

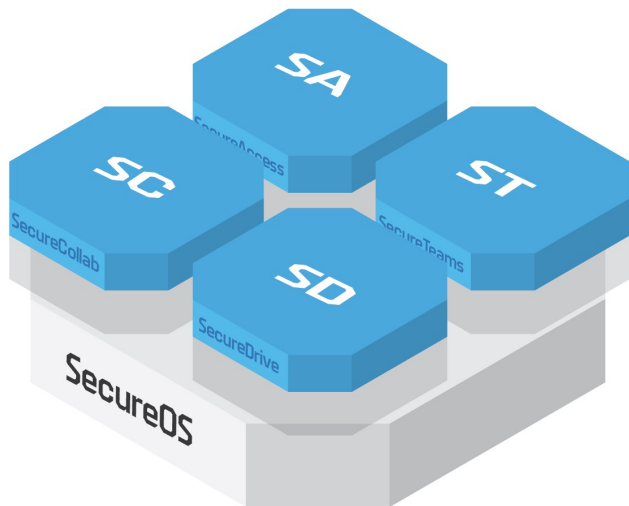


The Leader in Secure Collaboration & Distributed Data Access Controls

Enabling effective collaboration while ensuring data security,
access control and compliance

Crypto Powered, Business Enabled

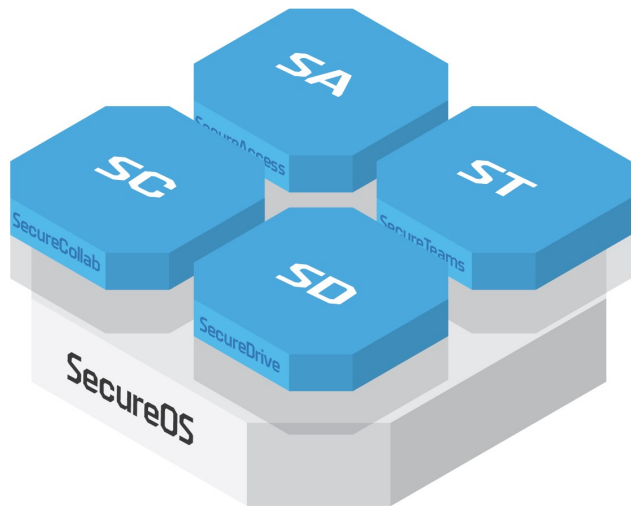
Powered by a distributed cryptographic key management infrastructure, products enable businesses to engage securely in a decentralized,



For the first time in my 30 years working here, we have a reliable and secure way to communicate with team members and suppliers without having to worry about loss of our intellectual property or regulatory compliance problems.

Director Research and Development IT at a global materials science company

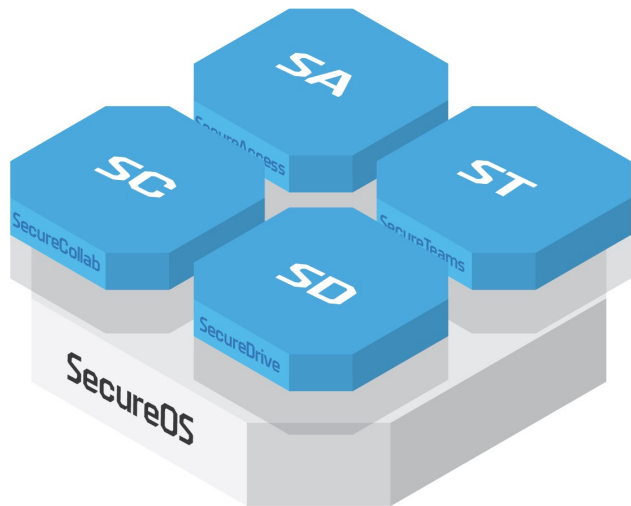
SecureOS: HighSide's Distributed Encryption System



SecureOS

Designed as a high-integrity communications layer, the SecureOS architecture is a cross-platform software system which allows for users to enjoy the benefits of confidentiality and integrity through various applications. SecureOS's strength lies in its distributed private root of trust system - basically, the way that it distributes encryption keys and manages identity away from centralized identity stores, many of which rely on traditional Public Key Infrastructure (PKI).

