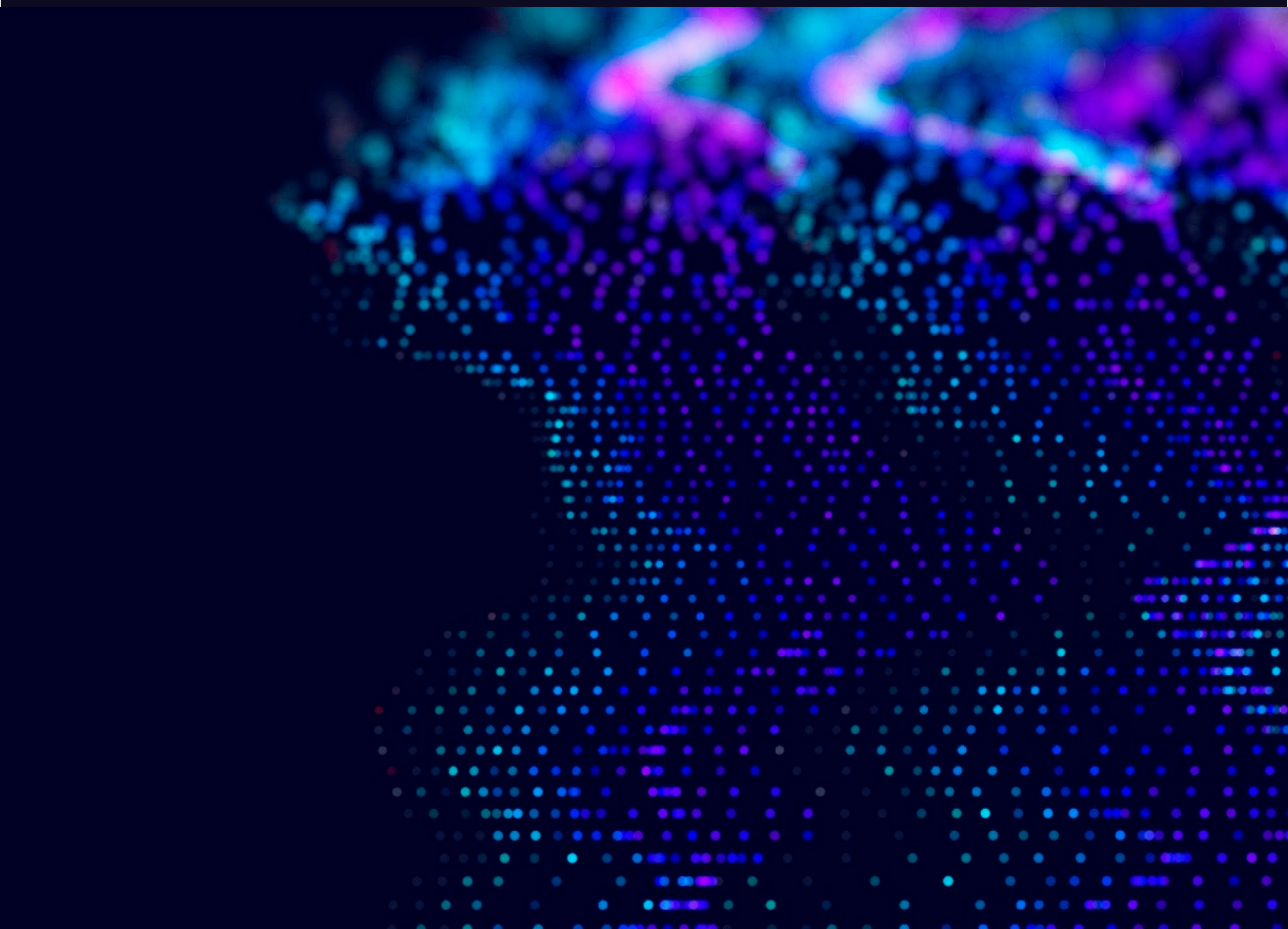
HIGHSIDE

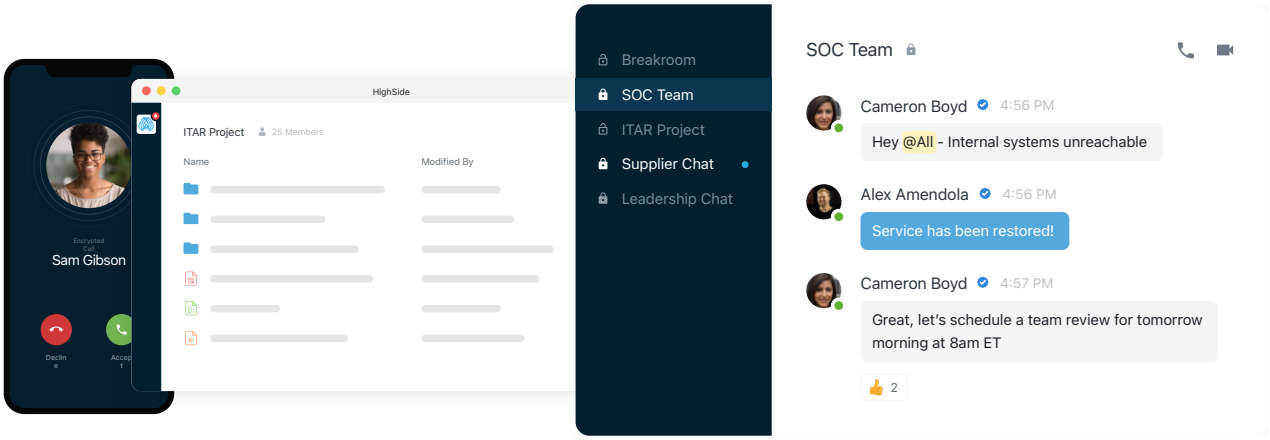
HighSide **One:** One Platform, Countless **Secure** Capabilities

Datasheet: Platform Overview



HighSide One is the leading platform for secure, compliant, and out-of-band collaboration.

Powered by a decentralized E2E encryption protocol, HighSide One delivers productivity capabilities such as secure & out-of-band messaging, controlled file-sharing, and sensitive data management. In use by government agencies and enterprise organizations around the world, HighSide One is changing the way the digital business works. From enabling teams to share and manage their sensitive business data to delivering a secure, highly available, and segmented system for mission, project, and cyber operations teams to ensure persistent communications, HighSide One delivers. With a full RBAC access control system, Active Directory connection for enterprise user management, and an integrated e-discovery and compliance suite, HighSide One is truly revolutionizing secure collaboration.



Encryption & Security

While privacy is the central demand of individuals, data security, control, and compliance are key challenges facing the enterprise.

Building on the work started by privacy advocates and decentralized currency visionaries, HighSide One's collaboration capabilities are powered by a decentralized end-to-end encryption protocol. The HighSide protocol introduces a truly private root of trust, generated and compartmentalized in a NIAP validated application - available on desktop and mobile devices. By decentralizing the means to encrypt and decrypt data, whether a chat, emoji, voice call, or file-share, HighSide's protocol eliminates most of the security concerns plaguing traditional cloud applications and makes it truly zero trust.

