Seismic

The Seismic Advantage:
Security, Privacy, and Compliance Without Compromise

Table of Contents

Introduction

Data breaches, regulatory compliance, and maintaining business agility are top concerns for every reputable company.

In today's digital landscape, securing data and ensuring compliance with constantly changing regulations is essential. But it can also be a daunting task, especially for teams that are already stretched thin.

The Seismic Enablement Cloud™ is a robust platform that provides everything your customer-facing teams need in one place. It's backed by our state-of-the-art infrastructure, advanced enterprise security, stringent privacy controls, and a commitment to rigorous data governance and ongoing compliance.

Data

Seismic defines data as the following in this whitepaper:

Personal data: Personal information, or personally identifiable information (PII) as further defined under applicable privacy law(s), is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Customer account data: Information pertaining to customer's relationship with Seismic, including name, contact details, authorized access, billing information, and data used for managing relationships, verifying identities, and ensuring legal compliance.

We believe that in today's fast-paced and ever-connected world, your business shouldn't have to choose between security and agility. With Seismic, you can have both.

This whitepaper provides a comprehensive overview of Seismic's robust security capabilities, availability measures, commitment to privacy and transparency, governance policies, and regulatory compliance. It will show you why Seismic is the trusted choice for customer-facing teams around the world. For more details on the content of this whitepaper, after NDA you can request to view our DPA and our SIG Bundle.

Customer usage data: Information collected by Seismic during service operation, including communication tracking, activity logs, performance optimization data, and data for preventing system misuse.

File metadata: Data related to files, such as modification timestamps, creation date, file size, and file type.

Customer content: All text, multimedia, graphics, audio, video, data, quizzes, practice scenarios, and other information and content provided by customer to Seismic for use within Seismic's services.

Non-Seismic materials: Mobile, cloud-based, and on-premises software applications, connectors and application programming interfaces, data, software development kits, or other materials owned by customer or a third party that interacts with Seismic's subscription services.
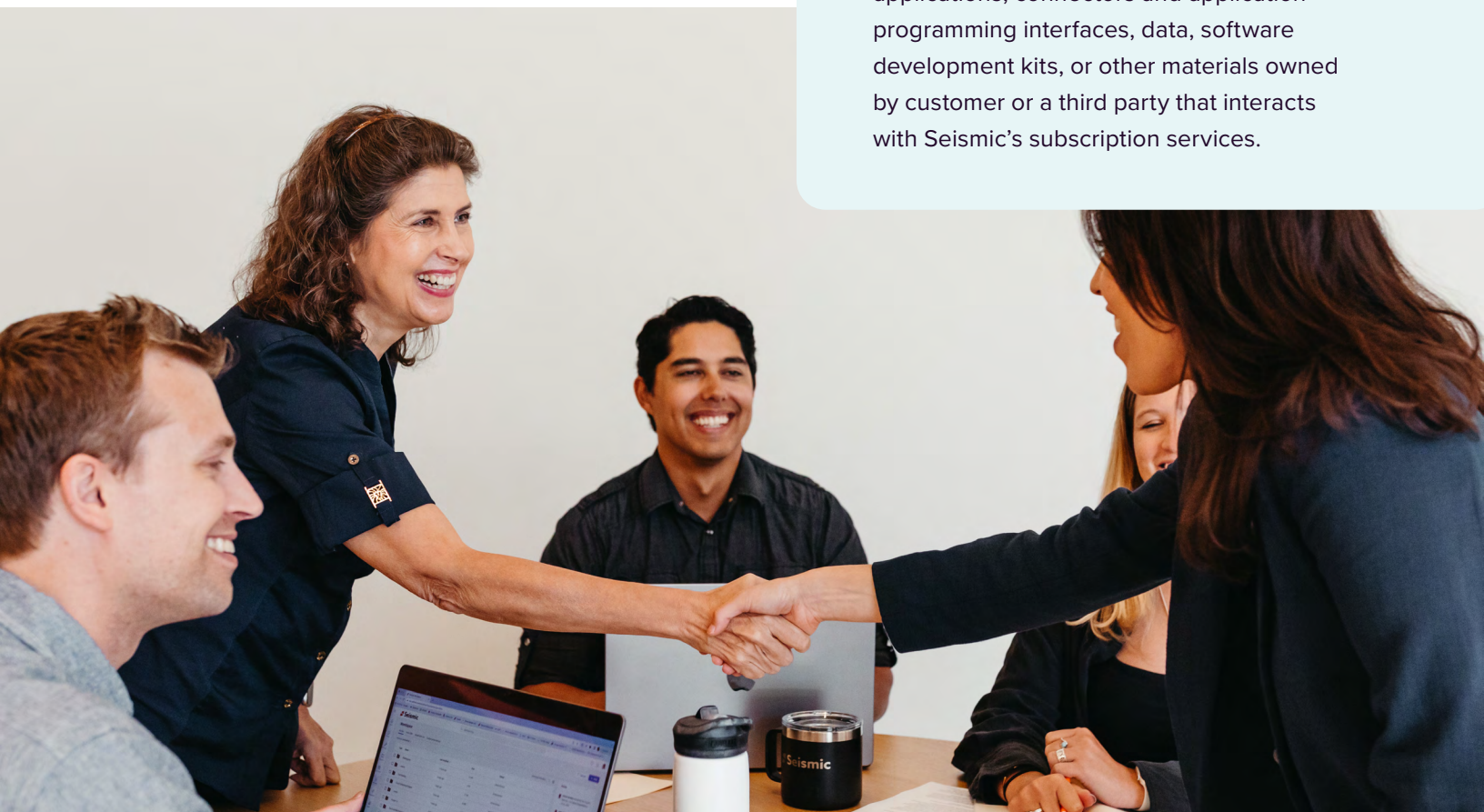
The Seismic Enablement Cloud

Features and benefits

The Seismic Enablement Cloud, as shown in Figure 1, offers a wide range of features and benefits for go-to-market teams:

- **Efficient content creation and management:** Empower marketers to create, curate, and personalize content for diverse audiences and channels with ease.

- **Personalized content generation:** Enable sales users to independently generate personalized content, leveraging Seismic's AI-powered recommendations and insights.

- **Improved go-to-market efficiency:** Streamline workflows, reduce tool fatigue, and onboard new team members quickly.

