

Out-of-Band Comms

Secure Out-of-Band Communication for Cyber Incident Response

When Your Communications Break Down, Your Response Cannot

When identity takeover, business email compromise, destructive malware, ransomware, or a major non-cyber outage strikes, the tools teams normally use to coordinate may be unavailable, compromised, or impossible to trust.

That creates a second crisis inside the first: the response team loses a trusted way to communicate, align leadership, and keep decisions moving when time matters most.

Where trust breaks down

- Compromised or unavailable email
- Untrusted chat and collaboration tools
- Disrupted video conferencing
- Fragmented executive updates
- Scattered decisions and records

Out-of-Band Comms

Out-of-Band Comms gives incident response teams, their leaders, and their business partners a secure out-of-band communication environment inside the Rex Platform™. Instead of moving only the conversation, organizations can move the response – connecting email, chat, video & audio, executive visibility, workflows, ownership, and documentation in one governed incident environment.

- Out-of-band communication when primary systems may be compromised or unavailable
- Shared context across messaging, chat, video, and executive visibility
- Cross-functional coordination across security, IT, legal, privacy, communications, and leadership
- Privileged communication channels tied to response workflows, decisions, ownership and identity, and the system of record.

Out-of-Band Comms – it's not just backup chat.

Out-of-Band Comms At-a-Glance

Features

- **Mobile Command™**
Secure mobile executive visibility into live incident status, changes, and decision-ready context.
- **Mail**
Out-of-band email replacement for incident communications when the corporate inbox cannot be trusted.
- **Chat**
Out-of-band incident, leadership, and action chats that keep response conversations connected to each incident.
- **Meetings**
Secure video and audio conferencing for live, synchronous incident coordination outside the normal collaboration stack.
- **Scratch Pad**
An out-of-band, collaborative document workspace built directly into incidents and exercises.

Outcomes

- **Privileged Response**
Sensitive incident communications stay protected under legal privilege—separate from the systems and devices used for everyday work.
- **Cross-Functional Continuity**
Give internal teams and approved external stakeholders a trusted place to coordinate when primary systems are disrupted.

Privileged Communications By Design

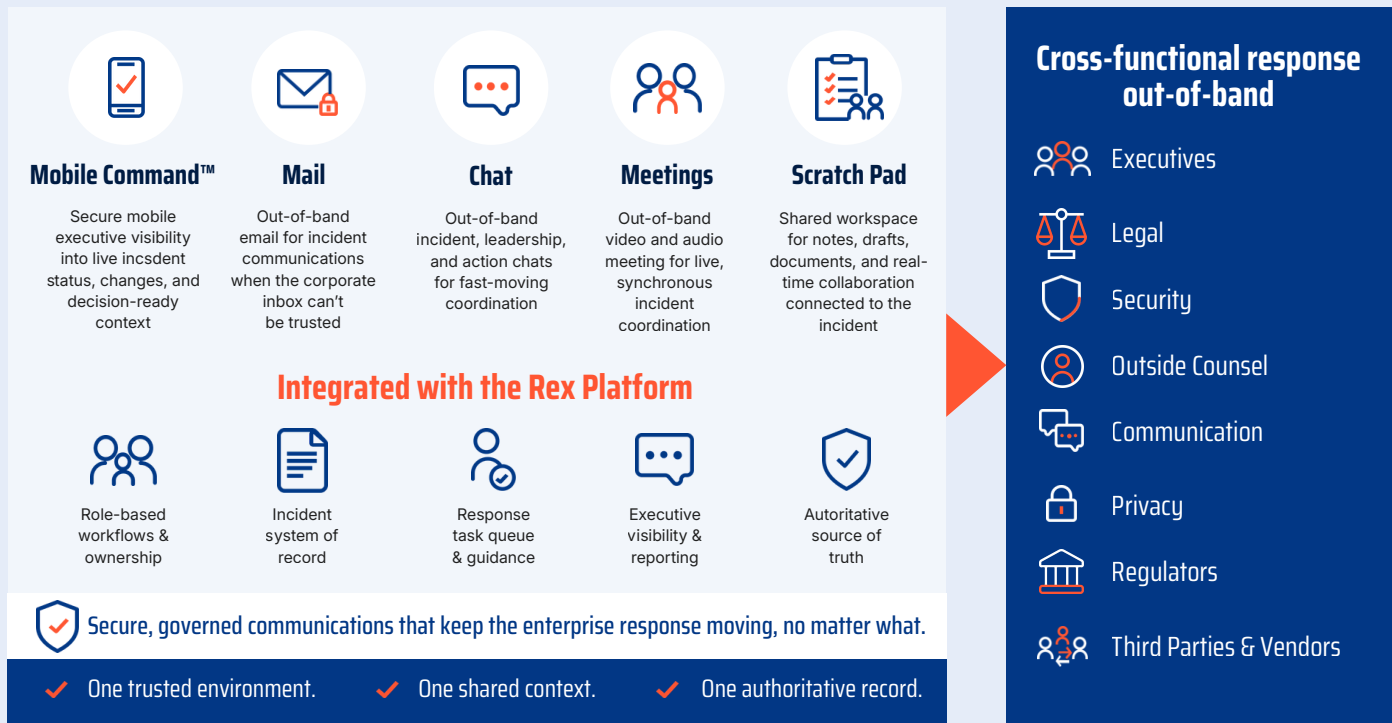
Out-of-band communication uses secure channels that operate independently of an organization's standard email, messaging, identity, and collaboration systems. They give incident responders a trusted place to continue operating when normal tools are unavailable, compromised, or untrustworthy.