In order to deliver both a system that offers zero trust data security and centralized control the HighSide protocol introduced a multi-key authentication system. Keeping data secure is the in- app generated elliptic curve public / private key pair, and ensuring segmented but centralized administrative functions to govern access, device authorizations, and deliver

compliance oversight is a team & server key. Each user's session is fully E2E encrypted, with the SecP256K1 elliptic curve algorithm, optionally available with quantum encryption algorithms. Each message and file-share is encrypted again with AES256 and signed by the server key. In order for a user to access a file or communication, each of these keys must be present and active, thus ensuring the data is obfuscated from any central authority, while giving authority to the centralized admins on who, when, and what devices are allowed to access the environment. This server key system enables HighSide to offer advanced access controls such as geo-location based, time based and device centric access permissions.

HighSide's encryption meets and exceeds FIPS 140-2 and the HighSide One application, across all desktop and mobile operating systems, is continuously validated to the NIAP security standards. HighSide One is authorized for CUI and FOUO information in its native cloud services configuration, and CLASSIFIED information in an on-prem deployment or special controls environment.

Productivity Modules

Secure Messaging & Collaboration

HighSide One was built to enable team collaboration - and communication is key to any team whether they are working on a project with external partners, communicating sensitive information with a customer, or collaborating internally with a cross-functional team. In order for teams to fully trust their communications they must know beyond a doubt that there is no "backdoor". They must also have assurance that if a data breach were to occur, or a network outage were to affect their organization, that digital communications would still be secure and accessible. This is HighSide One.

Don't leave disaster communications to chance...