- **Enhanced buyer engagement:** Connect with buyers more effectively across digital channels and deliver engaging, personalized experiences with tools like LiveSend and Digital Sales Rooms.

- **Operational optimization:** Organize content effectively, automate content production, show impact and ROI, and optimize enablement strategy.

- **Streamlined training and coaching:** Facilitate onboarding and training sellers at scale with interactive courses and practice options.

- **Agility and speed to market:** Launch products, deploy sales plays, enter new markets, and update sales methodology quickly.
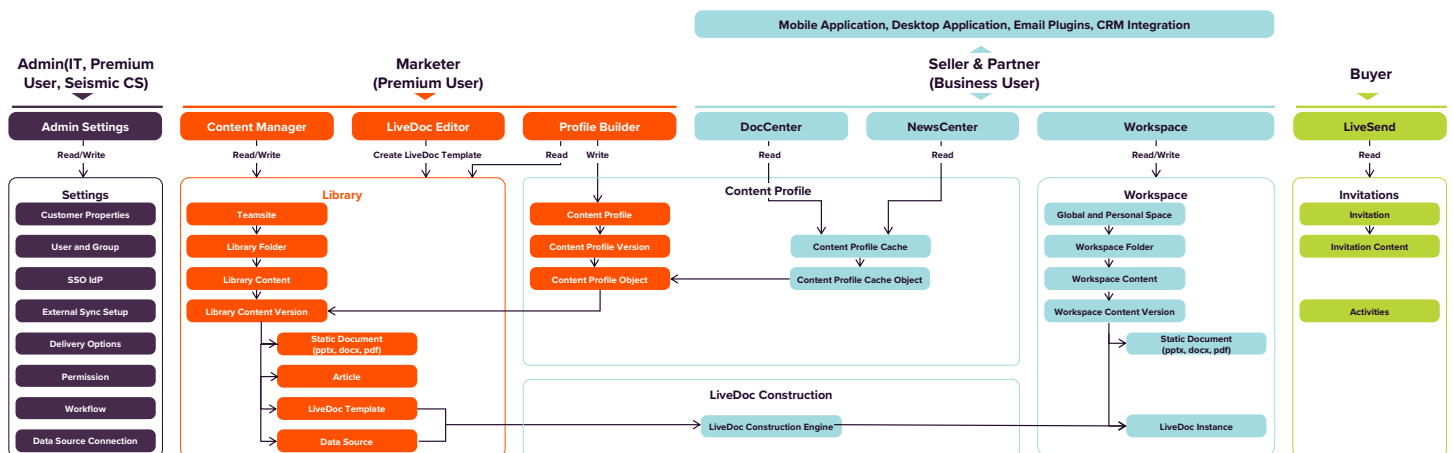

Figure 1: The Seismic Enablement Cloud

Under the hood

As depicted in Figure 2, the Seismic Enablement Cloud is built on a horizontally scalable microservices architecture, which ensures data security through encryption during both transit and storage. Seismic also maintains region-specific uptime data, accessible at status.seismic.com, with a reliability rate consistently exceeding 99.5%.
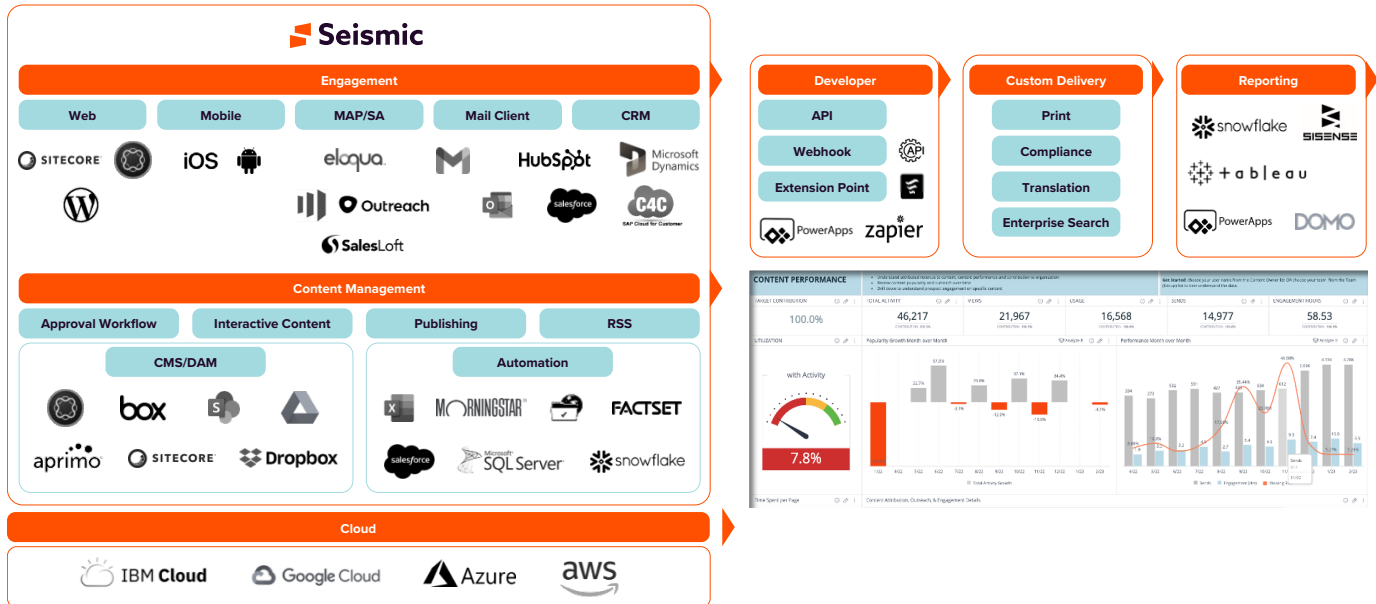

Figure 2. The Seismic Enablement Cloud: Integrated Architecture

Seismic operates using a network of web, application, and database servers hosted on a third-party cloud computing platform, such as Microsoft Azure, Google Cloud, or IBM Cloud. The underlying infrastructure is managed by the cloud provider.

Metadata and file contents are securely stored within a cloud provider's storage system in the cloud provider system, while data is encrypted at rest, meeting stringent security standards.

