public places like coffee shops or while riding public transportation, where third parties might be able to view your screen and printed documents. It's best to avoid public Wi-Fi, opting instead for secure, password-protected home internet or a personal hotspot.

Be wary of emails originating outside of the firm that may be phishing attempts disguised as COVID-19 updates or revised company policies. When in doubt, don't click on any links in an email or download any attachments.

Shut down (instead of restarting) your laptop to clear temporary files and run updates every day. Power off your company-issued mobile device every night to allow for a full reboot to clear harmful files.

Conduct work-related communication on company communication systems, never via personal devices, or by posting on social media platforms.

Save company materials on devices configured with company-sanctioned anti-virus software, password protection, and secure network connections. Gain remote access only through a virtual private network (VPN) with end-to-end encryption. A VPN has a critical function when it comes to data protection: it establishes secured connections and encrypts all internet traffic, making online activities untraceable.

Conduct any collaboration — whether that's working on redactions, sharing documents, or communicating with colleagues — via a secured ediscovery platform. The more digital and unsecured channels a legal professional uses to conduct their work, the more prone they are to attacks from opportunistic hackers.

If you believe that a possible data security breach has occurred, inform your organization's designated security officer as soon as possible.

Choosing a Secure Ediscovery Solution

When legal organizations bring in new tools, the security and compliance of the solutions are instrumental in maintaining trust between legal professionals and their providers. It's critical for legal organizations to evaluate their ediscovery tools, not only for their functionality, but to ensure that proper cybersecurity considerations have been put in place to protect sensitive information. And that's why ediscovery providers need to take a holistic and comprehensive approach when it comes to implementing the right security measures and compliance programs for their platforms.

Compliance Considerations

For legal organizations, finding an ediscovery solution that properly prioritizes security and compliance is easier said than done. Prior to taking the initial steps on their ediscovery journey, legal professionals should keep in mind some key considerations before committing to a provider.

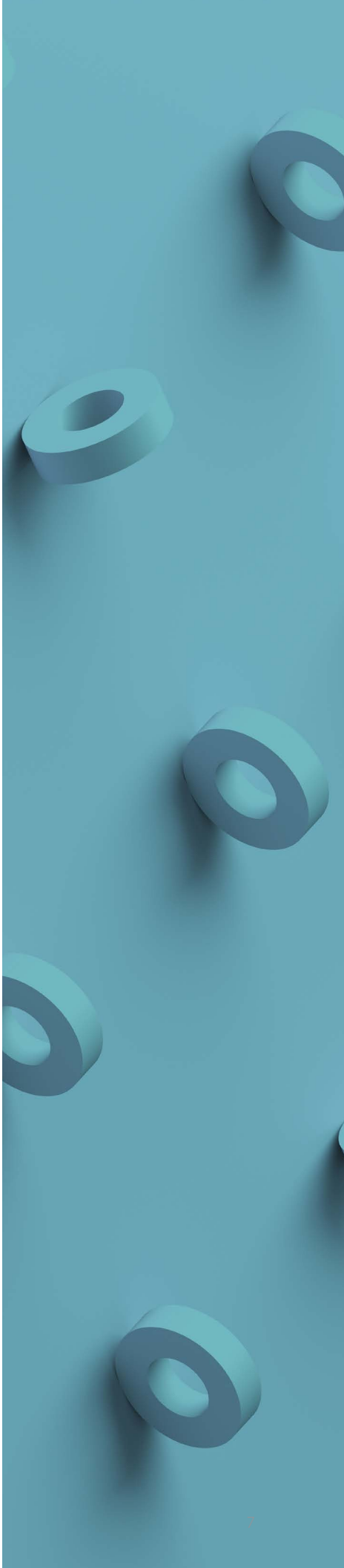
INTERNAL GOVERNANCE

An ediscovery provider should have a compliance program that establishes a formal system of internal control and should always ensure that their platform is secure. For example, this can include third-party audits to test the compliance program's operational effectiveness and practices, annual face-to-face security and privacy awareness training, and yearly policy, compliance, information security, and privacy training modules.

