CUSTOMER PROFILE

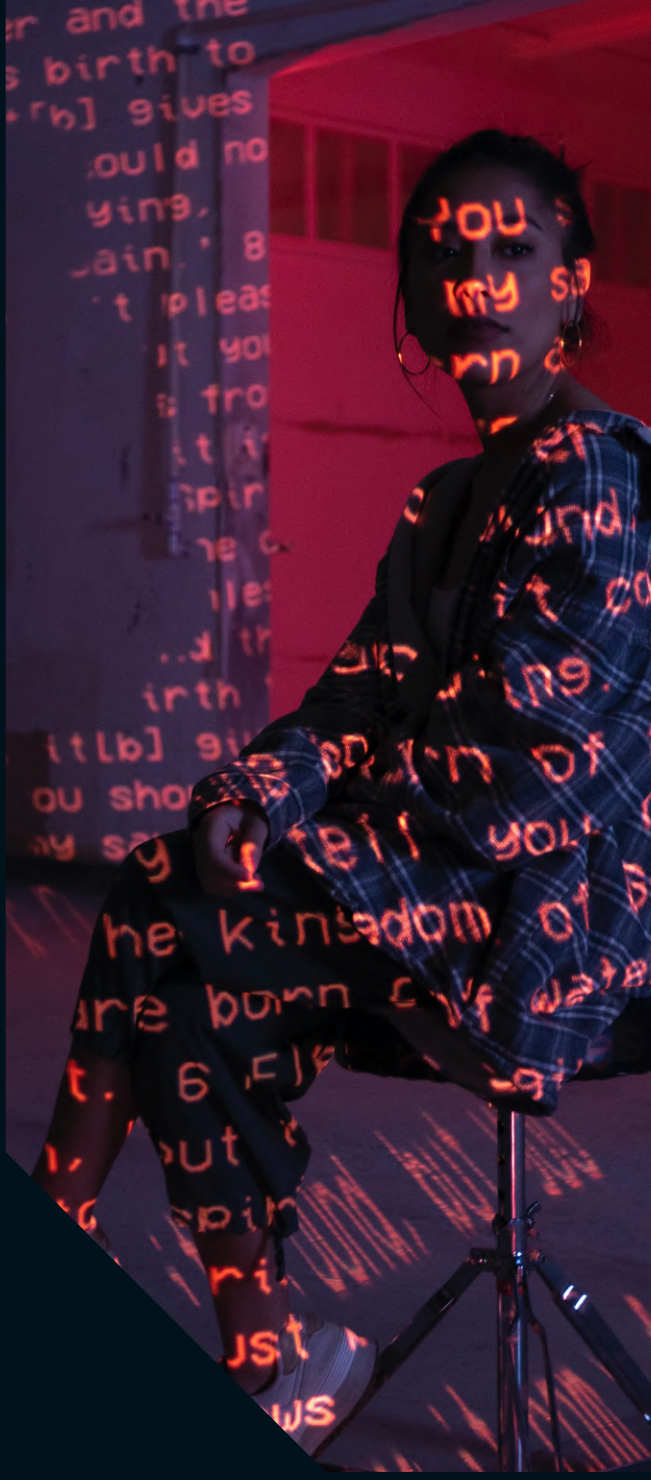
This case study is based on use of the HighSide platform by an early stage strategic and competitive intelligence firm. The company uses its deep expertise and business acumen with global markets and governments to offer customized research and analysis, industry and competitor insights, due diligence and deal support, political risk assessments, and litigation support.

The company prides itself on delivering world class open-source information and insights that lead to wins for their customers. They've helped c-suites improve understanding of foreign competitor activities and strategy; provided a steady stream of in-depth, open-source research and analysis to government agencies; and supported precedent-setting litigation in a case against one of China's top state-owned enterprises.

CUSTOMER CHALLENGES

Wise beyond its years, this young company understands the magnitude of cyber and other risks emanating from nation states like China and other actors. It's the heart of their business. Just as it seeks to inform and protect its customers from these risks, the company knows it must conduct business in the safest way possible without harming its own productivity. This includes the imperative of finding an easy-to-use communications and collaboration solution that offers protections typically only available to large, established corporations.

The scale and scope of the challenge is indeed global. Take, for example, a major network incident that occurred in the European Union in June 2019[2]. For a period of several hours, China Telecom used a series of network exploits to route millions of internet users' traffic through the China Telecom surveillance infrastructure, most likely to gain insight into EU and U.S. trade negotiations at a critical time in the U.S.-China trade war.



Any user of a system like Zoom, Teams, Slack or any other traditional enterprise-grade collaboration platform could have been subjected to significant data loss in an attack like this.

In addition, as significant portions of the Zoom platform are developed in China, many of Zoom's encryption keys are pre-compromised to allow Chinese surveillance teams to obtain access to Zoom teleconferences without users' consent or knowledge[3]. Zoom is not alone in the way that it compromised its systems to allow for Chinese surveillance anywhere in the world, even outside the borders of China and Hong Kong.

When Microsoft acquired Skype in 2008, it kept many of the backdoors in place which allowed international espionage teams access to nearly all information flowing through the system[4]. Microsoft has continued to rely on easily-defeated security technologies that can allow sophisticated adversaries to intercept and manipulate information flowing through their Office365 platform, including data shared through Teams. Other platforms such as GoToMeeting and Webex have security controls that can be compromised using open-source intercept tools and lack integrity when it comes to protecting sensitive data from nation state actors.