Deployment and data residency

Seismic's SaaS deployment leverages the Microsoft Azure infrastructure. Seismic provides every customer with both primary and disaster recovery tenants, which are geographically separated to enhance data resilience. Customers have the flexibility to choose their tenant location upon onboarding.

As illustrated in Figure 3, Seismic operates within a global network of data centers across different regions:

- **Microsoft Azure:** West U.S. (California), West U.S. 2 (Washington), East U.S. (Virginia), East U.S. 2 (Virginia), Central U.S. (Iowa), Canada Central (Toronto), Canada East (Quebec City), Western Europe (Netherlands), Germany West Central, Switzerland North, U.K. South, Australia East, Australia Southeast

- **IBM Cloud:** U.S.-East and Japan Tokyo regions

- **Google Cloud:** U.S.-West 1 region

Figure 3: Seismic Deployment Locations and Data Residency

This extensive network of data centers ensures optimal performance, redundancy, and offers customers the ability to store their data within their preferred region.

Availability

Seismic is committed to keeping your business and your data running and available 24/7. We have a comprehensive disaster recovery and business continuity plan in place to ensure the safety, availability, and integrity of our services and data. We proactively take steps to ensure that we can respond quickly and effectively to any unexpected challenges.

Our robust infrastructure includes:

Frequent rolling database and storage backups.

Failover mechanisms strategically positioned in close geographic proximity, independently powered to enhance reliability.

Seismic has established recovery point and recovery time objectives, ensuring minimal data loss in the event of an incident and enabling swift system restoration should an unexpected disruption occur.

BCP/DR and IR tests are conducted annually and are available in the SIG bundle once under NDA.

Security

Seismic keeps customer data secure by assessing risks and continually improving the security, confidentiality, integrity, availability, and privacy of our systems. We regularly review and update security policies, provide security training, perform security testing, monitor compliance, and conduct risk assessments. Seismic's SIG Bundle is a compilation of security, privacy, audit, and architecture documents for each platform.

A multi-layered approach

Seismic's security strategy is founded on three core pillars:

- **Physical:** Maintains physical security protocols to prevent unauthorized access to company offices and systems as well as continuous security training for employees and evaluation of its facilities.

- **Principle of least privilege:** Ensures that users only have access to the data and resources they need to perform their jobs. This helps protect data from unauthorized access and accidental breaches.

- **Confidentiality, Integrity, and Availability:** Implements security and risk management policies, robust logging and monitoring practices, and employs a comprehensive approach to collect and assess data related to potential security threats and vulnerabilities across 18 critical risk domains.

These pillars ensure the highest level of security for your assets and operations within the Seismic ecosystem.

User access controls

User access controls are designed to protect your data and ensure that only authorized users can access your specific tenant. We offer a variety of authentication options to meet the needs of your organization, and we integrate with leading identity management providers to simplify user provisioning and de-provisioning.

- **Single sign-on (SSO) using SAML 2.0:** Enables users to access multiple applications with a single set of credentials, simplifying user provisioning and enhancing security.

- **Authentication options:** Offers three authentication options, as observed in Figure 4, to meet a variety of deployment needs: SSO, open application programming interface (API), and Flatfile.
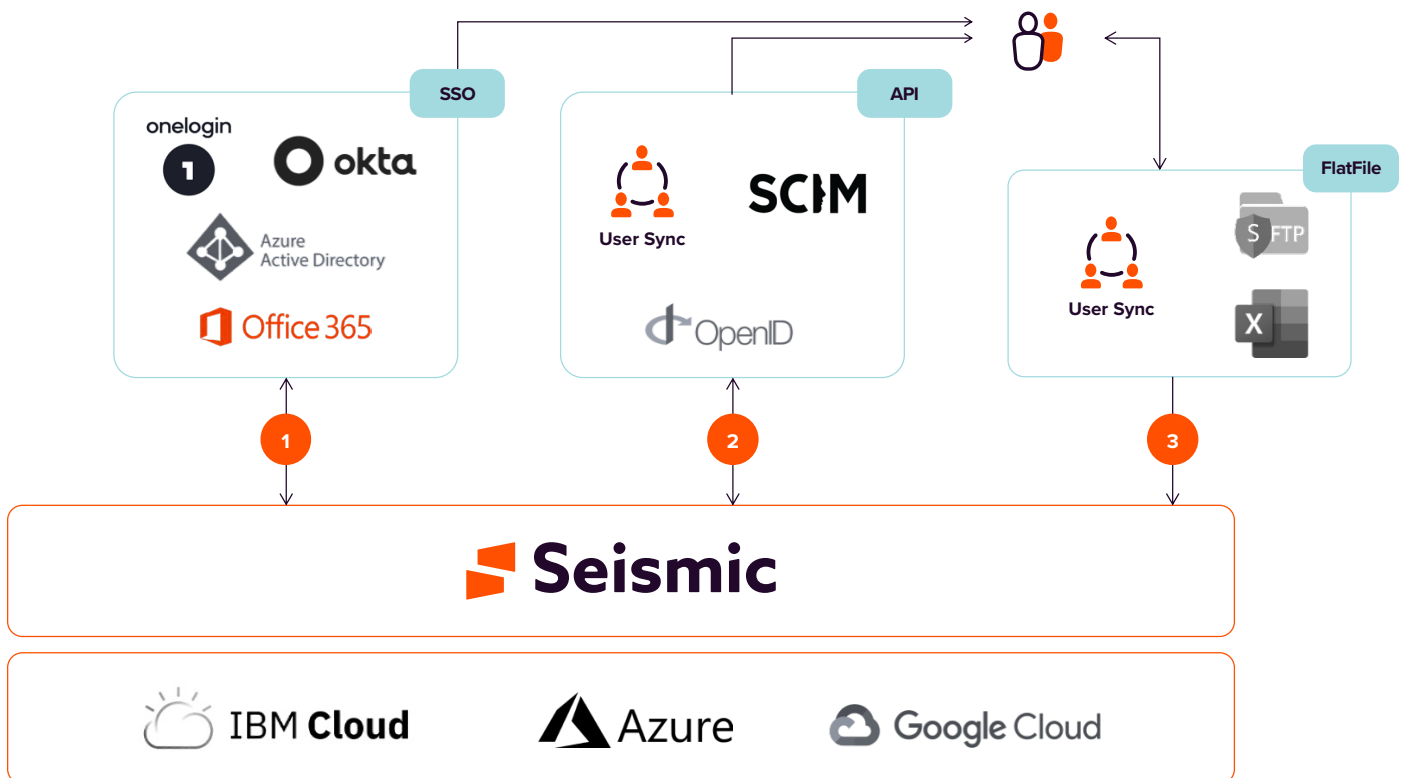
MS Entra and Purview also used to monitor accounts.