HighSide Product Suite



SecureCollab

HighSide's secure collaboration platform, SecureCollab, bridges the gap between data security requirements and business productivity demands. A modern collaboration environment built for security conscious organizations and regulated industries, provides a true end-to-end encrypted environment complete with the features and functionality your employees demand.

SecureAccess

HighSide's zero trust access & identity management application fulfills the promise that authentication security should enable users, not confound them. Broker access with or without credentials to internal and 3rd party systems via HighSide's distributed private root of trust Identity environment and integrated user management.

SecureDrive

SecureDrive ensures data portability without sacrificing data security, compliance and real-time access controls. Fully encrypted file sharing & cloud storage merges the ease of use employees expect from consumer grade systems, with the data security and compliance controls enterprise's require.

SecureTeams

Encrypted messaging integrated directly into Microsoft Teams ensures both sensitive and every day business conversations can take place in the same place. Push-button deployment brings end-to-end encryption to Microsoft Teams, allowing users to securely encrypt messages and files sent through your existing Teams deployment across all devices. features you can't find elsewhere.



SecureCollab: HighSide's Secure Collaboration Platform



HighSide's secure collaboration platform, SecureCollab, bridges the gap between data security requirements and business productivity demands.

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.

Why HighSide?

- ★ Unmatched security & compliance functionality
- ★ Feature parity with less-secure alternatives
- ★ Easy to use and deploy
- ★ On-prem or SaaS
- ★ Secure even on BYOD/commodity devices
- ★ Built-in MFA/identity controls





SecureCollab: Advanced Features




- 1-to-1 & group messaging + voice/video conference calls
- True e-2-e encryption & identity management/controls
- Built-in geolocation-based access controls
- Can be deployed in the cloud or on-prem
- Secure on BYOD devices with device hygiene checks & local encryption
- No concept of usernames & passwords, novel authentication methodology not vulnerable to phishing/spoofing
- E-2-e encrypted file storage archive with functionality similar to OneDrive/Dropbox
- Protection from ransomware & zero-day attacks
- Built-in MDM functionality with the ability to lock out & remote-wipe lost/stolen devices or compromised users
- DLP & data residency controls
- RBAC & information barriers
- “Secure by default” architecture; nothing for users to turn on, configure or learn in order to use the app securely





HighSide vs. “Enterprise” Collaboration Apps



	 TEAMS	 ZOOM	 HIGHSIDE
1-to-1 & group chat, file sharing, etc.	✓	✓	✓
On-prem deployment options	✗	✓	✓
End-to-end encrypted messaging & files	✗	✗	✓
Closed-loop voice & video encryption	✗	✗	✓
High entropy tokens/identifiers	✗	✗	✓
Geolocation-based access controls	✗	✗	✓
Doesn't rely on usernames and passwords	✗	✗	✓
Doesn't rely on public TLS/SSL infrastructure	✗	✗	✓
User ID verification system	✗	✗	✓
Built-in MDM/DLP	Add-on	✗	✓
Granular user permissions	✗	✗	✓
Built-in eDiscovery/archiving compliance	Add-on	✗	✓



