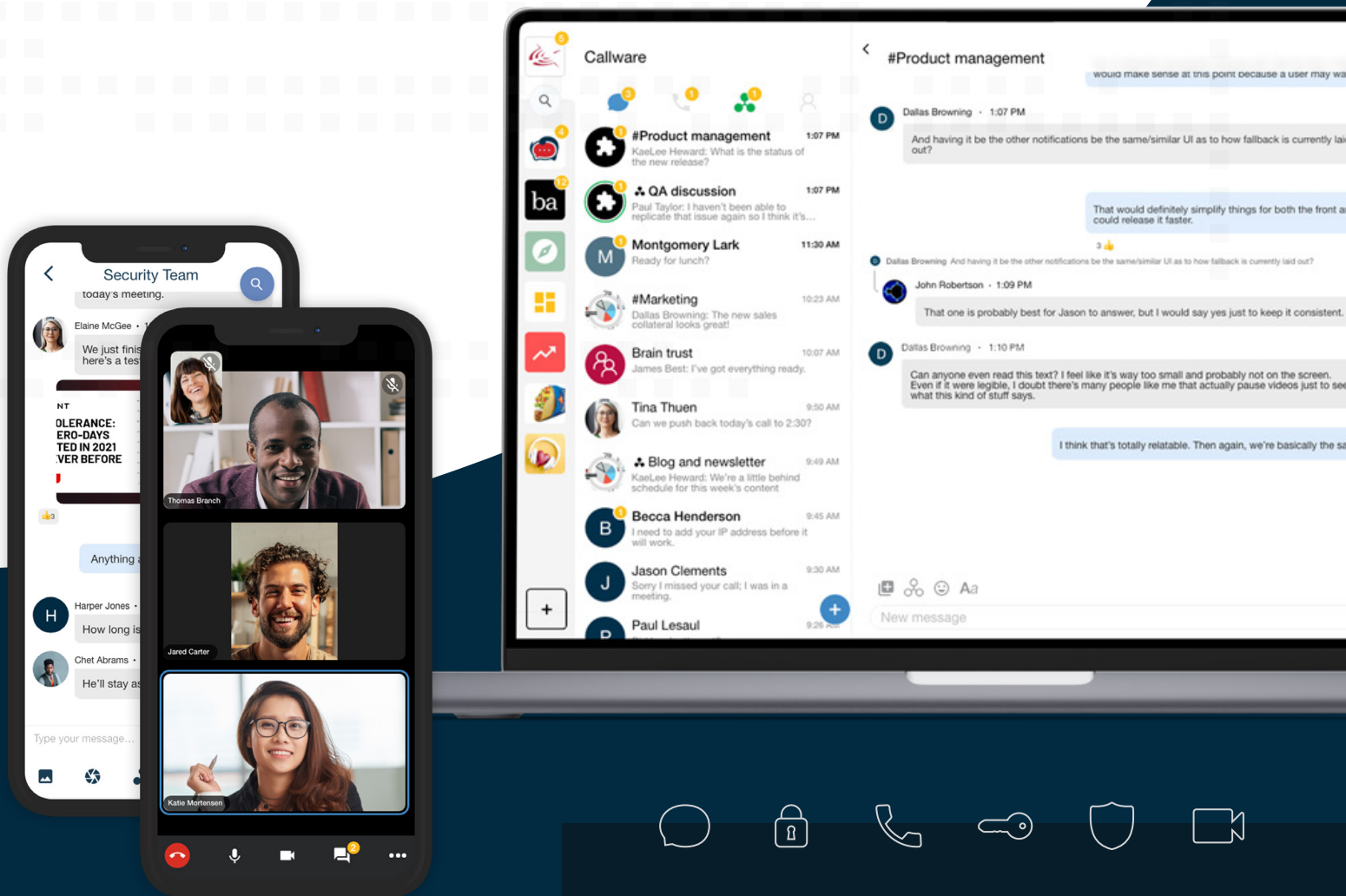


Advanced Remediation Protections Through Secure Communications



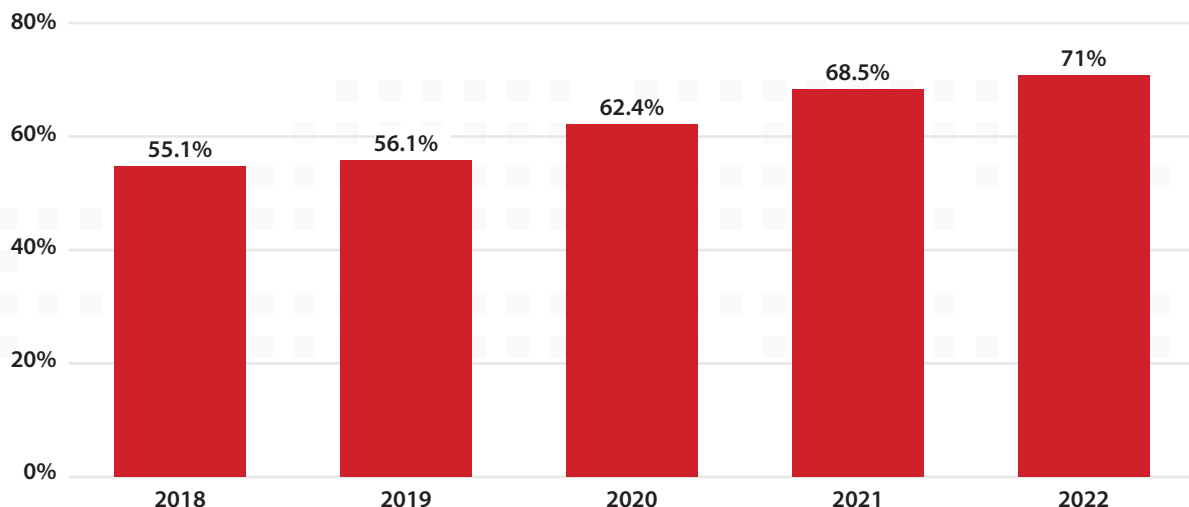
Lochbox is a cybersecurity communications solution that offers a novel defense against persistent threats during the vulnerable stages of remediation following a cyber attack and data breach.



WHEN, NOT IF

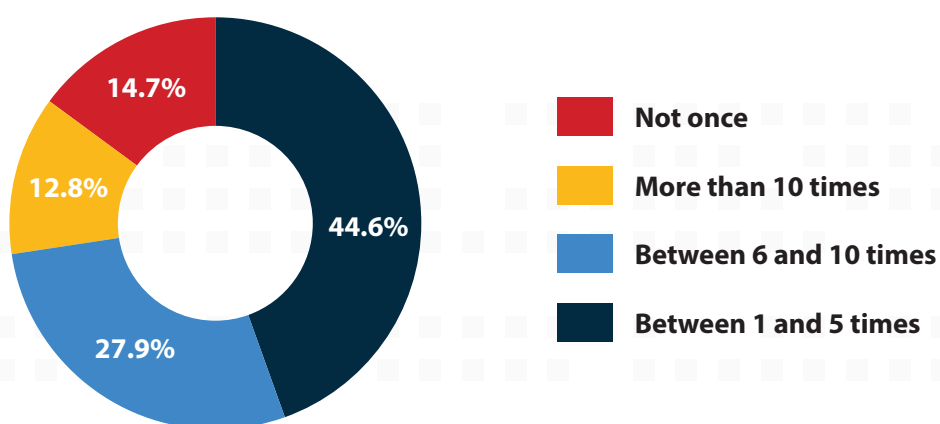
Ransomware attacks are constantly growing more sophisticated and organized which means your defenses against them have got to follow suit. In a survey of IT and security professionals, 71% responded that their organizations had been victimized by ransomware in the last 12 months. Those attacks help comprise the \$1.2 billion paid out by US companies for such attacks in 2021, a total that's almost triple the previous year.

