ZTEdge™
By Ericom Software

Instant Messenger Isolation

# Protect Your Organization from Malware in Encrypted Instant Messenger Content

Decrypt WhatsApp and Telegram messages and disarm malicious attached files before they reach your endpoints and networks.

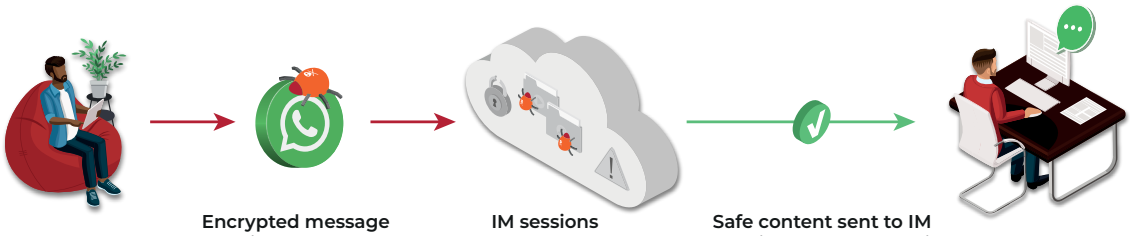
Instant messenger (IM) applications like WhatsApp and Telegram have been eagerly adopted by individuals worldwide as simple, user-friendly ways to communicate with almost everyone -- friends, family, business contacts, teachers, service providers. Strong websocket encryption reassures users that even 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.

Some organizations – enterprises, government agencies and not-for-profits – have integrated instant messenger APIs with their IT systems, allowing customers to, for instance, send insurance claim documents or other materials directly from their laptops or phones via IMs. Customers rely on IM applications' end-to-end encryption to ensure that documents they upload will be safe from hackers' eyes.

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.

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

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 sent privately to users or to organization accounts are opened and unencrypted in isolated containers in the cloud, using remote browser isolation (RBI) technology. Only safe rendering data is sent to users' regular browsers, on organization endpoints and networks, where they interact with it just as they would with directly-received IMs – only without the risk. All active web code, including any malware, remains in the isolated container and is destroyed along with it when the session ends.

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.

ZTEdge Instant Messenger Isolation also provides security to prevent data loss, with policy-based controls that restrict which content users can attach to outgoing IMs.



### ZTEdge Instant Messenger Isolation Highlights

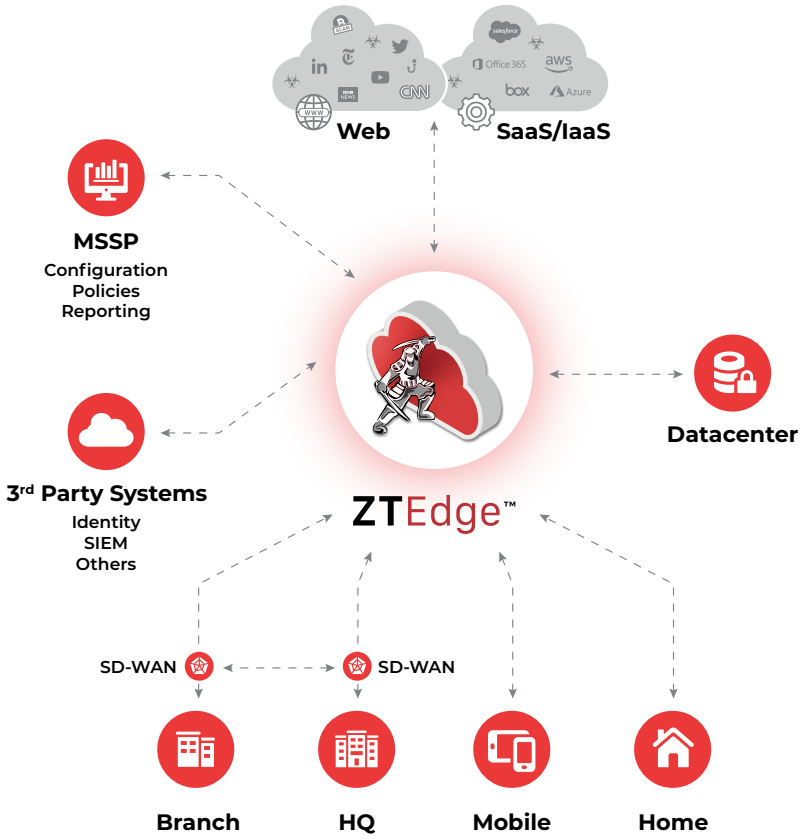
- Secures IM communications, eliminating risk that malicious content will get in
- Leverages remote browser isolation (RBI) to prevent risky IM content from reaching endpoints and networks
- Removes malware embedded in weaponized files sent via IM
- Protects organizations from data loss via IM
- Reduces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

ZTEdge™
By Ericom Software

Instant Messenger Isolation

# Zero Trust Security Capabilities for Organizations of All Sizes

ZTEdge is built to protect what matters for your small or mid-sized business – your users, data, applications and customers. The platform is flexible and evolves as your business grows and increasingly moves to the cloud. It is available directly or as a hassle-free service, managed by MSSPs.




> *ZTEdge offers a unique value proposition for organizations, delivering a comprehensive set of integrated Zero Trust security capabilities via a simple and affordable always-on cloud platform.*

Kamalika Sandell, Chief Information Officer at the New Jersey Institute of Technology

NJIT New Jersey Institute of Technology

## ZTEdge Capabilities

| Access Security | | Threat Prevention & Compliance | | |
|---|---|---|---|---|
| DNS Security | ZT CASB | Threat Intelligence Network | File Sanitization (CDR) | Cloud Data Loss Prevention (DLP) |
| Security Web Gateway | Identity & Access Mgmt. | Remote Browser Isolation | IDS/IPS | Zero Trust LAN Access |
| Cloud Firewall | Zero Trust Desktop | Anti-Virus | Ransomware Prevention | Network Traffic Analysis |
| ZT Network Access | SD-WAN | Anti-Phishing | SSL Inspection | Data Anonymization |


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