HIGHSIDE

Insecurities of Traditional Collaboration, Cloud File Storage, Sharing & Messaging Applications

WhitePaper

Executive Summary

In today's decentralized work environment, we've had to quickly adapt our security practices (or evolve, depending on how you look at it) to meet a new operating reality. Workers need a way to **remotely store, share and collaborate** around **sensitive data,** IT leaders need a way to ensure that only **authorized users** (in authorized locations, on authorized devices) can access internal services, legacy data stores and even cloud applications, and security and compliance teams need to make sure this is done **securely and in compliance** with government regulations.

Traditional cloud based sharing and collaboration tools are focused on the user experience with little concern for enterprise data security controls - in fact, many of the leading "business" tools were born from consumer applications. The lack of a security-first approach has left many organization's vulnerable across the tolls they rely on for data storage, collaboration, messaging and engagement.

Data security, data governance, and access controls have all been sacrificed in the name of collaboration and business continuity - but this doesn't have to be the case. This WhitePaper attempts to highlight some of the most glaring vulnerabilities these applications suffer from, but by no means is intended as an exhaustive list.

Key Vulnerabilities w/ Cloud Storage & File Sharing

In our new reality of distributed workers, we need to approach data sharing, access and collaboration with a new way of thinking. This way of thinking must prioritize security and compliance.

Consumers have long been drawn to the ease of use, simplicity and reliability of cloud storage solutions. Many of the big tech players in this industry have become household names such as box, Dropbox, OneDrive, and GDrive. Enterprises were traditionally resistant to these consumer focused startups, but consistent user pressure and a marketing campaign led by industry leaders started to sway IT leadership. However, simply marketing that you have enterprise security and compliance features does not make the product a secure solution.

There are many reasons as to why even the "enterprise" versions of consumer cloud storage solutions are not truly enterprise grade when it comes to security. The most obvious one however, is that they were built with a consumer acquisition & retention model in mind not an information security, compliance, or data access management focus. Let's take a look at the top security concerns that plague common cloud sharing and storage solutions and identify marketing pitfalls (such as claims of encryption that have little bearing on actual security) enterprise buyers should be aware of.

Browser Based Cloud Data Access Models

TL;DR: TLS/SSL encryption used for browser-based solutions is easily defeatable, vulnerable to browser exploits, simple memory exploits of applications (like file explorer, Outlook, etc.)

The TLS and SSL standards were built to allow for nation/states to eavesdrop on all traffic flowing over those channels. With the proliferation of 'work from anywhere', combined with the rash of home router exploits where attackers have injected SSL intercept capabilities into those devices, there really is no sense in relying on TLS/SSL to protect sensitive information from attackers. More information on the risks posed by TLS/SSL attacks on those who may be using non-enterprise (home, cafes, etc.) networks.[1]

How HighSide helps:

From a basic network analysis perspective, HighSide appears to use port 443 for its network communications. This is merely to take advantage of the fact that 443 is open on most networks. When looking at the packet structure within HighSide network traffic, it immediately becomes apparent that there is nothing like TLS/SSL being used for communications. In fact, HighSide has developed a new encryption protocol which leverages proven cryptographic algorithms (elliptic curve secp256 and per-message encryption using ephemeral AES 256 keys) instead of the highly-vulnerable algorithms and hashing used by traditional SSL. Also, there are no roots of trust which can be manipulated within HighSide's implementation. In traditional SSL and TLS implementations, if a device trusts an issuing root, any wildcard certificate from that root can be used to spoof legitimate TLS/SSL endpoints. In HighSide's implementation, there is no single root of trust.

How to distinguish a vulnerable cloud storage system?

Is it available to users through a web browser? Then it's vulnerable.

Real World Proof Point

China telecom rerouted a massive set of EU network traffic. Combined with their injected roots of trust in devices, this allowed Chinese surveillance teams to gain access to ALL TLS/SSL traffic flowing through those EU networks.[2]

On average, every employee has access to **11 million files**

17% of ALL sensitive files are accessible to ALL employees.

Bring Your Own (not very private) Keys & Memory Manipulation

TL;DR: Solutions that support a Bring Your Own Key option are not truly end-to-end encrypted and leave user's data vulnerable to provider breaches, insiders, and the aforementioned browser vulnerabilities.