Figure 4: Seismic Authentication Options

Data security

To safeguard your data, Seismic employs a comprehensive range of security measures:

- **Data classification:** Policies and procedures are in place to handle, classify, retain, and dispose of data. We work with you to ensure that your data is properly classified and retained.

- **Encryption:** Seismic employs strong encryption mechanisms to safeguard data both in transit and at rest. All customer data is encrypted at rest and in transit using industry-standard encryption algorithms:

  - **At Rest:** AES-256 bit encryption for data at rest along with the SHA-2 hashing algorithm.

  - **In Transit:** From end user applications to Azure using SSL/TLS and between components using SSL (https or encrypted TDS). Data protection between tenants is managed with technical controls (separate database schema and separate tenant-specific encryption keys) as well as isolation/protections in the Azure Fabric and Infrastructure.

- **Key management:** Seismic manages file encryption keys on behalf of users; for some select customers we offer an Advanced Privacy Management solution.

We do not process PCI, HIPPA, or PHI data. We also do not process GLBA within financials or non-public personal information. We process sales enablement data such as marketing data and platform data.

Furthermore, within the Seismic Enablement Cloud, you have full control over your data, including the ability to upload, aggregate, index, and organize it according to your needs. We don't share it with third parties beyond the terms outlined in our contractual agreements.

Application security

Seismic's web, mobile, and API interfaces offer robust security features to protect user data and ensure seamless access:

Authentication and authorization: Users must authenticate with valid credentials and are authorized to access only relevant resources and features.

Data encryption: All data in transit and at rest is encrypted.

Input validation: All user input is validated to prevent malicious attacks.

Secure session management: The web interface uses secure session management practices to prevent session hijacking.

Rate limiting: Seismic APIs implement rate limiting to prevent denial-of-service attacks.

Seismic is committed to protecting user data and ensuring the security of its web, mobile, and API interfaces. We regularly review and update our security practices to stay ahead of emerging threats.

Vulnerability management

Our InfoSec team conducts regular automated and manual security assessments, complemented by diligent patch management and collaboration with external experts to identify and address potential security vulnerabilities and bugs. We use EDR (Endpoint Detection and Responses) as well as XDR (Extended Detection and Response), data collection into our SEIM, and with regular scans to identify potential vulnerabilities. We promptly share findings and recommendations with management, assess them rigorously, and address them as needed.

In addition to regular security assessments, our security team also performs automated and manual application security testing on our web and mobile applications. We engage an independent, third-party testing firm to conduct regular penetration and vulnerability tests on our production environment, including network, web, API, and mobile application penetration testing. We also collaborate with external specialists, industry security teams, and the wider security research community to fortify our platform to go along with an active bug bounty program. Executive summaries of penetration tests are made available in the SIG bundles once under NDA.

Incident response

Seismic has a comprehensive incident management process to handle security incidents, including preparation, identification, containment, remediation, recovery, and root cause analysis. Incidents are tracked and categorized based on severity, and we conduct regular tabletop exercises to test our response plan. Seismic logs to Rapid7 Insight IDR, which is our SIEM and also uses NewRelic for tracking and logging capabilities. Seismic Information Security has rules set to alert on suspicious behavior. Logs are stored for at least one year and if an incident occurs we can provide logs to customers upon written request.

Our incident response teams are trained to swiftly respond to and assess incidents, implement mitigation and containment measures, communicate with internal and external stakeholders, preserve evidence for investigations, document post-incident analyses, and create triage plans. Our incident response policies and processes are regularly reviewed by independent auditors as part of our SOC 2, ISO/IEC 27001, and other security assessments.

Change management

The change management process ensures that changes to our production environment are made in a secure and controlled manner. We follow a structured, ticket-based process with documentation, testing, and approvals to ensure safe and efficient changes. We use separate environments and distinct branches for changes to prevent disruptions to production. Source code access is restricted, and we follow a DevOps model with strict monitoring.
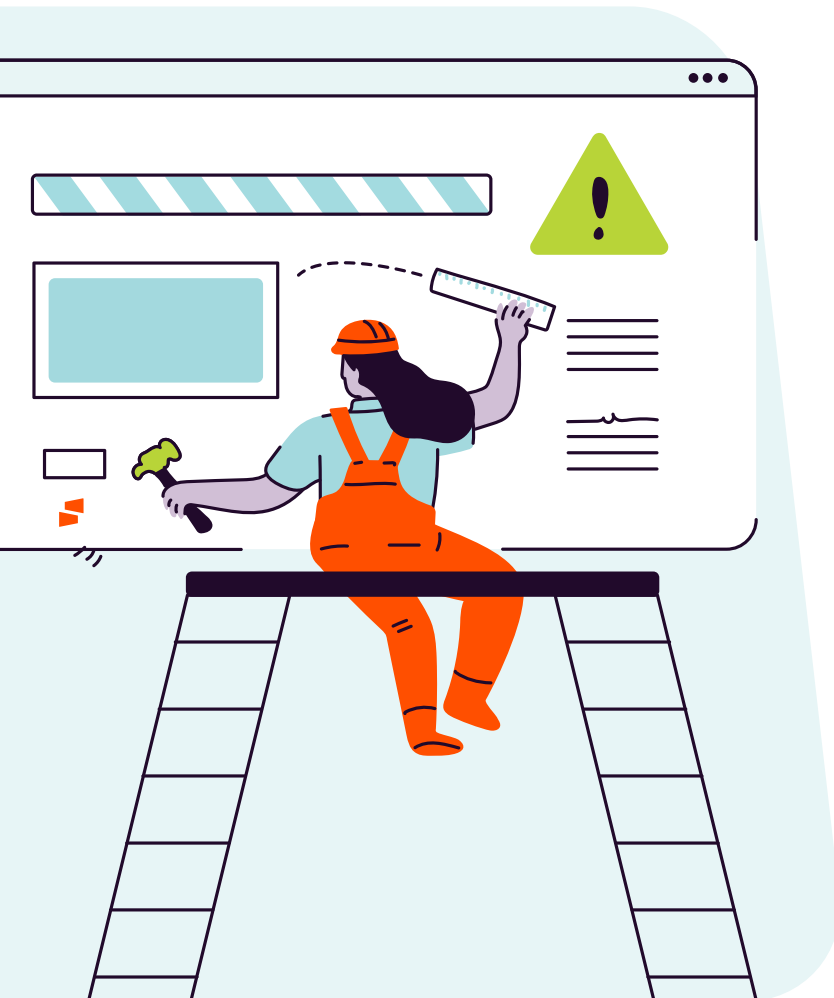
Security embedded in software development