Percentage of organizations victimized by ransomware attacks worldwide from 2018 to 2022



Despite your organization's best efforts, cyberattacks that may have once been deemed unlikely are now nearing inevitability. Defensive strategies can no longer only focus on preventing bad actors from gaining access but must also include a plan for when they do.

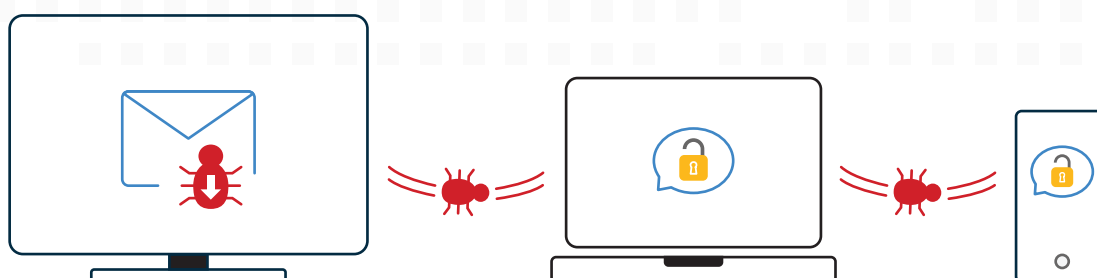
Frequency of successful cyberattacks in the last 12 months



AT YOUR WEAKEST

One of the most vulnerable times for a business is the latent period in operations immediately following the discovery of a cyber attack. A determined aggressor can use this time to gain an advantage over their victims to further inflict damages and enhance their efforts in getting everything they want.