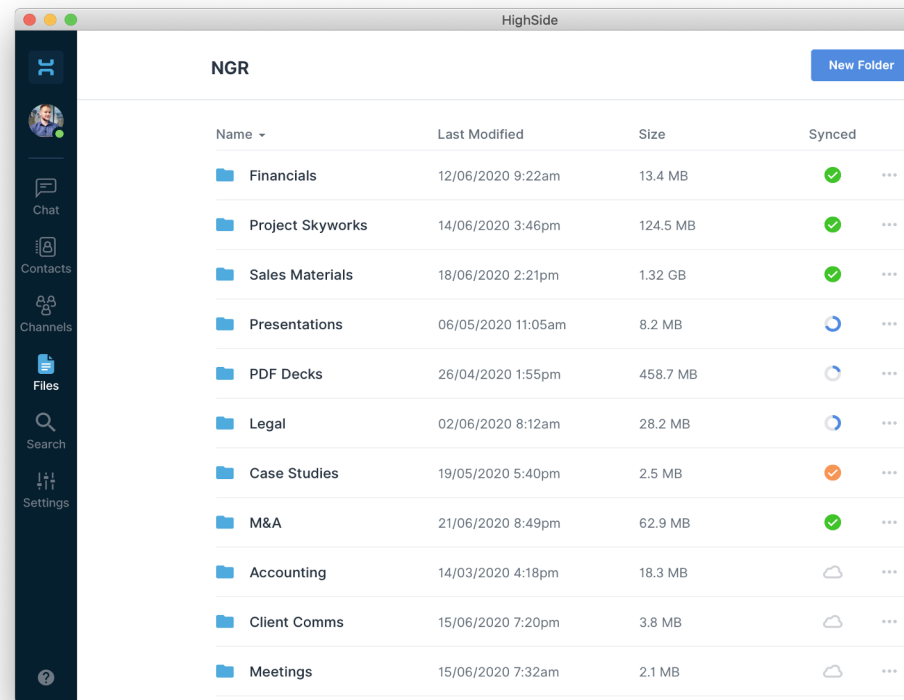
SecureDrive: Encrypted File Sharing & Cloud Storage



SecureDrive ensures data portability without sacrificing data security, compliance and real-time access controls

SecureDrive is a fully encrypted file sharing & cloud storage application - merging the ease of use employees expect from consumer grade systems, with the data security and compliance controls enterprise's require. Leveraging **SecureOS**, SecureDrive enables the freedom to securely share & collaborate across internal and external teams.

- Security first and foremost: HighSide's revolutionary distributed key architecture has "no single point of failure" and has no reliance on certificate authorities or SSL ensuring your files stay your files
- Built in data residency & retention tools give you granular control over your data - control who, what, where and when your users are able to access data
- Best-in-class version control enables multi-user editing on the same document providing a secure way to collaborate on documents and files regardless of file type.





SecureDrive vs. DropBox

Traditional “enterprise” cloud sharing and storage solutions lack real data security, compliance and access management controls.

	 DROPBOX	 HIGHSIDE
End-to-end encrypted?	✗	✓
Each msg/file cryptographically signed?	✗	✓
User identity authentication?	✗	✓
Built-in MDM & DLP	✗	✓
Relies on passwords for security?	Yes	No
Relies on SSL/TLS for security?	Yes	No
Users must trust provider?	Yes	No
Provider can access your data?	Yes	No
Max file transfer size?	20GB	1,000 GB+
Man-in-the-middle SSL attacks?	Vulnerable	Protected
Phishing attacks?	Vulnerable	Protected
Spoofing attacks?	Vulnerable	Protected
Web-based attacks?	Vulnerable	Protected
Server-based attacks?	Vulnerable	Protected
Msgs/Passwords previously compromised?	Hacked	Never

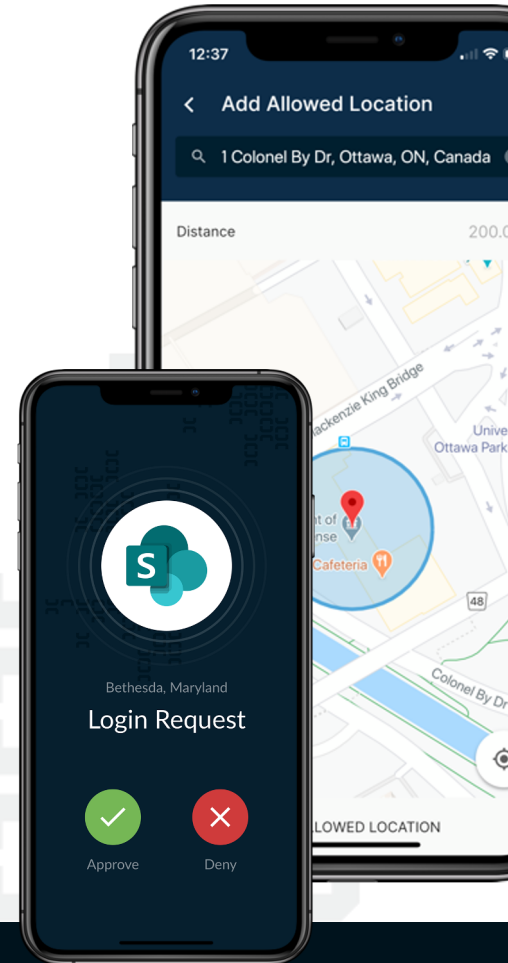


SecureAccess: HighSide's Distributed MFA

Zero Trust Access & Identity Management fulfills the promise that authentication security should enable users, not confound them