Secure communication is critical, but better yet, secure, segmented and out-of-band communication ensures security and continuity of access in crisis or disaster situations.

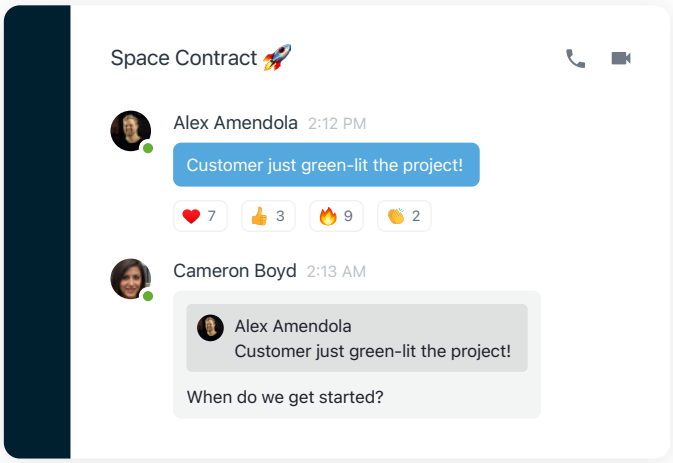
Beyond Zero Trust

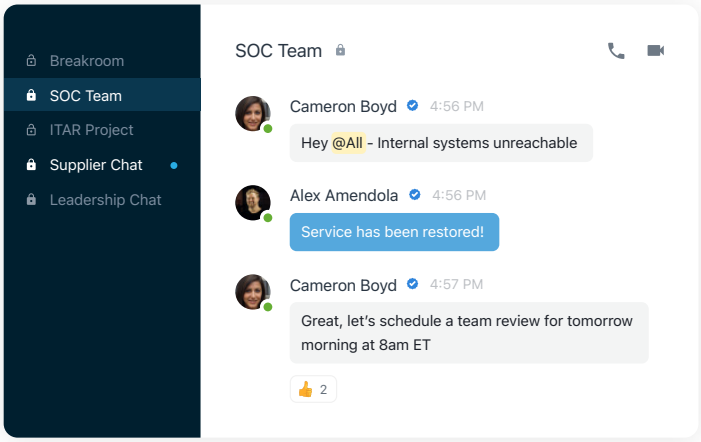
Powered by the HighSide decentralized encryption protocol, HighSide One delivers the most secure, controlled, and accessible collaboration platform on the market. With a true zero trust authentication & data access model, HighSide ensures sensitive communications are always protected.
While HighSide One embraces the authentication principles of zero trust, it goes far beyond in order to deliver an application that operates independently from

corporate infrastructure, while empowering admins to manage and administer access, devices, and data rights. Beyond zero trust makes HighSide One the solution of choice for organizations looking to ensure their team has a collaboration system that won't be affected by a network or system failure - whether it's a cyber attack, network outage or any other issue.

Messaging & Channels

HighSide One may be the most secure collaboration platform on the market, but it's also one of the most user friendly and functional apps available. Users of HighSide One will find a very familiar experience, letting them chat with their colleagues, create channels to collaborate around projects or initiatives, and even use the app to call other users or run encrypted group voice, video and screenshare meetings. HighSide's mobile app should also be familiar to users, with an experience just like the apps they use to chat with friends, HighSide ensures connectivity and communication are always at the ready. If allowed by the team admin, users can enroll multiple devices and stay connected to their projects, chats, and files from all their devices.





Most teams organize their collaboration with HighSide channels. Channels let users engage in project based collaboration, team based discussions or cross-functional working sessions. Share files, chat with partners, or engage with customers - channels give you a shared space to work collaboratively.

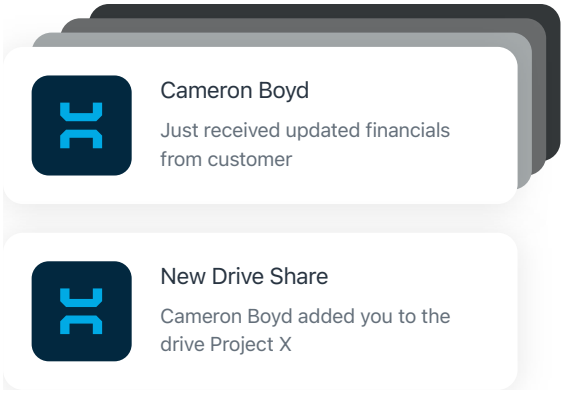
Public Channels - These conversations can be accessed by any member of the team (provided their RBAC controls allow for channel membership) and are designed to foster open dialogue across your teams.