Seismic's software development process is firmly rooted in the software development life cycle (SDLC), a robust framework that guides developers in crafting more secure software. We seamlessly integrate security requirements throughout the SDLC, from planning and design to development and deployment. We prioritize security measures, drawing upon the open web application security project (OWASP) Top Ten risks to ensure that security is an intrinsic and non-negotiable aspect of our software development process. Static code analysis is used to identify and address vulnerabilities. Well-organized patch management keeps our systems up-to-date with the latest security fixes. Our change management practices prioritize system integrity and security, fostering trust in data safety. - We use for application security, SAST (static), DAST(dynamic), SCA (Software composition analyis or Open Source testing). We deploy API scanning tools that run playbooks against APIs.

Securing data in partner collaborations

While connecting with partners and integrating with diverse platforms, Seismic places paramount importance on safeguarding your data. As evident in Figure 5, our integration architecture seamlessly interfaces with content management systems (CMS) and digital asset management (DAM) providers, facilitating efficient content synchronization and dissemination to web hosting applications. We also collaborate with third-party sub-processors to ingest content from various data sources, with a steadfast commitment to robust risk governance and management.
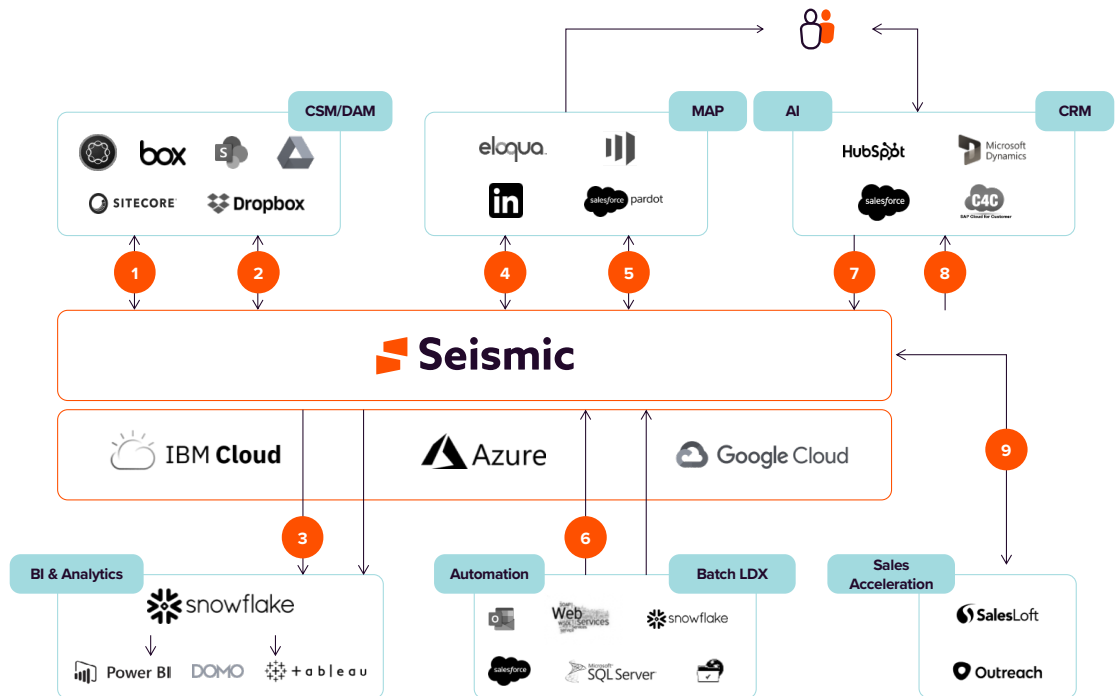

Figure 5. Seismic Integration Partners and Sub-processors

Vendor risk management program

To ensure unwavering adherence to stringent security standards, Seismic conducts annual vendor assessments and establishes legally binding contractual agreements with all sub-processors. They also conduct quarterly risk reviews to go with annual vendor assessments. Seismic's data processing addendum (DPA) provide comprehensive details on sub-processors, services provided, data storage locations, and treatment of PII and non-material data.

Your customer relationship manager will proactively communicate any new sub-processors before implementation. Notifications to subs are sent out prior to changes to allow customer review.

The Seismic Enablement Cloud empowers organizations with versatile integration capabilities, including inbound content sync, delivery approval, privacy management, and user management. While the core of our data-processing activities takes place within Seismic, upholding the highest standards of risk governance and management remains our top priority in collaborating with integration partners.

Privacy

At Seismic, we believe your data privacy is your right, and we are committed to protecting your data and giving you control over it. We abide by the following guidelines to ensure your data privacy:

- **Ownership and control:** You own your personal data, and we use it solely for the agreed-upon services.

- **Data location and access control:** Where your data resides is determined during provisioning where customers can choose their tenant and who can access it.

- **Data removal standards:** You have the assurance that we follow rigorous standards to remove your data when you discontinue our service. Data removal is done in accordance with the NIST SP 800-88 standard.

- **Responsible use of personal info:** We use your personal information only for the services you signed up for. You have the freedom to add, modify, or delete data as needed.

- **Data security:** We adhere to ISO 27001 and 27701, ISO's standards for Information Security and Privacy to keep your data safe.

- **Transparency:** You'll always be informed about changes to our trusted partners and suppliers that process your data and any changes that may impact your data.

- **Regular audits:** We undergo annual audits to maintain the Service Organization Control (SOC2) standard, and ISO 27001, 27701 certifications, ensuring the continued integrity of our data protection standards.