SecureAccess provides zero trust multi-factor authentication & identity management for both traditional and federated identity environments. Leveraging the **SecureOS** platform, and brokering access with an unlimited (x) number of trust factors through SAML, OAuth, OpenID Connect or LDAP-capable application controls, **Secure Access** provides a high integrity authentication mechanism that puts usability front and center.

- 4x “Factors” of Authentication: Who, What, When, Where
- **Proprietary geolocation-based encryption & access controls based not only IP addresses, but** GPS, Wifi, cellular towers, bluetooth mesh networks & more
- Ability to meet stringent export controls such as ITAR, as well as GDPR, HIPAA & more
- Built-in MDM functionality to remotely revoke access & keys
- Authentication context for users; “CallerID” for each request
- Simple integration with Active Directory for role-based access controls
- Deep integration with Palo Alto Networks next-gen firewalls to protect legacy & on-premise applications and data
- Granular logging of all security, session & privacy data, ready for SIEM import
- Available on iOS, Android, Windows, Mac & Linux devices



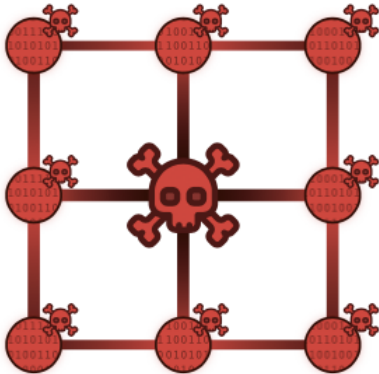


SecureAccess: Centralized vs. Distributed Authentication



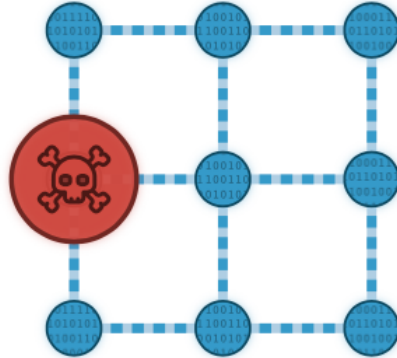
User identities are generated/controlled by the MFA provider, not your organization.

A breach of the provider, or a sufficiently privileged user within your organization, can result in a security breach of your entire organization.



Organizations generate their own encryption keys. HighSide never has access or control of customer keys.

A breach of any one user, even admins, does not result in a breach of your entire organization.





SecureTeams: HighSide's E-2-E Encrypted Teams Plugin



Enterprise security built for Microsoft Teams the HighSide way

HighSide's secure Teams extension is a lightweight distributed key management and encryption system that runs underneath your existing Teams deployment. It empowers your users with the ability to easily share sensitive information/data through Teams without having to install any new software, and protects your organization from sophisticated attackers/insider threats.

Why HighSide's Encryption Extension?

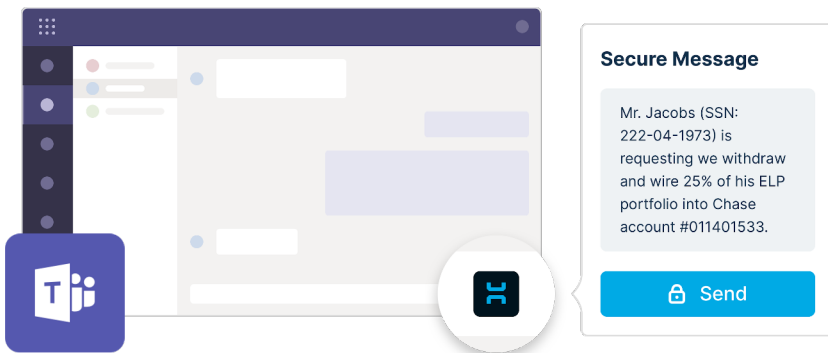
- ★ Eliminates the global admin/insider threat risk
- ★ Abstracts the keys away from Microsoft
- ★ Integrates well with Microsoft's DLP rules
- ★ Protection for Teams, similar to how you protect Outlook email
- ★ Incredibly easy to use, deploy and onboard users