Private Channels - Channels that are private can only be accessed by users who have been invited. Any historical channel content will not be visible to new participants for security & compliance concerns.

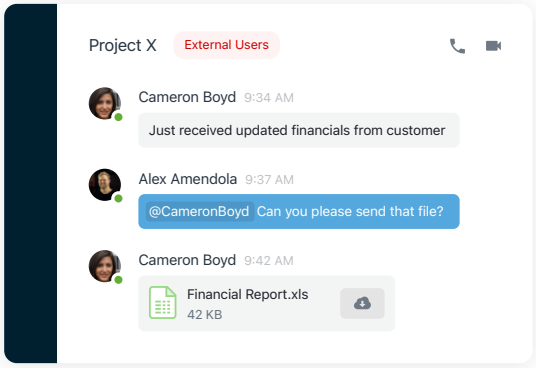
Guest Channels - Invite guest users to a channel and instantly start collaborating with users outside of your organization. All file shares and communications are secure, compliant, and most importantly controlled.

Usability & Notifications

Security and compliance are top priority, but if an application doesn't deliver productivity and user functionality there is little point. HighSide One delivers all the features users are accustomed to in other mainstream chat & collaboration platforms, such as emojis, message reactions, file attachments, in-line message replies, gifs, video & image previews, and more.



Most applications force users to suffer all or nothing when it comes to staying connected. HighSide lets users customize their notifications preferences based on device type, conversation, channel, and even message classification. Rather than forgo mobile notifications to keep your sanity, HighSide One users choose what content they need to know about immediately, and on what devices.



Guest communications

HighSide One enables managers & team leaders to extend communications to external (guest) users outside of your domain. When collaborating on a project or coordinating a cyber response, the ability to add users beyond your domain to HighSide messaging and collaboration platforms is crucial. Rather than relying on insecure comms channels like email or consumer messaging apps, HighSide One ensures all communications remain secure, compliant and within your control.

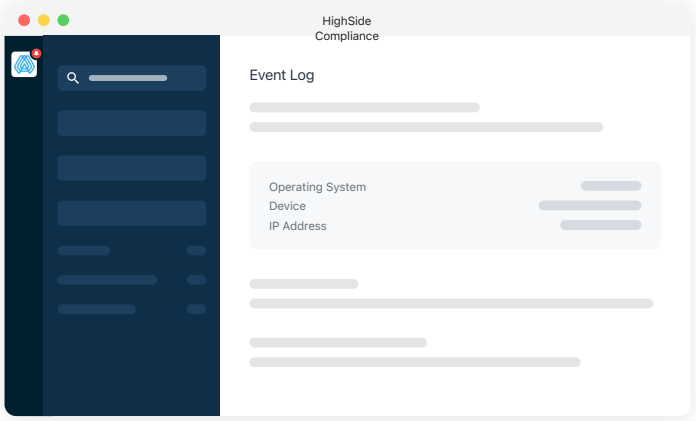
Voice & Video

Nothing replaces talking to your team via voice or video, especially when it's encrypted and built right into the HighSide One app. Let your teams chat, share screens, and collaborate in real-time through a secure application. Ensure that your project data is safe, your ITAR or HIPAA data is protected, or your security operations & incident response communications are secure, all while enabling your users to get their jobs done on mobile or desktop devices.

Admin, Compliance, and Control

HighSide One's administrative capabilities make it easy for admins to translate policies into technology enforced controls. With a full role based access control system, segmented channel & data management capabilities, advanced geo-location access controls and device-centric authentication, HighSide takes process and policies from paper to proveable. HighSide's integrated compliance suite let's admins take things a step further, such as proving compliance with CMMC policies, meeting FINRA e-discovery and message archiving requirements, or internal legal & investigation management. HighSide truly delivers a modern collaboration platform for the security & compliance focused organization.

requirements, or internal legal & investigation management. HighSide truly delivers a modern collaboration platform for the security & compliance focused organization.