Even in cases where Bring Your Own Encryption/Key (BYOK), the data must be decrypted in the cloud data storage repository. This allows for any employee of the cloud storage company to gain access to the data (yes, even in cases of BYOK, certain memory manipulations can be made to gain access to cloud stored files, and this has been done in the past for legal compliance reasons). This also allows anyone with access to the BYOK key material to gain access to the files without notifying the data owner of their access.

If a cloud storage system allows for cloud-based DLP rules processing, then it is not end-to-end encrypted. Solutions like Box, DropBox, OneDrive and OwnCloud all suffer from the fact that files are not truly end-to-end encrypted.

How HighSide Helps

HighSide's SecureDrive only decrypts the files at the endpoint, the cloud services are only used to store and forward encrypted file changes, and those changes are only correlated by the HighSide client. While we take all industry-standard efforts to protect our back-end services (whether those hosted for public use on AWS, within private AWS enclaves or private Azure environments), we assume for purposes of our threat model that those back-end servers and services can be compromised at any time. With all of the keys distributed to the clients, there is no centralized key repository which can be used to gain access to all of the files. Only authorized users on authorized devices can access files shared through the system.

Real World Proof Point

The Dark Halo attack showed that sophisticated attackers used weaknesses in M365 to allow for unauthorized access to 'encrypted' files within OneDrive. By abusing privileged access to M365 core services, the attackers were able to gain access to all files within OneDrive. In some cases, the attackers leveraged the fact that tenant administrators had not properly configured the Customer Lockbox feature within M365, which allowed the attackers to move among multiple M365 tenants and gain access to many organizations' data within OneDrive.[3]

Remote workers have caused a security breach in **20% of organizations.**

According to security research published by security firm Malwarebytes[4]

Cloud-based **cyber attacks rose 630%** between January and April 2020.[5]

81% of ALL DATA BREACHES involved weak or stolen passwords[6]

How to distinguish a vulnerable cloud storage system?

Any system which allows for a single data labeling process or which inspects files on the back-end for data is vulnerable to privilege abuse attacks which allow for unauthorized access to

Key Vulnerabilities w/ Collaboration & Messaging

There are two types of applications in use at enterprise and government organizations. The first being technology borne out of the consumer world with minimal security capabilities. These apps will often present easily compromised or vulnerable components of their system as secure. While technically accurate with their security claims (TLS/SSL in-transition encryption for example), beyond basic consumer usage, they fail to secure data, accounts, and information against even the most unsophisticated of adversaries.

The second type of technology are platforms that tout their security bonafides. Unfortunately, the simple thinking that the later is more secure than the former isn't exactly right. Let's dive into the security challenges present in the first group of technologies, those that

Standard consumer & end user focused apps

Apps such as Microsoft Teams, Slack, Mattermost (and even email) were never designed to withstand the level and sophistication of cyber attacks currently being levied against cloud applications. The list of vulnerabilities these apps face is too long to dive deep into all of them.

Most common & dangerous vulnerabilities

- Simple phishing & spoofing attacks
- Single-point-of-failure centralization of keys (a breach of the server, or of a sufficiently privileged user, leads to a breach of the entire organization)
- Keys generated and controlled by service providers, not by your organization (counterparty risk)
- Messages & files can be altered by attackers or sufficiently privileged users
- Known TLS/SSL vulnerabilities including man-in-the-middle attacks
- Common browser-based attacks
- Insider threats (Snowden-style attacks)
- Nation-state surveillance/eavesdropping

inSecurity in “Secure” Apps

When evaluating applications that tout security features as a core competency, like “end-to-end encryption”, it’s important to look a little deeper. Applications such as WhatsApp, Wickr and Signal, while presenting encrypted environments have serious vulnerabilities tied to user authentication, meta data harvesting, key management, product design and more. Additionally, these platforms, while security focused, were built for consumers without the security, access management and compliance capabilities that government and regulated industries require. This makes them at-best impractical for use by government and military agencies, and at-worst extremely dangerous to those organizations..