INDEPENDENT AUDITING AND TESTING

Speaking of audits, the right ediscovery provider should undergo rigorous security and privacy testing by independent third-party auditors. The stamp of approval of unbiased third-parties demonstrates a solution's security fitness. For example, Everlaw has achieved FedRAMP Moderate Security Authorization for its federal customer-specific platform, secured SOC 2 Type 2 certification in Security, Privacy, Confidentiality, and Availability, and completed voluntary independent audits for GDPR and HIPAA compliance.

For a company to receive SOC 2 Type 2 certification, it must have sufficient policies and controls operating to protect customers' data and must provide detailed evidence and pass independent testing of operational effectiveness through the audit testing procedures.



Functionality Considerations

In addition to ensuring that an ediscovery provider is compliant and up-to-date on the latest government rules and regulations, it's also critical for a solution to have the functionality to create a shared space that enables and enhances virtual collaboration. For one, that means there are features that allow for seamless collaboration with various internal and external partners, no matter their geographic location. Secondly, features should enhance security measures, protecting privileged information every step along the way. It's vital that an ediscovery solution has the capabilities that allow legal professionals to execute their work unencumbered.

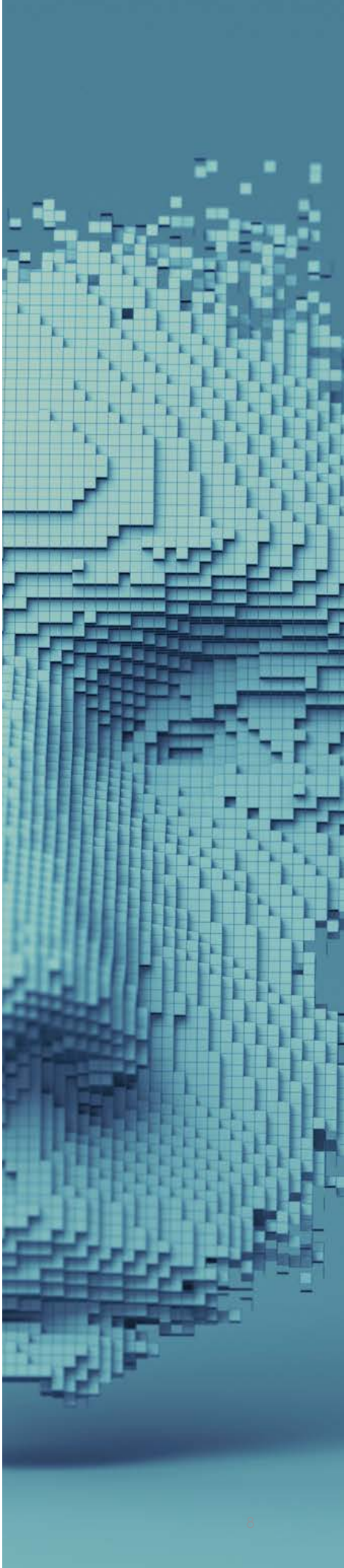
FEATURES THAT PROMOTE SECURE COLLABORATION

Legal teams frequently work cross-functionally with internal and external teams, so collaboration is fundamental to their success. Leveraging a secure ediscovery solution ensures that legal teams make the most of their time and provide access to privileged information to the right people. A consolidated platform centralizes communications, saving teams hours of lost productivity and reducing the risk of mishandled data. Innovative cloud ediscovery tools enable teams to share and communicate directly in the platform to promote secure, seamless collaboration.

Any cloud-based platform should ensure that the right members within a given legal team have access to the right data. For example, multi-factor authentication (MFA) and single sign-on (SSO) provide additional layers of security, which reduces the chance of unauthorized access to an account. Not only do these features improve security, but SSO also enhances the user experience by allowing users to log in via their organizations' existing directory service, eliminating the need to worry about managing yet another password.

