HIGHSIDE

Fortune 50 Financial Services Firm

Due to the sensitive nature of HighSide's usage at many customer organizations, the name and details of their business are representative, not exact. However, details around the requirements & needs of the customer as well as the usage & performance of HighSide are factual.

Case Study

Secure & Out-of-Band Communications & File-Sharing

Who is the Customer?

Acme Financial Corporation (AFC) is a publicly traded, US based financial services firm that provides mortgages and other loan products to consumers. Like most financial services firms, AFC places a high priority on ensuring the security of their customers' data, meeting industry compliance requirements, and protecting their intellectual property & infrastructure from constant cyber attacks. Within AFC the cyber operations team is responsible for coordinating security initiatives and executing incident response with a variety of internal and external stakeholders.

Customer Challenges

AFC's cyber operations team needed a secure, segmented and out-of-band system for communication and file sharing. Security leaders were concerned that their communications and sensitive data (IR playbooks, malware samples, disaster recovery plans, etc) were exposed to unacceptable levels of risk, both internally and externally – additionally they were aware that the reliance on a centralized system, such as Microsoft Teams, would expose their security operations in the event of a breach or a network compromise.

In addition to their need for an Out-of-Band communications platform for internal use, AFC's cyber team needed a way to communicate with their industry working groups, cyber first responders, and business partners.

Leadership was aware that traditional collaboration platforms were not only insecure but had centralized architectures that made them vulnerable to outage and compromise. However, being in a regulated industry, AFC has very tight compliance requirements to meet. Whatever system they selected had to meet their internal legal and compliance requirements for e-discovery, archiving, and message retention.

Key Concerns

- Without a segmented & secure communications platform, AFC's cybersecurity team could not ensure reliable communications during a breach or internal system compromise - impacting their ability to respond quickly.
- In addition to the security & operational integrity concerns, corporate administered systems did not offer flexibility to collaborate with external IR partners and industry working groups.
- While there are plenty of traditional collaboration & messaging apps available, none were an option as they lacked true E2E encryption, decentralized user management, secure file-sharing, messaging compliance, and e-discovery capabilities.

Customer's Must-Have List

- E2E encryption to ensure data integrity and to safeguard privileged communications
- Direct message and channel communications
- Encrypted meetings w/ screenshare for internal and external participants
- Active Directory integration w/ segmented user management allowing for continuous access regardless of network status
- Self-contained IAM system
- Full compliance suite delivering e-discovery and communications/ message archiving supporting legal investigations
- Ad-hoc guest collaboration and communications
- External encrypted file-sharing
- Desktop and mobile applications available
- Secure infrastructure and cloud hosting environment
- Disaster recovery support - failover users and self-contact access management

Meeting the Customer's Needs

HighSide One was selected after delivering on the must-have features and passing through a rigurous security, legal, and compliance review. Initially, AFC was only interested in HighSide's encrypted communications, but during the POC, the team identified significant value in HighSide One's SecureDrive data management and file-sharing capabilities.

HighSide One was selected for a number of reasons, but a few key differentiators drove AFC's selection.

- HighSide's decentralized / zero trust e2e encryption system
- Segmented cloud architecture
- Support for active-directory provisioning w/ stand-alone IAM
- Stand-alone compliance, legal and e-discovery suite.

HighSide One has been deployed as an out-of-band security and IT communications, secure file-sharing & collaboration application. Additionally, HighSide One is configured to operate as a disaster recovery / back-up collaboration system for a significantly wider user population.

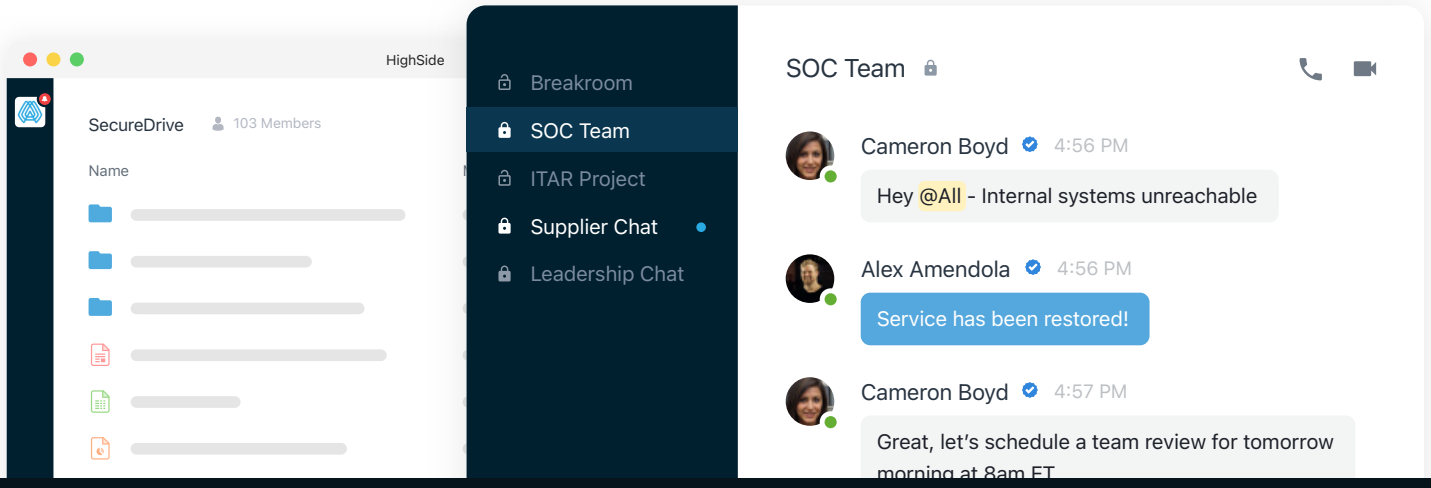
During the first year of operation, the use of the HighSide platform expanded beyond cyber response communications. The use of HighSide One has grown to supporting daily team standups, cross-industry collaboration and intra-department sensitive communications. Additionally, HighSide's SecureDrive is now the primary repository for IR playbooks, disaster response plans, and other sensitive cyber operations documents. HighSide is even being used for malware sample storage and sharing.

HighSide One: Out-of-Band Collaboration

HighSide's out-of-band collaboration platform provides a true end-to-end encrypted environment complete with the features and functionality your employees demand. Ensure every communication - chat messages, group conversations, file sharing & document collaboration, voice & video calls - are secure and compliant.

Integrated user management and real-time IAM sync gives security and compliance teams streamlined access controls based on pre-existing security policies. Automatically manage device authorizations and control when or where a user can access certain channels, chats, or files. Additionally, HighSide supports both internal team collaboration and third-party engagement in a single secure environment.

With a full compliance suite, a NIAP validated secure application, multi-region secure cloud hosting environments, and on-prem deployment options, HighSide brings modern business tools to sensitive, confidential and even classified projects.



HIGHSIDE

HighSide is the industry leader in Controlled File-Sharing & Collaboration, enabling teams to ensure their intellectual property, regulated data, and sensitive communications remain secure, compliant, and controlled. Powered by a decentralized e2e encryption protocol, HighSide's applications unify user-experience, productivity and data control.

Offering secure cloud, on-prem, or FedRAMP controlled deployment options, a continuously NIAP validated secure application, and FIPS 140-2 compliant e2e encryption, HighSide delivers out of the box security & regulatory compliance.

highside.io
sales@highside.io
866.693.8559