Until remediation is complete, any communications over a compromised network may be subject to the eyes and ears of an attacker. Conversations regarding remediation efforts, business operations, and more are at risk of being used to the detriment of the targeted organization.



RESPONSIVE REMEDIATION

Successfully recovering from ransomware requires a rapid and coordinated effort that, depending on the severity of attack, may necessitate the involvement of legal counsel, insurance, public relations, and more. Each additional person that needs to be involved increases the risk for repeat attacks and makes the need for secure communications all the more critical. Only by securing all remediation related communications can you be sure your efforts will be effective and lasting.

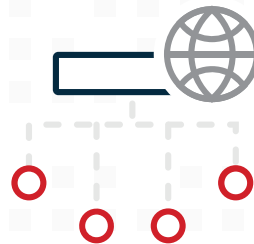
RECOVERING FROM RANSOMWARE REQUIRES A RAPID AND COORDINATED EFFORT

By adopting NIST standards for Zero Trust, Lochbox provides a maximum-security solution that is specialized for the safe exchange of the most sensitive information. More than just another messenger or meeting tool, Lochbox differentiates itself from competitors by designating each organization with the responsibility of independently managing its encryption keys external to our servers.

The use of an on-premise appliance or cloud server for encryption key storage empowers organizations with one of the greatest possible protections for their communications. Gaining the ability to have total control over who can access the app means an uninterrupted flow of communications for those explicitly authorized by organization administrators and no one else.

LOCHBOX FEATURES AND HIGHLIGHTS

- Exclusive control of your encryption
- 1:1 and group messaging
- Voice and video calls
- Unlimited meeting rooms
- Administrative controls
- User permissions
- Invite-only access
- Available on iOS, Android, and web



CLOSED NETWORK APP

Only those invited and approved by your organization's admin can view and participate in conversations.

ON-PREM SAFEGUARDS

An on-prem key server behind your firewall with optionally side-loaded mobile apps on burner devices provide maximum protection during incidences of cyber attack.

CONVENIENCE

Messaging, calling, and meetings for 1:1 and group conversations via the Lochbox mobile app or your favorite desktop browser.

PLAN TO COMMUNICATE SECURELY

A guide for how to respond to ransomware.

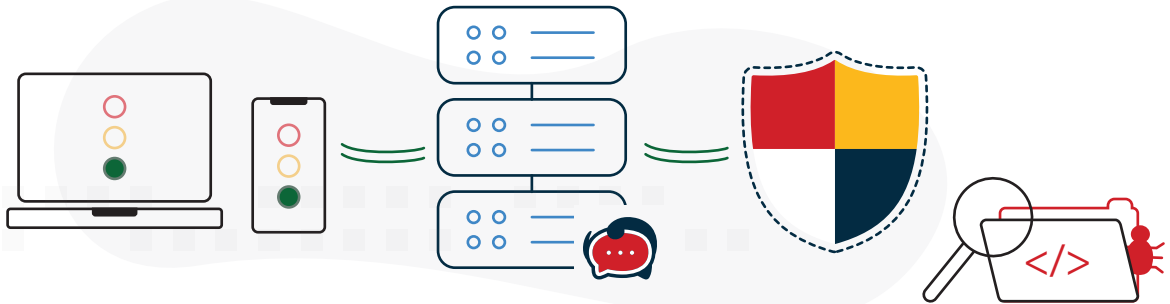
1 - DISCOVERY

Sensitive communications should cease on regular channels as soon as a security breach has been discovered. All existing networks should be considered as compromised until remediation is complete.



2 - DISPATCH

Consult with and appoint an incident response team (IRT) using a communication method unaffected by the attack. IRT should either A) be an established Lochbox partner or B) contact Lochbox for rush onboarding.

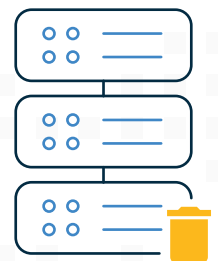


3 - DEPLOYMENT

The key server appliance is shipped and set up by IRT. All essential contacts pertaining to remediation (executives, security team, lawyers, insurance, etc.) are invited to join a dedicated channel within the app. Any conversations relevant to remediation are conducted via this channel (called an organization).

4A - DECOMMISSION

Victims can discontinue use of Lochbox and the key server appliance upon completion of remediation. All data on the appliance is destroyed and the appliance is returned to the distributor for refurbishment.



4B - ADOPTION


Alternatively, organizations can retain the key server appliance and continue to use Lochbox as part of an improved cybersecurity strategy.




Contact Us

 lochbox.app

 info@lochbox.app

 (801) 988-6800
(800) 225-5927

 8871 S Sandy Parkway, Suite 200
Sandy, UT 84070