Commitment

Seismic is committed to protecting your privacy and ensuring the security of your data. We have implemented a number of measures to ensure that your data is safe and secure and its access is strictly controlled and authorized, and adhere to the principles of least privilege:

- All debugging and troubleshooting tasks are diligently managed through robust logging tools.

- Access for Seismic project team members is intentionally transient and confined solely to the implementation phase or defined project timelines.

- Seismic support employees can only access customer data with customer authorization and only for the purpose of triaging support issues.

- Our dedicated InfoSec team maintains a vigilant watch, conducting regular audits of employee access.

Confidentiality

Seismic protects your privacy by keeping your data confidential. We employ comprehensive measures that ensure confidentiality:

- Prompt deletion of customer data upon termination or written request, with certification of disposal.

- Strong encryption for data at rest and in transit, including backup data.

- Confidentiality commitments outlined in customer contracts.

- Background checks as part of employee vetting for hire

- Annual security training required for all Seismic employees

- Confidentiality agreements required for all employees during their onboarding process.

- Documented policies for data retention and disposal.

Data isolation measures

Seismic's Infrastructure is designed to maintain logical isolation of each customer's data from that of others, even when residing on the same physical server. Access to customer data for troubleshooting purposes is precisely aligned with specific job functions and roles, adhering to the principles of "least privilege" and "need-to-know." Access privileges are intricately tailored to defined responsibilities.

Compliance

Seismic is committed to complying with all applicable laws and regulations, including global standards for data protection and security. This commitment extends to ensuring financial services organizations can seamlessly connect their systems to Seismic in order to adhere to various industry regulations.

Global standards

Seismic is GDPR-compliant and CCPA-compliant, and we adhere to the web content accessibility guidelines (WCAG) 2.1 level AA for inclusivity. We have implemented a data protection impact assessment (DPIA) process to validate our processing of personal data. We have a Modern Slavery policy statement and our employee handbook also contains key policies governing labor practices and ethical working conditions.

In addition, Seismic conforms to the following global standards:

- **ISO/IEC 27001 certified**

- **ISO/IEC 27701 certified**

- **SOC 2** Type II assessed in all 5 categories (security, availability, integrity, confidentiality, and privacy)

Seismic can share internal documentation and SOC2 Type II report (which is completed annually) for evidence if requested, please ask for the SIG Bundle after NDA.

Financial services regulatory compliance

Seismic helps financial services institutions address compliance and regulatory requirements in two ways:

Platform integrations to support review and approval workflows, archiving, supervision and recordkeeping requirements.

Product features designed to optimize workflows and ensure only approved content is shared by sales teams with existing and prospective customers.

This partnership approach ensures that customers are able to use Seismic Enablement Cloud while also adhering to specific regulations as follows:

Financial Industry Regulatory Authority (FINRA)

- **Books & Records:** Exchange Act Rule 17a-4

- **Rule 2210(b)(4):** Communications with the Public

- **Rule 2211:** Communications with the Public About Variable Life Insurance and Variable Annuities

U.S. Securities and Exchange Commission (SEC)

- SEC Books and Records (SEC17a-3, 17a-4, 17a-1)

- SEC Marketing Rule

- SEC Best Interest Rule

Canadian Investment Regulatory Organization (CIRO)

- Rule 3800: Dealer Member Records & Client Communications

Financial Conduct Authority (FCA) in the U.K.

- SYSC 9.1 General rules on record-keeping

Australian Securities and Investments Commission (ASIC)

- Books & Records

European Securities and Markets Authority (ESMA)

- Record-keeping requirements under the Benchmarks Regulation (ESMA81-393-288)

Please note that this list is not exhaustive; it is representative of how Seismic can help support compliance and regulatory requirements specific to the financial services industry. Seismic has partnered with more than 400 customers around the globe to help support their compliance and regulatory requirements through integrations and product capabilities.

Platform integrations

As a leading SaaS provider serving all aspects of the financial services industry, Seismic partners closely with their financial services customers to seamlessly integrate with their archiving, recordkeeping and supervision tools in order to satisfy compliance requirements.

The Seismic platform is not natively WORM compliant, doesn't store data for required timetables (generally 7 years) and as such, is able to integrate with customers' archiving, recordkeeping and compliance supervision tools in order to satisfy regulatory requirements. Data is securely provided in a daily export in adherence to compliance standards.
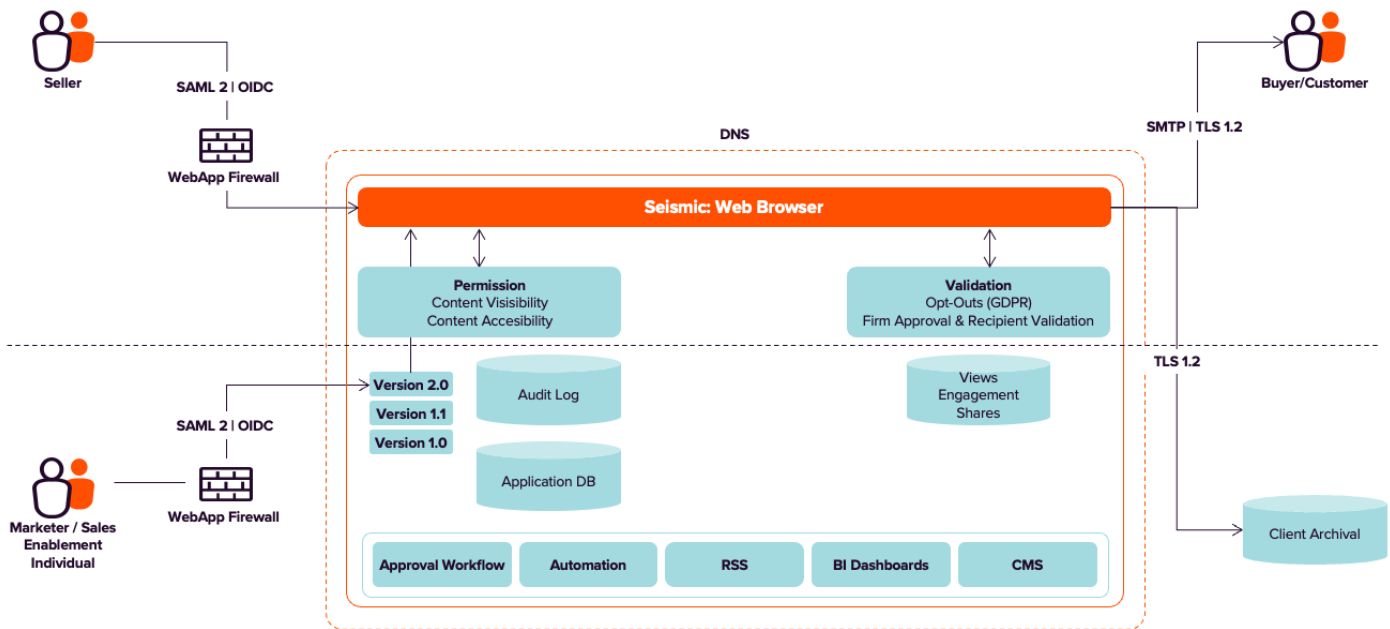