Better security ensures that users can focus more on their work and worry less about their data getting into the wrong hands. For example, Everlaw has integrated these key security features to facilitate secured collaboration amongst legal teams:

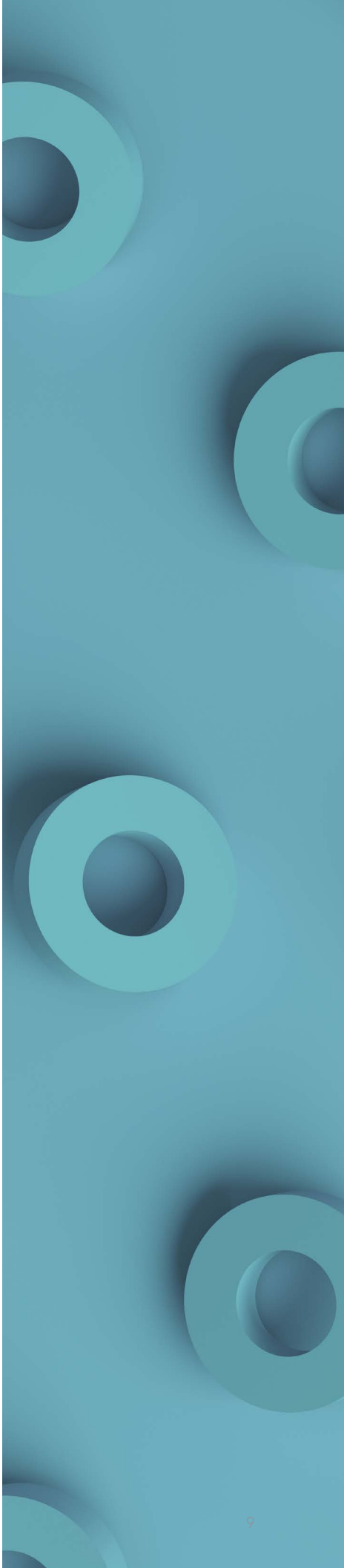
- Location Whitelisting: This feature gives organizations more control over who can access projects by allowing project admins to restrict access based on a user's IP address and country.
- In-platform Messaging: Keeping communication within a platform allows for direct sharing and communication between users, enabling users to bypass the typical process of downloading and sharing documents with colleagues via email and other forms of communication. This reduces tedious back-and-forth conversations and eliminates the need to attach sensitive documents in less secure channels.



- **Flexible Sharing Options**: Often, a review requires a third-party expert or co-counsel to access documents in order to complete a review project, offer an expert opinion, or manage project consultants. With this feature, users can organize, create, and share an appropriate subset of documents in a secure project, eliminating the risk of providing complete access to the entire document corpus.
- **Easy sharing of Productions**: Challenges, such as network interruptions, incomplete downloads, and other security vulnerabilities, can occur when sharing productions via traditional methods (e.g., downloading productions to a hard drive and then shipping them to an opposing counsel, or sharing via FTP connections). For a full production, or any of its subcomponents (e.g., load file and privilege log), this feature enables users to create secure, shareable links or email invitations. Additionally, users can set links to expire, and production access logs shine a light on the sharing and downloading activity for each production.
- **Granular Access Permissions**: Everlaw takes a granular approach to project permissions and gives project administrators precise control over user access. Furthermore, the document access management tool enables project administrators to customize access to subsets of documents by user groups. This level of customization is comprehensive across all areas of the platform, regardless of which features or functionality are in use. Additionally, users can easily turn these permissions on and off at any time. This helps legal professionals better organize their security settings and protect sensitive documents.

CLOUD SERVICE PROVIDER AND DATA CENTER SECURITY

Where and how an ediscovery provider stores data is a big indicator of whether it's truly serious about cybersecurity. For example, Everlaw's primary data source is on secure AWS cloud servers, which surpass industry standards for privacy and security. AWS has SOC 1, 2, and 3, ISO 27001, FedRAMP, and FIPS certifications, in addition to meeting compliance standards for many other legal, security, and privacy frameworks.



Final Thoughts on Cybersecurity in the World of Ediscovery

More than ever, prioritizing security can help organizations maintain business continuity and build their customers' and partners' trust and confidence. It's imperative for legal professionals to find an ediscovery solution that prioritizes protecting data, has a continued commitment to security, values transparency regarding policies and practices, and has third-party security certifications. Despite this, the onus is also on legal organizations to ensure that their legal teams practice precaution when working remotely because there will always be malicious actors looking to capitalize on any and all vulnerabilities.

everlaw

Contact us

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

UK
70 Wilson St.
London, EC2A 2DB
0800.068.9249

everlaw.com