TechVision RESEARCH

Protection 101: Why Your Business **Needs a Secure Collaboration Tool** Now

Analyst Report

Sorell Slaymaker, TechVision Research

TechVision RESEARCH

Why Today's Collaboration Platforms Are Not Secure Enough

From Microsoft Teams to Slack, today's cloud collaboration platforms are not secure enough for sensitive data. Messaging in workplace environments has overtaken email and other formal B2B systems because they are responsive, real time, and collaborative, just like in our personal lives. Enterprises and government agencies need modern messaging-based collaboration tools and also want to protect their intellectual property while meeting stringent compliance and privacy regulations. In order to achieve this, they should utilize a solution that includes a zero-trust architecture and multi-factor authentication while empowering security administrators to set policies controlling data access, based on time and location.

Additionally, enterprises today are exposed to the communications infrastructure vulnerabilities – described below - even if employees follow all guidelines and use typical security products. Enterprises should look for a solution that enforces a "least privileged access" approach to stop critical data leakage, while giving employees a secure channel to collaborate. A leading zero trust encrypted collaboration vendor, HighSide, is evaluated at the end of this report.

Why Today's Collaboration Platforms are Not Secure Enough

Many enterprises and users assume their mobile devices are secure and that using a corporate Mobile Device Management (MDM) solution is all the security they need. As part of this assumption, many organizations are using Short Messaging Service (SMS) to a mobile device as part of a multi-factor authentication strategy. While this is better than just a standard username and password, it is not good enough for sensitive information. Here are some security short-comings of collaboration platforms that are commonly used:

No SMS Encryption

SMS messages are sent as clear text which is readable by anyone on the sender's carrier network, anyone on the carrier-interchange network, and anyone on the recipient's carrier network. There is no integrity in SMS, it is vulnerable to all types of attacks, including the one suffered by German banking customers in 2017 as reported in The Register.

SMS Hijacking

Organized crime and sophisticated hackers can motivate international mobile network operator employees to misdirect SMS messages from the legitimate user to an attacker's device for a period of time to capture the private keys associated with a user's account. SMS services are not high-integrity systems, as the legitimate user would not be notified of the misdirection or the keys being sent to the attacker. The victim will get to know the consequences often much later after the attack. This was the case with Metro Bank UK Customers in 2019 which raised the bank's risk exposure by $900 million.

The US Department of Homeland Security issued a warning on SMS "...it's time to stop using SMS for sensitive stuff... [SMS] can be exploited by criminals, terrorists, and nation-state actors / foreign intelligence organizations"

Cellular Communications Infrastructure Vulnerabilities

State-sponsored attackers have gained access to cellular network subscriber information which can then be used to gain access to large amounts of meta data. For organizations concerned with protecting the integrity of the data their users are sharing, the disclosure of Call Detail Records (CDRs) is a significant threat if users are relying on SMS or any communications platform which relies on SMS for authentication or encryption key delivery. One example of this is Operation-Softcell.

SIM Swapping Exposure

The Subscriber Identity Module (SIM) inside a smartphone is used to uniquely identify its owner. Criminals who gather details about a victim such as their mobile phone number can get a wireless network company to transfer a phone number to a new phone for a short period of time. Attackers can then trick banks and other companies into granting a password reset sent to a new phone, enabling them to gain entry into a victim's most sensitive online accounts. This problem was recently reported in the Wall Street Journal.

iMessaging Weaknesses

iPhone users will claim that iMessage is a superior technology, but it is vulnerable to just as many problems. For example, every iPhone inherently trusts over 150 organizations, some of which are affiliated with nefarious, known-cyber-attackers and authoritarian regimes. Apple makes the list of these trusts available on their help website. The map below lists of some of the countries, in addition to the United States of America, which are allowed full eavesdropping on iMessage:

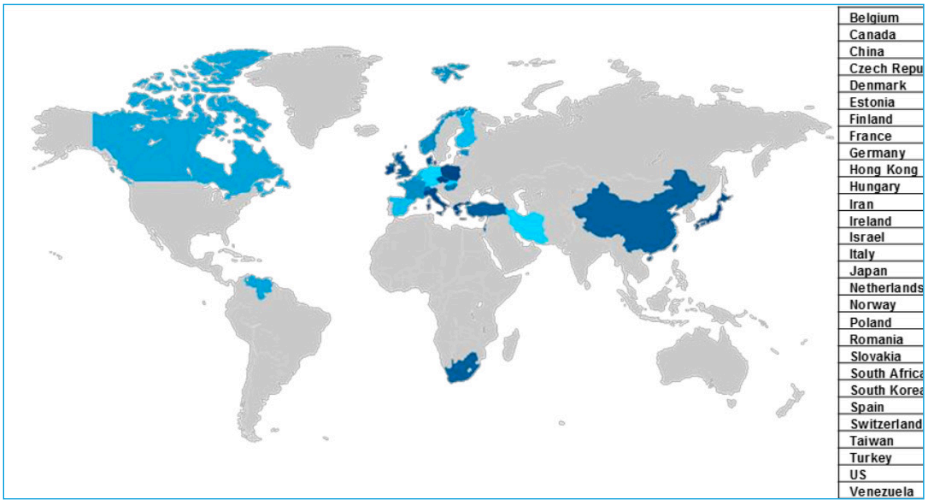


Figure 1: Countries That Have Access to Apple's iMessage

Application Spying Risks

Jealous lovers, frenemies, and other acquaintances who have physical access to your mobile device(s) while you are sleeping, in the shower, or at the gym can load spyware on your mobile device. Once running, they can monitor and record phone calls, track GPS location, read emails and instant message chats, check online activities, view photos, videos, and calendar entries, and remotely control the device. XNSPY is an example application that anyone can acquire for a monthly fee.

Consumer-Grade 'Secure' Messaging Apps

WhatsApp, Signal and other consumer-grade secure messaging applications rely on users' mobile phone numbers as unique identifiers to deliver private key material. Due to the risks outlined above in the SMS and SIM Swapping sections, attackers can temporarily hijack the target user's SMS number (either virtually through and international carrier or physically through a SIM swap), send a request to the Signal or WhatsApp service and then receive the recovery

Fact - Messaging Apps are Not Secure Either

Relying on an email address or phone number has inherent security flaws and not secure enough for highly privileged, confidential, or intellectual property.

keys for those applications, giving the attacker full access to messages and information sent through those systems. With the disclosure of state-sponsored attackers harvesting CDRs, that information can be used by those attackers to map out which consumer-grade apps that teams are using, then go about harvesting the keys for those consumer-grade apps to gain access to content shared through those platforms.

Fact - Too Many Messages Open to Too Many People

Team applicatiobns make messages available for everyone in that group versus enforcing controlled, need-to-know, and least priveleged messaging access

'Enterprise-Grade' Cloud Messaging Susceptibility

Cloud based messaging allows back-end server operators access to all of the data that is sent through the system. While there are rules that the operators adhere to that minimizes this possibility, there is still potential for their employees to violate those policies or for attackers to design exploits which bypass these policies. Permission models are quasi-public and not based on principles of need-based and least privileged access controls, including for guest accounts. This means guests (those who are not employees of your organization) can access documents in channels, resources, chats and applications. Thus, enterprises struggle to control or have visibility into what the organization is sharing. This is especially true when the service operator is presented with lawful intercept demands, in which a government law enforcement or espionage teams order the service operator to share all of the enterprise's information with them, many times without the enterprise's knowledge or consent. This is a concern for companies that are sensitive to information intercept by governments. The passage of the CLOUD Act gives US Law Enforcement full capability to intercept and store any data which they deem to be within the bounds of any ongoing investigation.

Shadow IT

The vast majority of people automatically default to using tools and applications they already know or perceive as the easiest to use or most used by others. This is no different with employees. If the tools the internal IT department provides are not in the 'known, easy and used-by- others' categories, they will be ignored and replaced in the daily working process. This means that sensitive company data routinely flows through Dropbox, Slack and WhatsApp without the owner's consent or knowledge. Security concerns are further exacerbated by trends such as BYOD (Bring Your Own Device) and BYOA (Bring Your Own Application) and the Gig Economy.

Nation State Security Risks

As if these vulnerabilities were not bad enough, there are also serious risks that international business travelers face. Customs in many countries requires

the user to provide their devices and passwords prior to leaving the country. Intellectual property is worth a lot to the right buyer, and where money is involved there will be corrupt and malicious officials who will steal information. Organized crime and hackers are becoming more like spies and recruiting employees and officials to help them exploit enterprises.