Figure 6: Seismic Data Compliance Architecture for the Financial Services Industry

As shown in Figure 6, Seismic connects to firm archiving, recordkeeping and supervision tools in support of regulatory compliance.

This approach ensures that firms can take a consistent and streamlined approach for communications that take place on Seismic and other technologies that are subject to regulatory audit.

AI

Whether internally or externally hosted, our latest generative AI models meet Seismic's best-in-class data privacy and security standards. We remain committed to data protection, ensuring the AI models we leverage reside on your cloud platform of choice.

When our generative AI technology utilizes third-party GPT models, your customer data will not be logged or used for model training by the third party. Our product design is centered on integrating generative AI into your workflow while prioritizing transparency and choice of using AI. Each of our generative AI features is indicated in the interface by our AI icon, so users are informed when they are engaging with generative AI technology.

Seismic's generative AI features are turned off by default and can be enabled as needed. Each provides the ability for user feedback to improve performance. We do not train models using customer data, for Seismic-managed models we train or fine tune data using open source, third party models. Our AI recommendations and models are also reviewed for bias. We highly value the trust you have placed in Seismic, and we've diligently worked to design our products in accordance with the core tenets of global privacy laws.
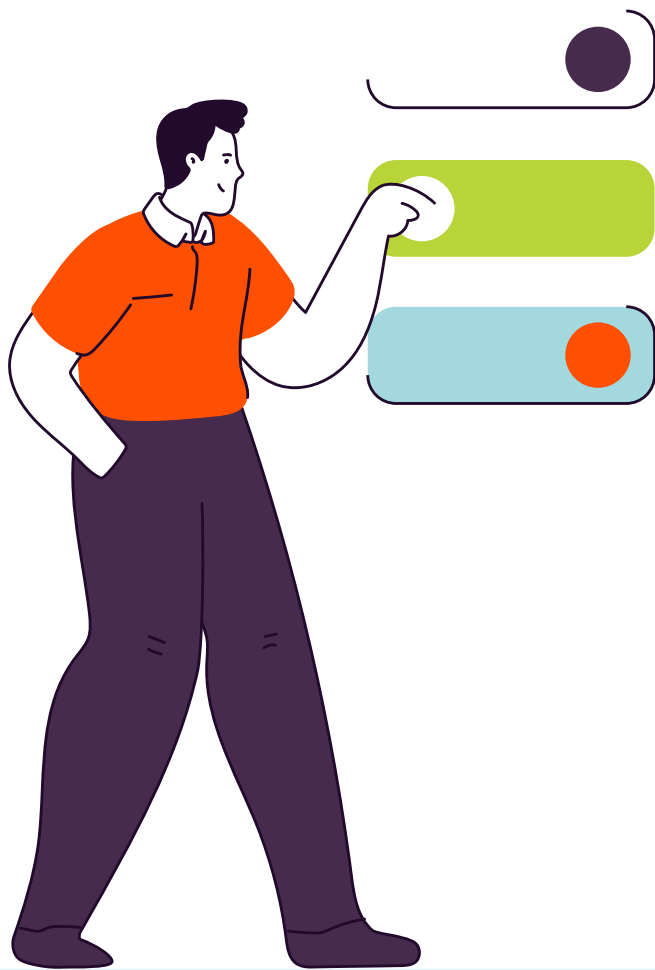
For more information on our AI please review **Seismic Aura & AI Standard Privacy & Security Frequently Asked Questions.**

Social media

Specific to Seismic's LiveSocial product, Seismic partners with leading compliance providers to support profile monitoring, profile management, compliance indexing and group-based compliance rules.

Product features

In addition to the security of the Seismic Enablement Cloud platform, the integrations to archiving, recordkeeping and supervision platforms and partnerships with compliance solution providers, Seismic also helps firms comply with legal, compliance and various industry regulatory requirements through functionality designed to help firms streamline their processes and ensure that only approved content is distributed outside their organization.

Content Governance

Seismic plays an important role in helping firms establish processes and controls to help marketers efficiently maintain up-to-date content and help sellers source accurate and compliant content.

These features include:

Version Controls

With Version Controls, customer-facing teams are presented with the most up-to-date, approved content as assets are created, updated and improved over time.

- **Centralize content control:** Automate processes to create, update, and improve content while maintaining a central source of truth.

- **Manage customization:** Allow content to be personalized while protecting source versions.

- **Handle versions:** Maintain control over source content.

Best For:

- Customizing pitch books without impacting source content

- Giving sales and other client-facing teams with the flexibility to personalize assets that do not violate compliance and regulatory requirements

- Maintaining ongoing content library hygiene to ensure that only approved content is shared with existing and prospective customers

Approval Dashboard & Workflows

- With Approval Dashboard & Workflows, teams have the tools needed to address timely content review and approval processes that adhere to compliance and regulatory requirements.

- **Establish processes:** Streamline review, edit, and approval cycles with customizable workflows to keep content updated and impactful.

- **Ensure compliance:** Review and approve content that meets regulatory or marketing compliance, including content customized by sales teams.