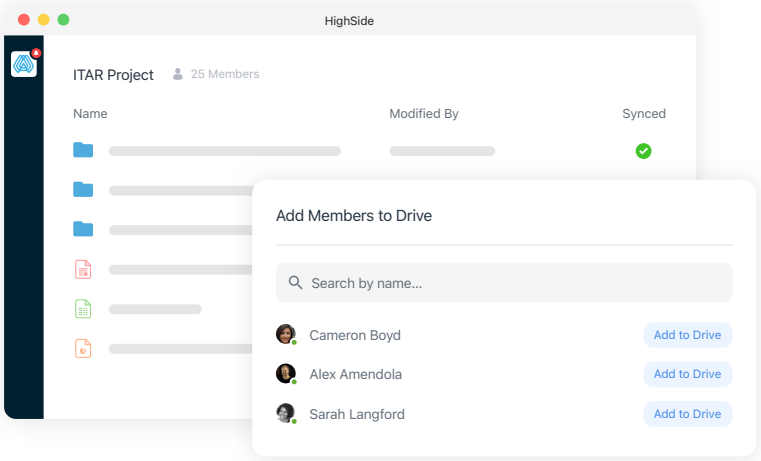


Additional Features

- Individual, group and external-user messaging across desktop & mobile devices
- Custom notifications set per channel or conversation
- Time and location based user access controls ensures controlled & compliant access
- Duel user management via Active-Directory or HighSide's encrypted identity system
- Public, private and guest channels let teams organize conversations
- External user restrictions ensure productivity without risking data or communications integrity
- 1,000s of supported integrations make the transition between digital applications seamless, and opens a world of possibilities for how to use HighSide One
- Passwordless architecture lets users get to work quickly, an minimizes support overhead.
- Device authorizations let admins configure how users add devices to their account; set-up approval queues, set acceptable device policies and more.
- File-sharing in chats, channels, and via the integrated SecureDrive capabilities ensure your team never uses email for data sharing again.
- Customizable classification system let's teams classify channels, files, and messages to ensure users know how and where they can use data - and to aid compliance.

Secure Data Management & File-Sharing

Today's digital business relies on the availability of data - this demand for data accessibility has precipitated the massive rise in data breaches, security incidents, and compliance violations.

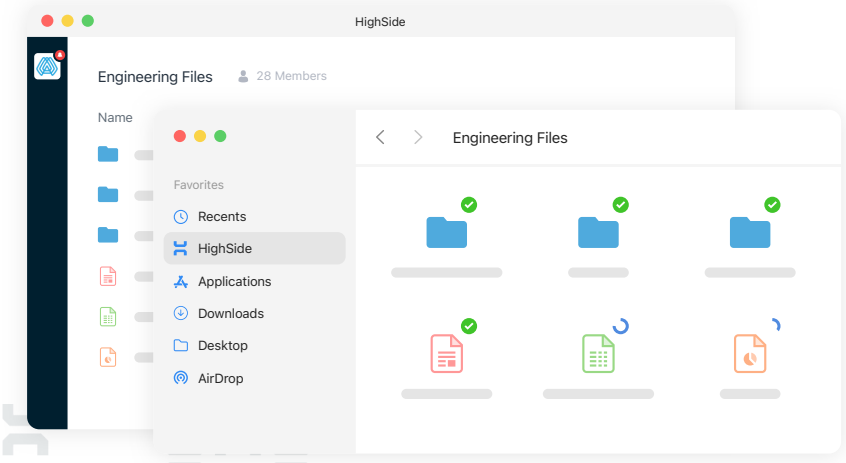


It's not enough to simply secure the way you share your data, but enterprise and government organizations must secure, and make even sensitive files available to authorized users. Combining a focus on the digital business & productivity with the demands of data managers such as file visibility & classifications, access controls, and compliance logging is where HighSide One's SecureDrive comes into play.

SecureDrive

Delivering a secure enterprise grade file share & management system, with enhanced user features such as version management, file-level permissions and access rights, and data management capabilities such as file classification, time & location access restrictions, segmented data manager views, and a full compliance suite. HighSide One's SecureDrive is not just an evolution from traditional DFS and NFS systems, but a revolution marrying the best of the cloud collaboration world, with the security and control requirements of the enterprise.

HighSide One makes the complex task of managing data at the enterprise level a straightforward affair. Ensuring data is accessible by only the right users, that sensitive data doesn't "walk out" of the enterprise, and that data stores don't fall victim to ransomware or cyber attack is at the core of HighSide One's default configurations. Add into those capabilities a complete compliance suite, proving compliance with even draconian regulations (like ITAR) and you have a revolutionary solution.