	Standalone Teams	Teams + HighSide
End-to-end encrypted messaging & files?	✗	✓
Doesn't rely on TLS/SSL?	✗	✓
User ID verification system?	✗	✓
Keys NOT accessible to Microsoft?	✗	✓
Built-in MDM/DLP?	Add-on	✓
Man-in-the-middle SSL attacks?	Vulnerable	Protected

Summary of HighSide features compared to known Microsoft Teams features as of April 13, 2020.



SecureTeams Extension Provides You With:



- True e-2-e encryption; no HighSide/Microsoft servers or employees will ever have the ability to decrypt messages sent through the extension
- Novel distributed key architecture with no single point of failure and no reliance on TLS/SSL for encryption
- Protection from global admin/privileged user attacks & insider threats
- Built-in MDM functionality giving your organization the ability to revoke user access to data at any time
- Frictionless, automatic setup & onboarding for your users
- Available everywhere they use Teams, on all their devices and browsers
- Quick/easy deployment for your Teams administrators

"Employees won't keep secure practices on their own, and employers must consider how they will secure workforce communication over messaging and collaboration tools, just like they did with email."



Archiving & Compliance



With all HighSide apps, built-in archiving & compliance capabilities help financial organizations meet FINRA & SEC requirements for securely storing and transmitting data.

HighSide's built-in compliance suite allows for auditability of **immutable event, message and metadata logs**, or exporting logs into existing monitoring/archiving systems.

HighSide has previously been **measured against NSA ICD 503, DISA STIG and NIST 800-171 standards** for US government and Fortune 100 implementations where protection of sensitive military IP was required.

HighSide

COMPLIANCE

Dashboard

Message Log

Event Log

Live Event Log

Settings

Event Log

Configure a search below to see the event log.

22 Jul 18 26 Jul 18 [View Log](#) [Save Log](#)

Showing 92 results.

Jul 23 at 1:13 AM
Bob Jones successfully connected.
London, United Kingdom · 81.147.15.193 · HighSide Desktop Client 2.1.1 · Darwin 17.5.0 · Full Info

Jul 23 at 1:17 AM
Alice Smith created a new private channel called "BizDev".
New York City, United States · 96.102.65.172 · HighSide Desktop Client 2.1.1 · Darwin 17.5.0 · Full Info

Jul 23 at 1:18 AM
Mike Francoise successfully connected.
Paris, France · 76.726.19.201 · HighSide Desktop Client 2.1.1 · Darwin 17.5.0 · Full Info

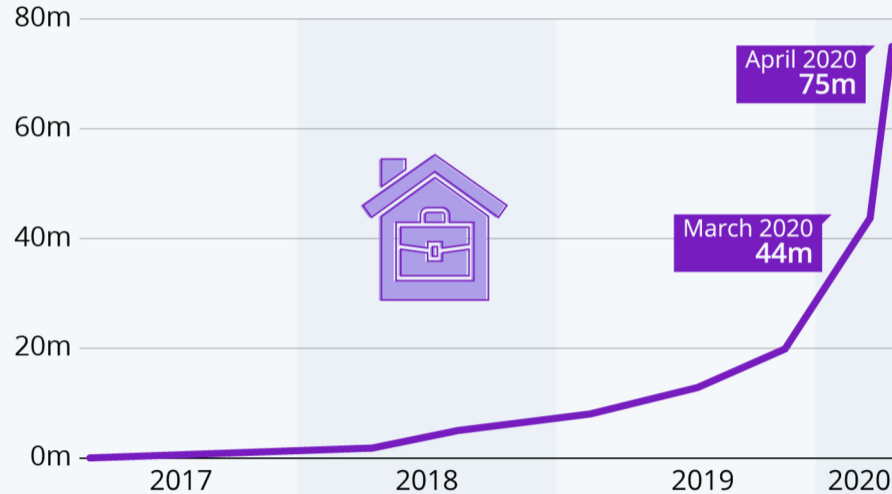
Jul 23 at 1:18 AM
Bob Jones invited a new user "Henry Davies" to the company.
London, United Kingdom · 81.147.15.193 · HighSide Desktop Client 2.1.1 · Darwin 17.5.0 · Full Info

Jul 23 at 1:18 AM

Why Do You Need HighSide?