Compliance and Privacy

Regulations create liabilities for those companies which do not implement the proper tools and controls. Recent regulations like GDPR, ITAR, HIPAA, CCPA (California Consumer Privacy Act), and local labor laws require enterprises to have data controls in place to protect sensitive data in all situations, regardless of which systems are used or what infrastructure is relied on. Enterprise compliance and security teams are looking for solutions that support their objectives of ensuring the traditional A-I-C requirements for data protection.

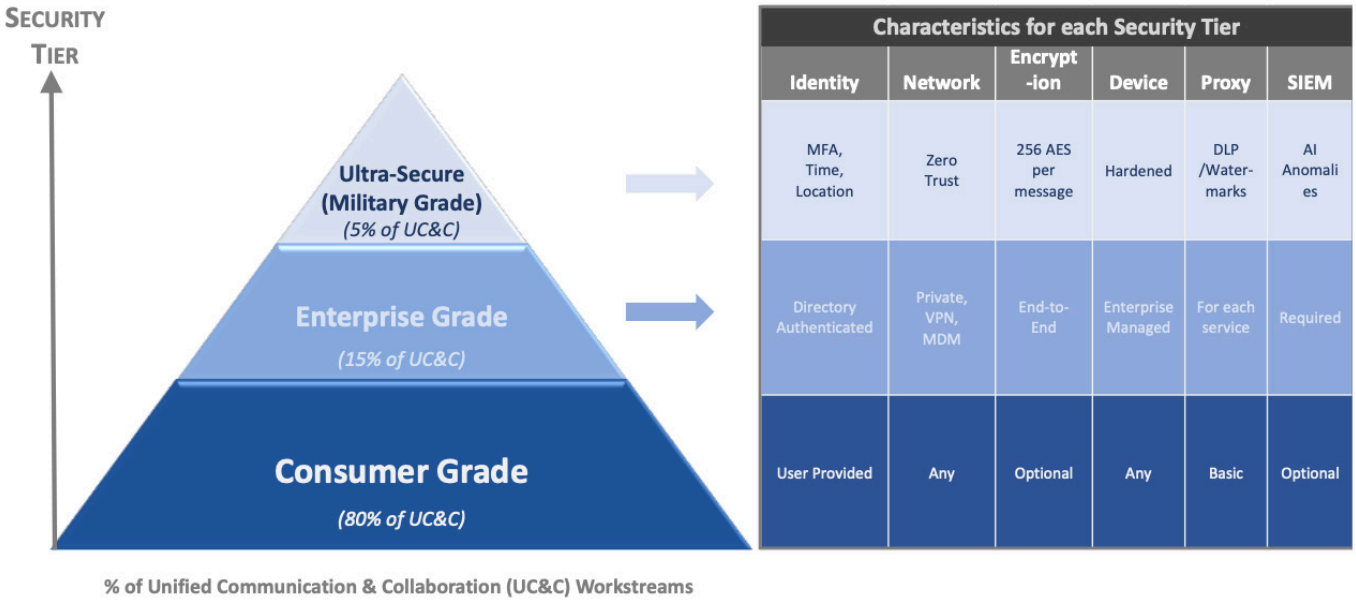
- **Availability:** Critical data is available to the right people at the right time in the right locations
- **Integrity:** Ensure that the data being shared among team members is trustworthy, accurate and not manipulated by any outside party.
- **Confidentiality:** Prevent sensitive and regulated data from being accessed by an unauthorized individual, whether a nation-state attacker, service provider, or malicious actor.

Tiers of Unified Communications Security

Many enterprises try to have a single collaboration platform. The challenge with this model is that enterprise grade security is not “good enough” for highly sensitive information or the level of compliance and privacy required. More and more enterprises and government institutions are adopting a multiple platform strategy to balance costs and ease of user experience with the appropriate level of security and compliance required for a team or group of employees and their associated external and frontline partners.

Research TechVision presented at Enterprise Connect in March of this year on Unified Communications & Collaboration (UC&C) Security recommended a tiered approach. Figure 1, below, shows a three-tiered UC security model with consumer, enterprise, and ultra-security grades. Advanced security is required for protecting intellectual property, for privileged company communications such as M&A deals, for compliance requirements and to ensure privacy.