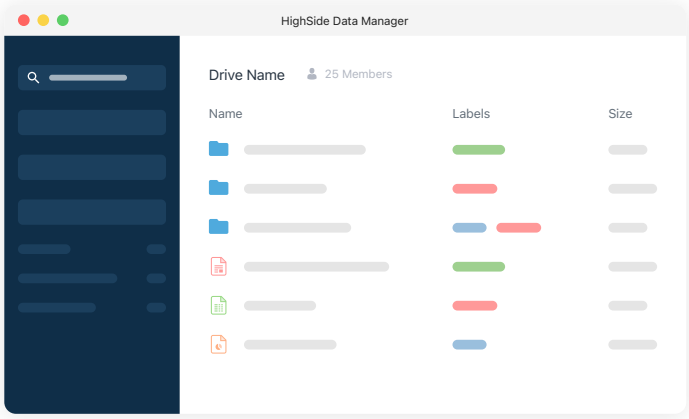


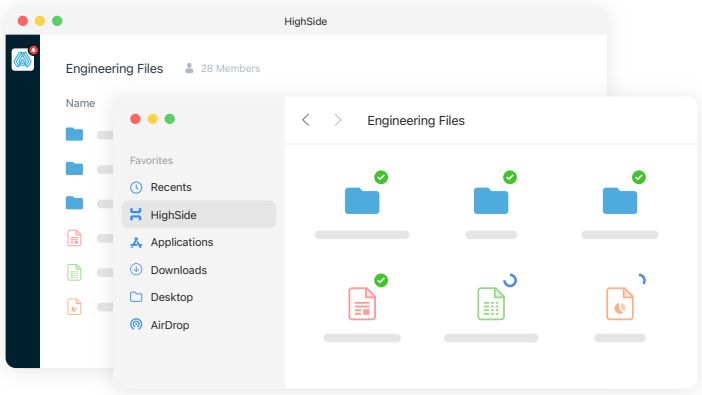
Secure File Sharing

SecureDrive lets data managers or authorized users create e2e encrypted “drives”, where they can create complete directory structures complete with access permissions. These drives are made available to users based on predefined user groups or shared with specific users individually. When a drive is made available to a user, they can access the contents in the secure HighSide One application, or if authorized, can sync the drives to their workstation delivering a familiar experience to that of a networked drive system. Data managers and data owners have the ability to apply specific permissions to files and folders, ensuring that if documents are meant to be viewed but not edited, this is strictly enforced. Additionally, if data should never leave the HighSide One application – making contents only viewable via the in-app system – data managers and owners can simply change file permissions to enforce these controls.

Data Management & Access Control

HighSide’s multi-key decentralized E2E encryption protocol allows data managers to be granted the ability to view file metadata (such as file name, size, location, user access, and data classification) without exposing the contents of the files. This functionality is incredibly valuable for organizations that work with sensitive data, compliance controlled materials, or outsource data management & administrative tasks to remote offices. When data access must be restricted to specific physical locations (due to compliance restrictions or internal policies), HighSide makes this easy with RF signal location triangulation access controls. Admins can set geographical boundaries for data access, whether that’s an entire country or a specific radius around a corporate office - even an authorized users home office. This geo-fence is used by the system as a required validation / authentication gate for users to access the HighSide One system. If a user is not within the authorized location, the data is inaccessible - and the compliance team can prove these restrictions to auditors internal and external.





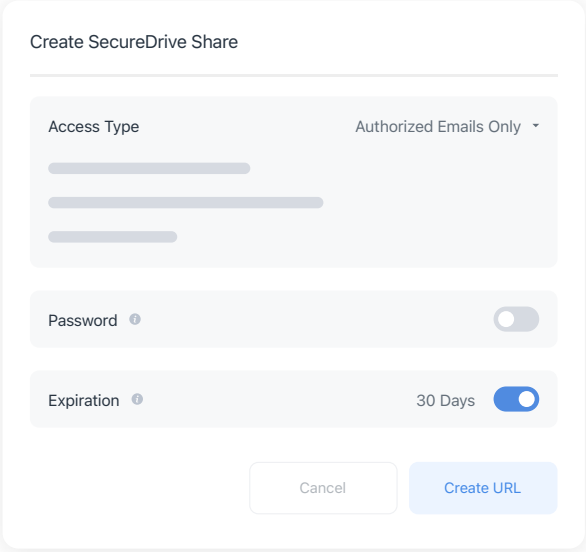
Version Control, Sync, and Data Usability