COVID-19 Accelerates Adoption of Remote Work Collaboration Apps

Number of daily active users of Microsoft's workplace communication app Teams



Source: Microsoft

“From Microsoft Teams to Slack, **today’s collaboration platforms are not secure enough for sensitive data.**” - Sorell Slaymaker, TechVision Research & former Gartner Analyst

These platforms suffer from:

- Centralization of keys & single-point-of failure architecture
- Reliance on usernames & passwords for security
- Phishing & spoofing
- TLS/SSL vulnerabilities
- Weak privacy policies/a history of monetizing customer data
- Man-in-the-middle attacks
- Browser & server-based attacks
- Credential leakage through integrations
- Provider-controlled encryption
- Well-documented history of major data breaches





“Hacking **Slack** accounts: as easy as searching Github.”



“Vulnerability in **Microsoft Teams** could allow hacker to gain complete control of your infrastructure.”

Forbes

“New **Microsoft Teams** Password Hacking Threat To 75 Million Users.”

Leading to a *massive* increase in attacks...

“Usage of collaboration platforms such as Microsoft Teams and Zoom has jumped 600%, with McAfee estimating that external **attacks on cloud accounts are up 700%** since January.”



“It's Not Just Zoom. Google Meet, **Microsoft Teams**, and Webex Have Privacy Issues, Too.”

WIRED

“**Zoom** Flaw Gives Hackers Easy Access to Your Webcam.”



“Hackers Penetrate **Pentagon** Email.”



What About Protecting 3rd Party Apps and Data Behind the Firewall?

Because **81% of all security breaches involve weak or stolen login credentials**, organizations are increasingly turning to MFA as an additional layer of protection against identity-based attacks.



Unfortunately, **traditional SSO & MFA providers aren't solving the problem.** They are vulnerable to sophisticated attacks, suffering from:

- Centralization of keys & single point of failure architecture (Ex. RSA/Lockheed)
- TLS/SSL Vulnerabilities
- Easily spoofable location restrictions (often relying exclusively on IP addresses)
- Easily intercepted & difficult to use authorization codes
- Inability to protect on-prem/legacy data & applications

[1] <https://www.verzondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/>

[2] <https://www.scmagazine.com/home/security-news/rsa-confirms-lockheed-hack-linked-to-securid-breach/>



**“RSA CONFIRMS
LOCKHEED HACK
LINKED TO SECURID
BREACH.”**

Lockheed Martin suffered a major breach of secret US military technology linked to their MFA provider, RSA SecurID, being compromised.



Already Committed to Microsoft Teams?



When you send a message on Microsoft Teams today, who can **intercept/manipulate it**?

1. Microsoft Servers/Employees
2. Office 365 Global Administrators (insider threat)
3. Nation/states with lawful or compromised TLS/SSL certificates
4. Any attacker who successfully:
 - Breaches the Microsoft Server
 - Man-in-the-Middles the SSL connection
 - Compromises *any* of your Administrators (“Privileged Access Attack”)

Cybersecurity

INSIDERS

“WHEN IT COMES TO DATA ENCRYPTION, WHICH APP IS BETTER - SLACK OR MICROSOFT TEAMS?”

Neither. Enterprises concerned about data-at-rest protection should look to third party security technologies.”

What Happens When a Bank is Hacked?



