ZTEdge™
By Ericom Software

Instant Messenger Isolation

Protect Your Organization from Malware Delivery and Data Loss Enabled by Instant Messenger Encryption

Decrypt WhatsApp and Telegram messages to disarm malicious attachments and apply DLP to content to prevent sensitive data loss.

Instant messenger (IM) applications like WhatsApp and Telegram have been eagerly adopted by individuals worldwide as simple, user-friendly ways to communicate with almost everyone -- friends, family, business contacts, teachers, service providers. Strong websocket encryption reassures users that even sensitive communications will remain private. While leading IMs originated as cell phone apps, most now offer web clients, which many users find so convenient to use that they keep the IM permanently open in a browser tab on their laptop or desktop device.

Organizations have also adopted IM as an efficient channel for customer service and communication. IM power virtual assistants with valuable features such as automated messages, quick replies and chat labels that streamline 24/7 customer support. Customers appreciate the convenience of communicating with businesses and government offices on a familiar platform, much as they do with family and friends.

For organizations, however, the IM encryption that protects user privacy poses a serious threat to the devices on which IM web clients are used, the networks they connect to, and the organization as a whole. Secure web gateways, tasked with identifying malware in incoming web traffic, have no visibility into messages secured by websocket security. Weaponized IM attachments or SQL injected messages are thus the perfect way to deliver ransomware or other malware, along with innocent user conversations or customer IMs.

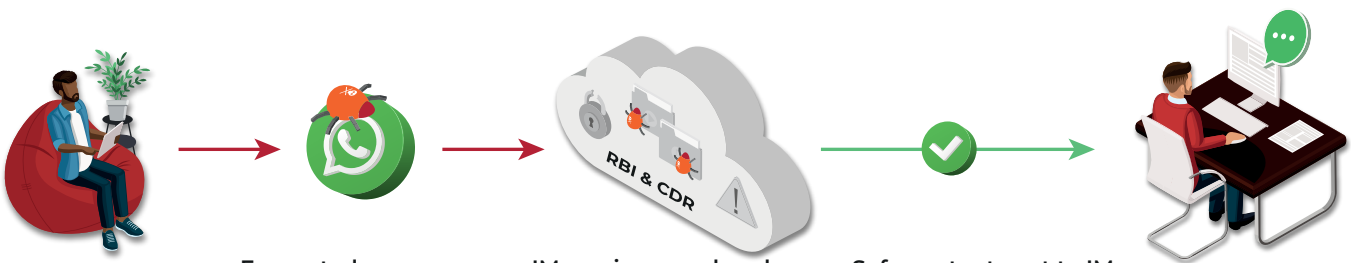
Instant messengers also represent a significant data loss threat. Once inserted in chat text or added as attachments, confidential files and data, like user credentials, are invisible to traditional data loss protection (DLP). While access to IM web clients can certainly be blocked, doing so would increase user frustration as well as reducing efficiency due to distracting use of phone-based IM apps.

The Solution: ZTEdge Instant Messenger Isolation

Block Malware from Reaching Endpoints

ZTEdge Instant Messenger Isolation protects organization endpoints and networks from malware, ransomware and exploits within instant messages, while enabling the IM access users view as essential.

All instant messages received on endpoint browsers are opened and unencrypted in isolated containers in the cloud, using remote browser isolation (RBI) technology. To protect your organization from malware hidden in files attached to IMs, ZTEdge Instant Messenger Isolation applies content disarm and reconstruct (CDR) to all attachments. Within the isolated container, files are downloaded, examined for malware and, if necessary, disarmed. The files are then reconstructed with (desired) native functionality intact and delivered to endpoints.



Encrypted message with malware

IM sessions rendered remotely; files scanned

Safe content sent to IM web client on user's device

ZTEdge™
By Ericom Software

Instant Messenger Isolation

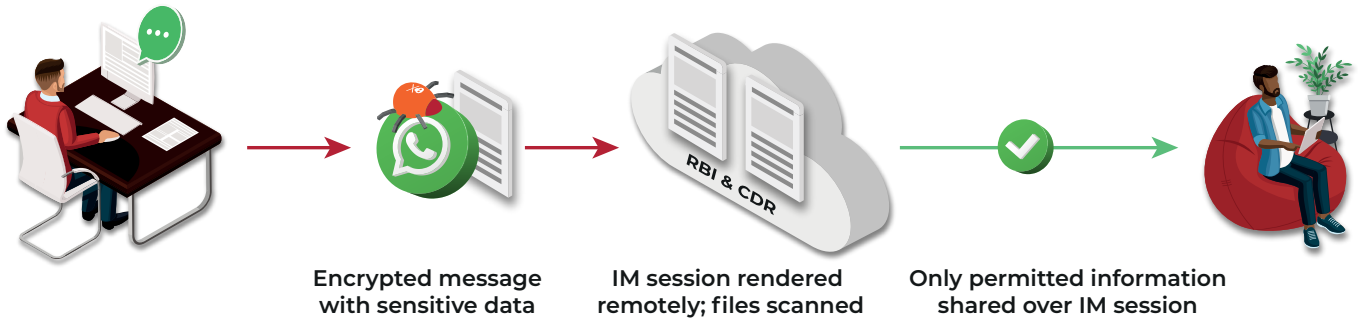
Prevent Data Loss via Encrypted IMs

ZTEdge Cloud Data Loss Prevention (DLP) applies granular controls, established by IT admins, that govern what data may be shared, how and by whom, as well as which data is protected. It protects organizations from IM-enabled malicious exfiltration of sensitive content, deliberate (but non-malicious) sharing, and accidental data loss.

All conversations on instant messenger web portals are routed via a virtual browser located in an isolated, cloud-based container, where they are decrypted and inspected. Text messages are scoured for dozens of types of sensitive personally identifiable information (PII), based on standard ID number, credit card account, passport number and bank account formats used in tens of countries worldwide. Admins can also create custom PII formats using regular expressions.

In the cloud-based container, policy-based controls are also applied to files that are sent via IM to determine whether data restrictions apply. Restricted files -- based on file type, location, user profiles and categories, or other factors -- are scrubbed from the message to prevent exfiltration and destroyed along with the container.

In both cases – PII text and restricted attachments -- if sensitive data is detected, it is removed before the message is sent and an alert is issued to the admin. Alerts may also be sent to the user, if desired.



ZTEdge Instant Messenger Isolation Highlights

- Secures IM communications, eliminating risk that malicious content will get in
- Leverages remote browser isolation (RBI) to prevent risky IM content from reaching endpoints and networks
- Removes malware embedded in weaponized files sent via IM
- Protects organizations from loss of restricted files via IM
- Blocks theft of employee and customer PII and credentials
- Reduces user frustration by eliminating need to block IM web clients

www.zerotrustedge.com

Americas:
T +1 (201)767-2210
E-mail: info@zerotrustedge.com

UK & Western Europe:
T +44 (0)1905 777970
E-mail: info@zerotrustedge.com

Worldwide:
T +972-2-591-1700
E-mail: info@zerotrustedge.com

Follow us