HighSide One solves many of the drawbacks DFS / NFS systems present to the users, such as lack of version history, and the

inability to lock documents for single user edits, thus eliminating data conflict. HighSide One's multi-user share & sync system is even more critical in organizations that work with large engineering and CAD files as they require local software for editing and manipulation and can lead to hours of work time thrown away without proper version and edit management. SecureDrive delivers a full version history system, making up to 1,000 unique document versions available. Additionally, file-lock allows for users to edit data locally without fear of another user corrupting their changes. When a user saves their updates and releases the lock the HighSide One application automatically propagates the changes to every user shared on the file. If authorized, real-time file sync ensures users have the most up to date data on their machines at all times - no more waiting to download a multi-gigabyte file from a central storage system, productivity happens instantly.

Controlled File-Sharing

When the job requires data to be shared with external users, HighSide One's SecureDrive Share capability let's authorized users create E2E encrypted share links that can be shared via email or other communication channels. These share links let users share drives, folders, or individual files with customers, suppliers, or partners while maintaining the integrity of data. Ensure the shared files are secure with E2E encryption and lock the access to authorized email addresses, or apply a password and expiration. HighSide One records all external file shares and makes the data available to data managers and compliance users - as well as providing access logs & download records to the users who shared the files for an immutable audit trail of receipt and review.

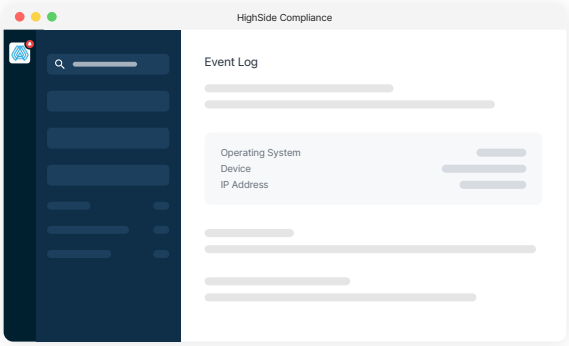


Additional Features

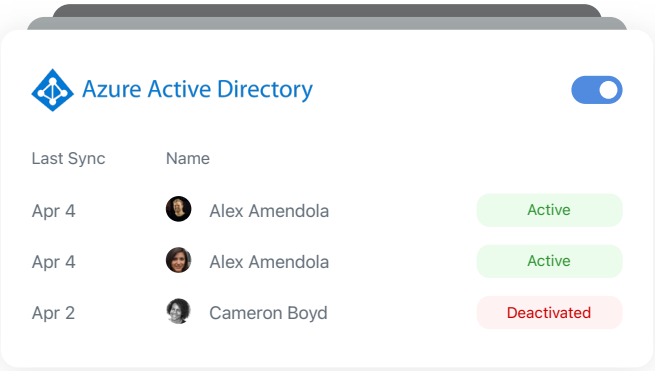
- E2E encrypted file storage, sharing, editing, and management environment
- Segmented data management system uses HighSide multi-key encryption system to separate data access & admin
- Geo-location access controls prevent data access from unauthorized locations
- Included compliance suite enables validation of ITAR, HIPAA, CMMC, e-Discovery and other requirements
- Safeguard up to 1,000 version and quickly restore a prior version eliminating ransomware risk from local data systems
- File & folder permissions offer control over how users interact with data, limiting files to view-only or read-only
- Off-line data access with selective-sync for on-the-go users (configurable by user security groups and file type)
- Multi-geo data residency options including US, UK, EU, and private cloud instances via On-Prem deployments
- Securely share files via e2e encrypted URLs with password & timeout features
- Access your data on desktop and mobile devices
- Real-time activity feed for your data gives you collaboration at a glance
- Data managers can organize, manage and classify files without requiring data access

Compliance & Access Management

Productivity isn't only for users, HighSide One delivers a productive administrative environment for team admins and data managers as well as a set of simplified compliance capabilities to meet the needs of even the most demanding legal and compliance users.



HighSide One comes with an integrated Compliance Suite that serves as the hub for all compliance related activities. In order to maintain a true E2E encrypted environment and deliver capabilities such as messaging e-discovery and archiving, HighSide's compliance users generate a cryptographically unique set of encryption keys that are appended to every message and file share within the platform. Data is not stored on a local server or device, ensuring the message and file data remains in it's E2E encrypted state within the HighSide cipher text data lake. Only when there is an investigation or compliance need does the user activate their keys and selectively access an immutable record of the activities within the platform.