For example Signal, widely used by executives across the government, military and regulated industries, suffers from:

- **Authentication vulnerabilities:** Signal users are authenticated based on their phone number, leaving them vulnerable to a myriad of attacks ranging from SS7 to sim-swapping
- **Spoofing:** because Signal has a consumer-first design, there are no organizational controls whatsoever; users can simply change their display name and profile picture to impersonate someone else
- **Metadata leakage:** Signal can expose sensitive metadata to their servers/ attackers, potentially even including your physical location

Remote work has increased the average cost of a data breach **by $137,000.**

According to security research published by IBM[7]

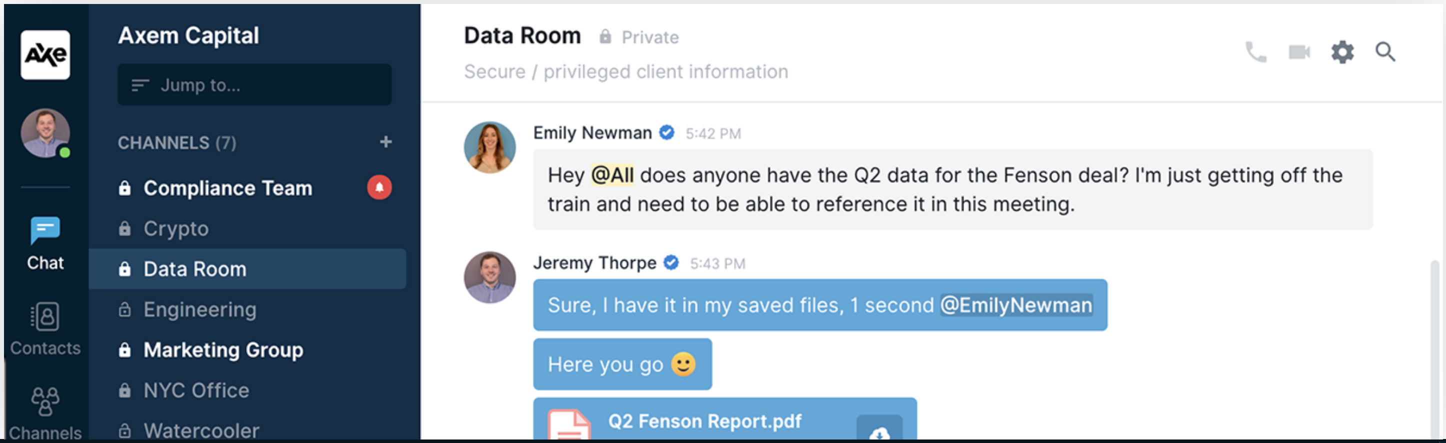
[1]: https://www.zdnet.com/article/for-two-hours-a-large-chunk-of-european-mobile-traffic-was-rerouted-through-china/
[2]: https://www.iansresearch.com/portal/faculty-reports/ensure-traveling-users-understand-and-mitigate-potential-infosec-risks
[3]: https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/
[4]: https://resources.malwarebytes.com/files/2020/08/Malwarebytes_EnduringFromHome_Report_FINAL.pdf
[5]: https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/
[6]:Microsoft
[7]: https://www.ibm.com/security/data-breach

HighSide: Collaboration, Cloud Storage & File Sharing for Security & Compliance Conscious Organizations

HighSide's secure 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 control 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 and a FedRAMP cloud hosted environment supportingisolated computer environemnts up to Impact Level 6, on-prem deployment options and a public cloud, HighSide brings modern business tools to sensitive, confidential and even classified projects.



Emily Newman 5:42 PM
Hey @All does anyone have the Q2 data for the Fenson deal? I'm just getting off the train and need to be able to reference it in this meeting.

Jeremy Thorpe 5:43 PM
Sure, I have it in my saved files, 1 second @EmilyNewman
Here you go 🙂
Q2 Fenson Report.pdf

HIGHSIDE

HighSide is the global leader in secure cloud sharing, collaboration & access management. Powered by a distributed cryptographic key management infrastructure, HighSide's suite of products enable businesses to engage securely in a remote first world. Through our zero-trust technology, teams have access to a modern unified communications and file sharing platform including voice, video, text and files, reducing risk of shadow IT and reliance on dated and insecure communications channels.

HighSide delivers applications that users actually want to use and that security leaders want to deploy. Founded in 2015, the company has offices in Columbia, MD, Esch-sur-Alzette, Luxembourg and New York, NY.

highside.io
sales@highside.io