TechVision Research did a survey of 20 large enterprises, and the results were that about 80% of enterprise UC&C interactions need consumer-grade security, 15% need enterprise-grade, and 5% require advanced security. To say this a different way, every large enterprise has use cases where Ultra-Secure communications is required, and the weighted average of these use cases across the 20 large enterprises came out to be 5%. In other words, 1 in 20 business workstreams should use Ultra-Secure or Military-Grade UC&C Tools.



Characteristics for each Security Tier					
Identity	Network	Encrypt -ion	Device	Proxy	SIEM
MFA, Time, Location	Zero Trust	256 AES per message	Hardened	DLP /Water-marks	AI Anomali es
Directory Authenticated	Private, VPN, MDM	End-to-End	Enterprise Managed	For each service	Required
User Provided	Any	Optional	Any	Basic	Optional

Figure 2: Tiers of Unified Communication & Collaboration (UC&C) Security

HighSide's E2EE Collaboration Platform Just Might be the Answer

The HighSide E2EE secure messaging and collaboration platform aims to solve the security and compliance problems that businesses face today. HighSide provides direct messaging, group chat channels, voice & video meetings, and file sharing with easy-to- configure policy and management controls that exceed the toughest A-I-C requirements.

- **Availability:** Application administrators can set policies which control access to data according to time and location-based restrictions. This patented capability helps with compliance and policy enforcement, only allowing data access WHEN and WHERE appropriate. Data deletion and retention policies can be set by administrators for compliance purposes.

- **Integrity:** All message content is controlled within a closed-loop system, with each message digitally signed, fully auditable and traceable and no reliance on usernames and passwords, eliminating the spoofing and phishing problems that email suffers from.
- **Confidentiality:** Every message is end-to-end encrypted, and the entire system is based on a zero-trust architecture. No data is ever exposed to back-end servers or to untrusted parties while in transit or at rest.

Leading HighSide E2EE Collaboration Use Cases

According to research publiched by TechVision Research, 1 in 20 workstreams are sensitive, requiring secure methods for sharing, storing and collaborating like end-to-end encryption (E2EE)

1. **Protecting Intellectual Property:** R&D team chats, files, and interactions are secured and controlled via strictly defined access rules including location such as R&D facility and manufacturing plant in foreign country
2. **Ensuring Privileged Company Communications:** CxO and Exec Management interactions regarding M&A deals, Investor relations, Sensitive HR comms, CxO status meetings
3. **Providing Ultra-Secure Communications:** In the event of a cyber-security breach or suspected attack, being able to communicate in a secure, out-of-band, trusted-circle or channel is critical so hackers cannot be part of your remediation actions
4. **Securing Sensitive Customer Service Interactions:** Some external customer and frontline communications need to be kept from going rogue under any circumstances due to potential brand and reputational damage implications
5. **The Best Compliance:** Manage GDPR cross-border PII data transfers without hassles, Comply with labor laws such as “right to be forgotten,” or “right to disconnect,” be able to offer CCPA protection to customers without skipping a beat, ability to provide compliance audits, HIPAA related communications, etc.

HIGHSIDE

Encryption Specifications

- Per-message 256-bit AES encryption
- User-to-user mutual authentication with 512-bit secp256k1 elliptic curve cryptography
- SHA256 hashing for message and authentication packet integrity

Zero Trust Architecture

- HighSide's servers are merely 'dumb switchboards' serving to connect two HighSide users without any insight into message content or files shared
- All encryption keys are maintained at the endpoints and while access to those keys is not available to admins, the usage of those keys can be controled by the company administrator
- All application traffic is end-to-end encrypted
- No unencrypted application data is ever exposed on HighSide's back-end servers

Time and Location Policy Enforcement (patented)

- Using a unique combination of on-device sensors, HighSide locks all data in the app based upon location and schedule restriction policies
- Time restrictions can be set to comply with labor law requirements, preventing off-the-clock compensation claims due to salaried employees contacting hourly employees after work hours
- The first enterprise collaboration application which complies with the new French Labor Code Article 55 or 'right to disconnect'
- Exceeds the requirements for US labor law compliance for preventing employee work- related communications outside of paid work hours for hourly employees
- Location restrictions can be configured to assure that data is only available either at specific company locations or within approved countries
- The first country-level location restriction policy for enterprise collaboration applications to facilitate endpoint data compliance with GDPR
- Permission and data access models are based on principles of need-based and least privileged access controls
- Exceeds even the most-stringent requirements of data portability laws such as ITAR / EAR, CCPA and HIPAA