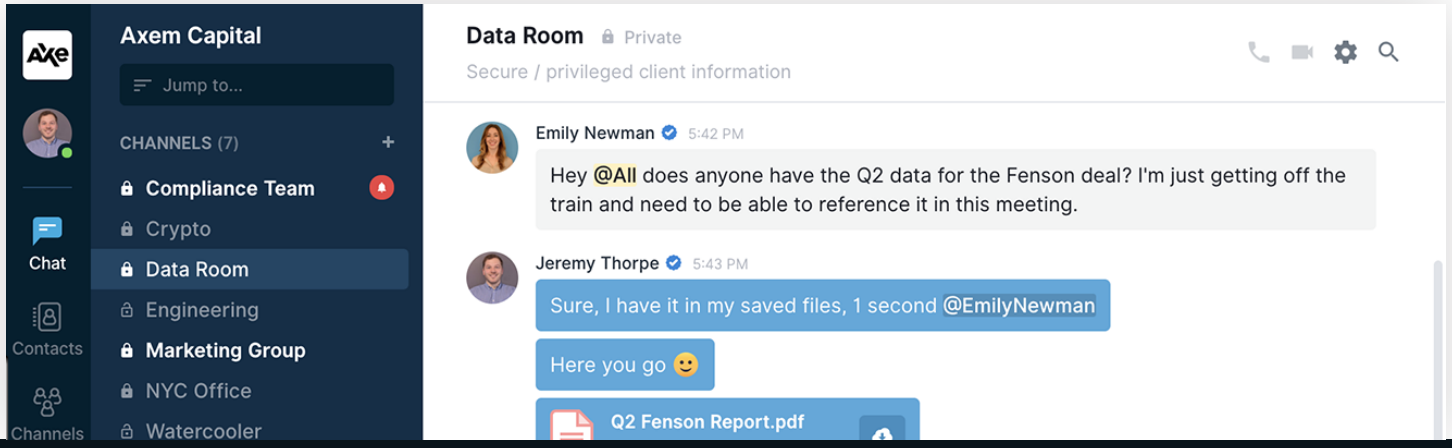
While the HighSide Compliance Suite delivers everything a legal or compliance user would need, many enterprise organizations have already invested in third-party compliance management platforms. Whether integrating via the HighSide streaming compliance events API or through filtered export of messages and files, HighSide integrates tightly into existing compliance configurations.

Ensuring compliance isn't all about logging and message discovery, it often comes down to user access controls. To meet the needs of large scale enterprise organizations, HighSide One integrates with Active Directory to provision and deprovision users. However, as an out-of-band collaboration system, HighSide does not rely on AD connectivity for user access management. The HighSide encrypted

Cloud SaaS, Data Residency & On-Prem

HighSide One can be consumed in different deployment options, none of which change the functionality or capabilities of the solution. Most customers choose to run in the HighSide secure cloud, but those with compliance or regulatory requirements dictating where data is resident have further options. The standard secure cloud is hosted in the United States, but full hosting locations in the United Kingdom and the European Union are available to Enterprise customers.

While HighSide's secure cloud offering is right for most organizations, some government and enterprise businesses have on-premise expectations for communications and data management applications - not a problem for HighSide. Leveraging an easy to deploy Kubernetes setup, HighSide's enterprise and government customers can quickly deploy a secure infrastructure to power their HighSide One team. Whether you opt for the secure cloud or the on-prem infrastructure, HighSide One's key features, capabilities, and compliance tools remain unchanged.



HIGHSIDE

HighSide is the recognized industry leader for Secure Communications & Collaboration, delivering NIAP validated software that enables teams to ensure their intellectual property, regulated data, and sensitive communications remain secure, compliant, and controlled.

Powered by a decentralized E2E encryption protocol, HighSide delivers productivity capabilities such as secure & out-of-band messaging, controlled file-sharing, and sensitive data management. In use by government agencies and enterprise organizations around the world, HighSide is forever changing the way the digital business works. From enabling teams to share and manage their sensitive business data to delivering a secure, highly available, and segmented system for mission, project, and cyber operations teams to ensure persistent communications, HighSide One delivers. With a full RBAC access control system, Active Directory connection for enterprise user management, and an integrated e-discovery and compliance suite, HighSide One is truly revolutionizing collaboration... securely.

highside.io
sales@highside.io