Financial Loss

Avg. **\$7.91 Million** per Incident
+ Regulatory Fines



Customer Attrition

60% of customers think about leaving, **up to 30% do**



Opportunity Cost

~206 days to detect a breach,
and ~ 70 days to contain;
ongoing training + lawsuits,
remediation



Employee Termination

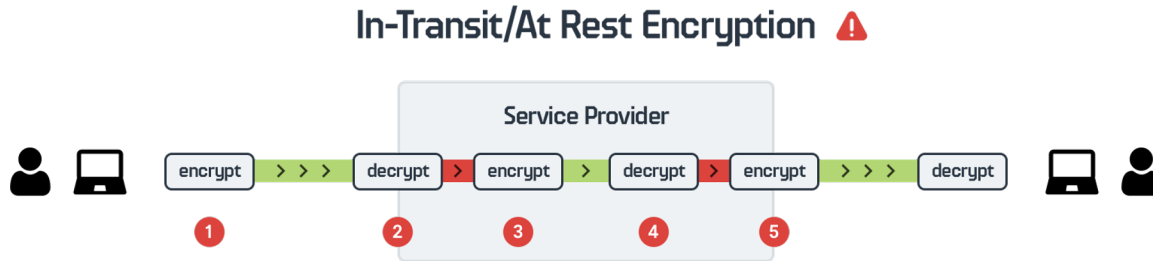
31% of breaches lead to
executives getting fired

Collaboration breaches are made **exponentially worse** because of single point of failure encryption architecture, and TLS/SSL vulnerabilities.

Because of the way most collaboration apps encrypt data, a breach against one becomes a breach against your entire system/server/application.

With in-transit, and at-rest, encryption your data is *necessarily decrypted at the server*. Data may then be re-encrypted at-rest, but this is almost useless because the server has the decryption keys. This is a single point of failure for your organization.

EKM/key management servers *do not* eliminate the risk.



<https://highside.io/blog/forest-applesfbj-slack-gmail-have-backdoors/>

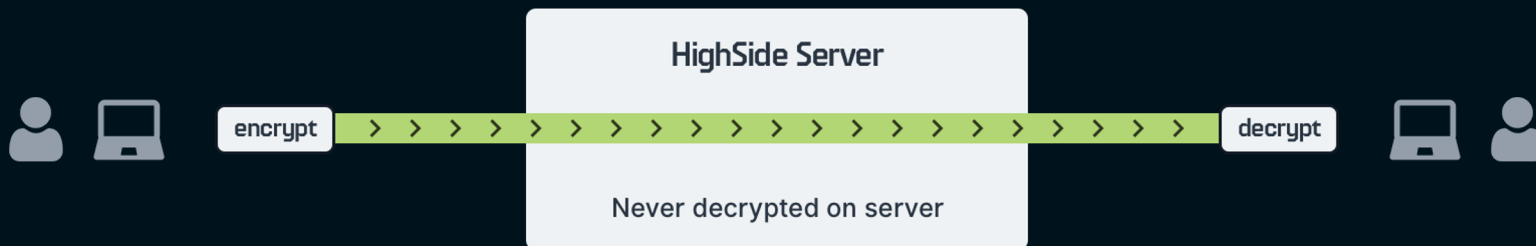
1. Data is encrypted with TLS/SSL (vulnerable to intercept & manipulation)
2. Data is then temporarily decrypted on the server (service provider/attackers can access)
3. It is then re-encrypted w/ a shared server key ("single point of failure")
4. Data is again temporarily unencrypted by the server (due to the way TLS/SSL works)
5. Finally, it is again re-encrypted w/ TLS/SSL and sent to the recipient (vulnerable to intercept & manipulation)

Solution: HighSide's Distributed Identity & Encryption Protocol

HighSide has developed the world's first distributed private root of trust system which can be easily and rapidly deployed without any dependencies on traditional public key infrastructure.

What that means is, with HighSide's protocol there is no single point of failure, no reliance on TLS/SSL, and a true zero-trust implementation which cryptographically proves your users are who they say they are, are where they're supposed to be, and restricts their access only to the data you've explicitly granted them.

End-To-End Encryption





HighSide, Inc.
Columbia, Maryland HQ
<https://highside.io>

Contact & Support

For questions on deployment options, or support with testing, please contact:



support@highside.io

sales@tetranetuk.com

Tetranet Limited

Offices 1 St. Mary's Courtyard, East Farm
Codford, Warminster, Wiltshire BA12 0PG

T: 01926 356580 | M: 07789861675

E: mquick@tetranetuk.com

TetranetUK.com