It is also important to note that any system providing participants an option to dial into a teleconference using the public telephone system has significant vulnerabilities. With the virtualization of the infrastructure which provides the phone numbers that participants can dial, attackers have focused on the Session Initiation Protocol (SIP) infrastructure underpinning those numbers[5]. Without any real potential for monitoring the integrity of the SIP numbers participants dial, any teleconference platform that has even one participant dialing in via telephone can be monitored by an unknowable amount of people.

HIGHSIDE'S SOLUTION

The company featured in this case study works to balance risks like these with the need for collaboration. It has tried different options but struggled to find a solution that gives the desired levels of confidence. They now use HighSide because it offers the highest level of security of any collaboration platform its executives have found available to global businesses.

Combining the power of HighSide's distributed identity and encryption platform with state-of-the-art voice and video delivery, the company is assured that only authorized individuals in authorized locations can join their teleconferences and working sessions. HighSide's compliance suite also provides the company a comprehensive log of every working session, where the participants were physically located during calls and visibility into all files shared among team members.

HighSide is the only teleconference solution with built-in adaptive authentication. Team administrators can quickly and easily restrict users to only connect to collaboration sessions from precise locations. In a remote work environment like the present, HighSide's location-based authorization tokens can be used to lock down certain sessions between locations as precise as an employee's home address. Location restrictions can also be used to block all users outside of authorized countries, significantly reducing the likelihood that sensitive conversations are accessed by attackers in cyber-crime-friendly jurisdictions in Asia or Eastern Europe.

Compared to traditional collaboration platforms like Zoom and Team, every HighSide voice and video session uses a unique set of identifiers. Zoom and Teams have static identifiers that allow attackers to listen in on calls, sometimes without knowledge of legitimate and authorized users. One case in point is what happened to UK Prime Minister Boris Johnson when he inadvertently disclosed his static Zoom identifier on social media[6]. HighSide will never be vulnerable to similar situations, because every conference between HighSide users has a randomly-generated session code that would take attackers over 2 years to guess.

HighSide's encryption is the best available to commercial, non-military users. It is so good that many international intelligence agencies and military forces rely on HighSide's platform for international secure communications. Using a combination of up to 9 different encryption keys for each session, every message and file shared through the HighSide platform has per-session and per-file integrity that can be proven throughout its journey through the internet. HighSide does not rely on the use of TLS or SSL for the delivery, generation or management of user and team keys. And, at no point is the HighSide system vulnerable to public SSL root attacks which can be used to intercept Zoom, Teams and other conferences. Compared with organizations like Zoom[7] and Microsoft[8], HighSide has never collaborated with authoritarian regimes in sharing encryption keys or user content.

That same encryption assures that only authorized individuals receive conference invitations, assuring closed-loop communications. If individuals outside of the organization need to attend a conference, a unique set of encryption keys can be generated for that user within a matter of seconds by simply sending them an email or SMS invitation. These same keys can be rapidly revoked after the conference to prevent those individuals from reconnecting to conferences in the future.

The HighSide system was designed from the ground-up to deliver integrity and confidentiality of all information flowing through it. At no point are encryption keys ever shared with HighSide's team or infrastructure, ensuring a true zero-trust capability.

Compared to other zero-trust messaging platforms like Signal, HighSide provides the unique capability to allow for the tracking and logging of all information that flows through the system. The HighSide Compliance Suite allows organizations to set data retention polices, archive all data sent through the system, and provide capabilities to respond to eDiscovery and other regulatory requests.

HighSide Voice and Video Features:

- **Mutual authentication for every user session**
- **Integration with Active Directory for internal user provisioning**
- **All conference session details and attendee information is captured in compliance logs**
- **Access can be granted in a matter of minutes and revoked immediately when users leave a session or project**
- **Location-based Multi-Factor Authentication (MFA)**
- **No single-point-of-failure for username or password theft, no capability for phishing users with malicious hyperlinks**
- **User identities are neither disclosed to HighSide servers nor advertised to other HighSide users outside of the organization**

RESULTS

With HighSide Voice and Video, the strategic intelligence firm featured here has improved the protection of their operations while giving users greater flexibility to communicate with each other, even in extreme times of social distancing and remote work from their choice of device.

By providing the HighSide platform to their users, the company has been able to sustain team productivity, continue delivering for its customers, and maintain the confidentiality and security of its information and communications. This also has prepared the company for long-term success and for any other global event it might confront.

1 Update to the IP Commission Report: http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

2 BGP event sends European mobile traffic through China Telecom for 2 hours: https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-through-china-telecom-for-2-hours/

3 Zoom's Encryption is "not suited for secrets" and has surprising links to China: https://theintercept.com/2020/04/03/zooms-encryption-is-not-suited-for-secrets-and-has-surprising-links-to-china-researchers-discover/

4 Skype can be intercepted by intelligence agencies: https://www.itnews.com.au/news/skype-can-be-intercepted-by-intelligence-agencies-report-336790

5 VoIP's Big Security Problem? It's SIP: https://www.pcmag.com/news/voips-big-security-problem-its-sip

6 Boris Johnson's Cabinet meeting could be HACKED as EU refuses to use video conferencing: https://www.express.co.uk/news/politics/1266226/Boris-Johnson-coronavirus-latest-cabinet-meetings-Dominic-raab-video-conferencing-zoom

7 Warning: Zoom Makes Encryption Keys In China (Sometimes): https://www.forbes.com/sites/thomasbrewster/2020/04/03/warning-zoom-sends-encryption-keys-to-china-sometimes/

8 Microsoft now reviewing Skype audio in 'secure' places (not China): https://nakedsecurity.sophos.com/2020/01/14/microsoft-now-reviewing-skype-audio-in-secure-places-not-china/