Best For:

- Verifying fact sheets before distributing to sales teams, clients, and publishing to websites

- Ensuring that marketing materials are properly reviewed by key stakeholders, legal, compliance, and other approvers

- Ongoing marketing asset reviews and approvals

Content Controls & Expirations

With Content Controls & Expirations, firms can establish automated processes that trigger content reviews and updates, asset expiration, and archiving of outdated content

- **Manage content access:** Ensure the right teams can find and use the right content.

- **Trigger content reviews:** Set automated triggers so marketers and others can review, edit, and update, or unpublish content.

- **Automate archiving:** Set specific dates for content assets to be archived in the system or get automated retire recommendations based on utilization.

Best for:

- Unpublishing time-dependent content

- Periodically reviewing sensitive assets like product brochures, sales ideas, marketing commentaries, and pricing documents

Metadata at Scale

Saves time and avoid costly errors by automating content publishing and updates.

- Automate which teams see what content without a heavy manual lift.

- Use conditional and dependency logic to create guardrails around tagging content to support publishing at scale.

Best For:

- Streamlining bulk updates

- Ensuring all content is tagged and tagged correctly

- Ensuring updates are made across multiple versions of the same asset
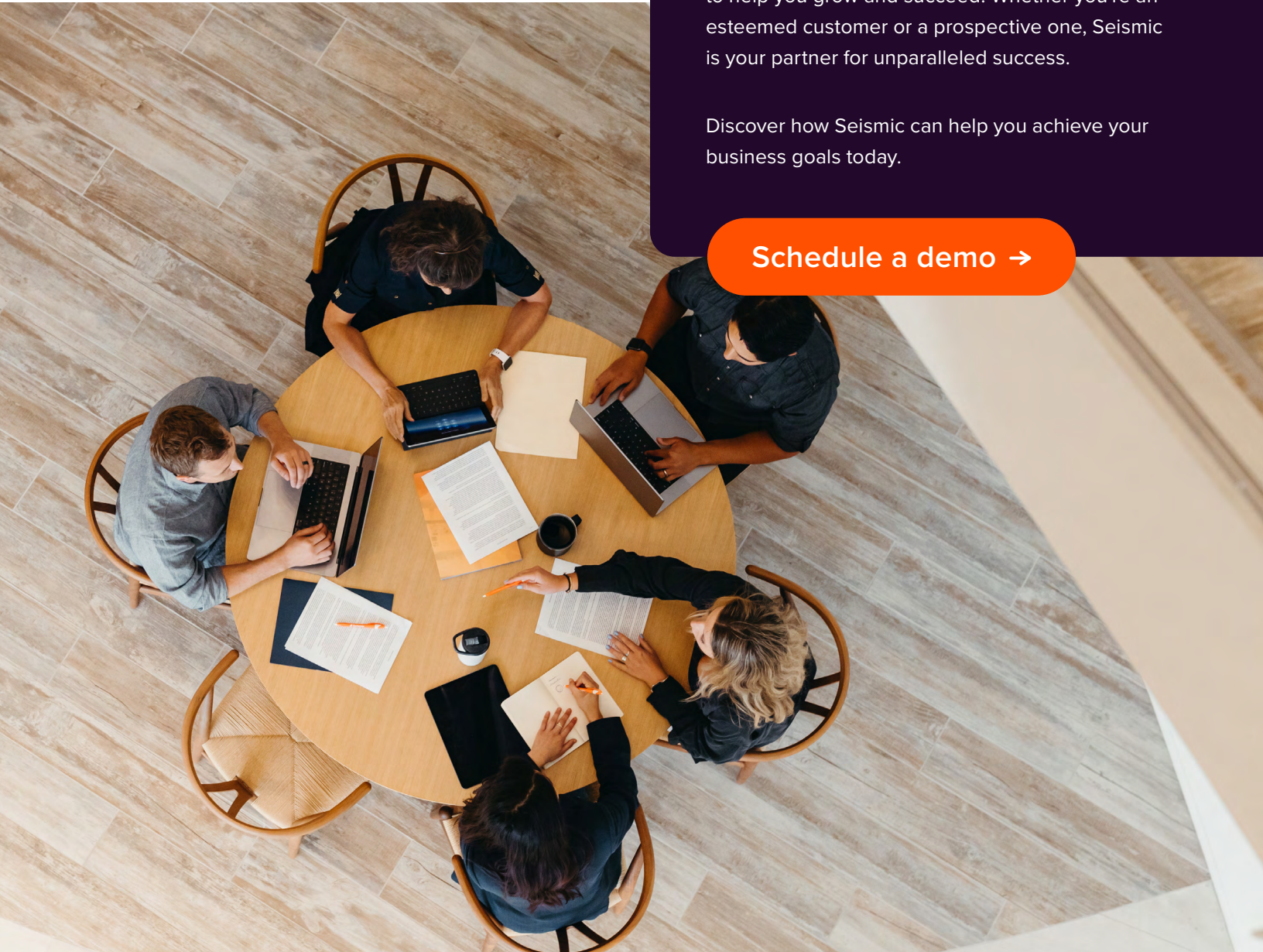
Seismic:
Your trusted partner in enablement

Trust is the foundation of our partnerships with thousands of organizations across the globe. At Seismic, we're committed to protecting your data and privacy, upholding industry benchmarks, and helping you achieve unparalleled success.

When you choose Seismic, you gain access to a world-class platform and a dedicated team poised to help you grow and succeed. Whether you're an esteemed customer or a prospective one, Seismic is your partner for unparalleled success.

Discover how Seismic can help you achieve your business goals today.

Schedule a demo →

About Seismic

Seismic is the global leader in enablement, helping organizations engage customers, enable teams, and ignite revenue growth. The Seismic Enablement Cloud™ is the most powerful, unified enablement platform that equips customer-facing teams with the right skills, content, tools, and insights to grow and win. From the world's largest enterprises to startups and small businesses, more than 2,000 organizations around the globe trust Seismic for their enablement needs. Seismic is headquartered in San Diego with offices across North America, Europe, and Australia.

To learn more, visit **Seismic.com** and follow us on **LinkedIn**, **Twitter** and **Instagram**.

Visit our Website →

This publication/these materials are provided for informational purposes only and [does not/do not] constitute legal advice or other professional advice or services. Nothing herein is intended to certify or otherwise warrant or guarantee that Seismic's products and tools will comply with, or satisfy, regulatory requirements. You should review applicable legal, privacy and security requirements and make decisions based on your own review.