But secure messaging alone is not enough. Enterprise incidents demand coordinated execution across security, IT, legal, privacy, communications, executives, outside counsel, crisis comms, and response vendors. The communications layer has to support the response – not become another disconnected side channel.

Out-of-Band Comms is connected to the governed Rex incident response environment so teams can keep communicating without losing response context, ownership, or the incident record.

Familiar interfaces. Mail, Chat, Meetings, Scratch Pad, and Mobile Command use familiar interaction patterns modeled on the everyday tools users already know, helping teams move out-of-band without learning a new way to work during an incident.

Enterprise identity integration. Integrations with leading identity providers such as Okta and Microsoft Entra ID let customers manage access to the BreachRx platform through their existing identity tools, so users can be added or removed quickly without a separate access-management process.



Mobile Command™

EXECUTIVE VISIBILITY & DECISION SUPPORT

Mobile Command extends secure incident visibility directly to executive leadership through a mobile-first experience built for live cyber response.

Leaders can stay current with incident status, what changed, and where attention may be required without being pulled into operational details. Response teams spend less time recreating status updates, while executive actions remain connected to the same governed incident context used by the broader team.

- **Decision-ready context.** Give leadership the information needed to act without exposing them to every operational detail.
- **Less reporting churn.** Keep executives informed without turning responders into a manual reporting desk.
- **Protected out-of-band access.** Give leaders a secure, trusted channel to incident status when primary corporate communications may be compromised or unavailable.



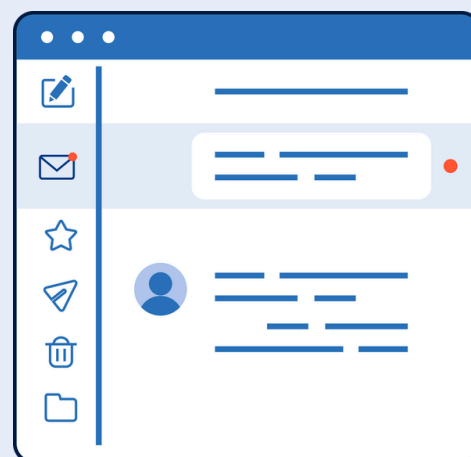
Mail

OUT-OF-BAND MESSAGING & EMAIL REPLACEMENT

BreachRx Mail provides an out-of-band alternative to corporate email when primary communications may be compromised, disrupted, or untrusted. It gives response teams a dedicated environment for critical correspondence without depending on affected email infrastructure.

Instead of shifting incident communications to personal accounts or improvised tools, teams can continue exchanging sensitive information through a purpose-built channel designed for crisis continuity.

- **Communication continuity.** Keep critical messages moving even when corporate email is unavailable or cannot be trusted.
- **Controlled participation.** Give internal responders and approved external stakeholders a protected place to exchange information.
- **Reduced fragmentation.** Keep important correspondence out of scattered personal accounts and temporary channels, making communications easier to manage and review.



Chat

INCIDENT, LEADERSHIP & ACTION CHATS

BreachRx Chat gives response teams dedicated out-of-band chat for the conversations that drive an incident forward – from operational coordination to leadership alignment and action-focused discussions.

Purpose-built incident chats help teams separate conversations by audience and response need while keeping them tied to the active incident environment. Instead of scattering coordination across corporate chat, text threads, and dozens of temporary channels, teams can keep fast-moving collaboration aligned to the same response context.

- **Purpose-specific coordination.** Support incident, leadership, and action conversations while purposely protecting legal privilege.
- **Cross-functional alignment.** Keep security, IT, legal, privacy, communications, leadership, and approved partners connected.
- **Governed collaboration.** Reduce fragmented coordination activities outside the response environment.



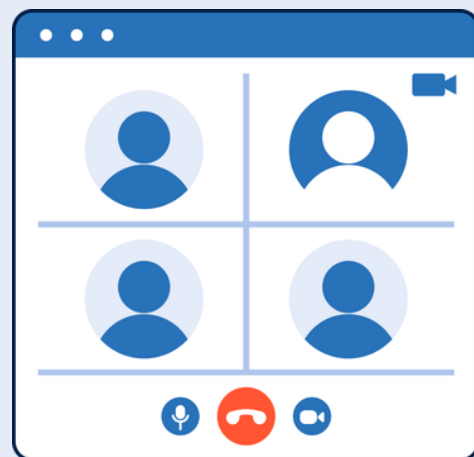
Meetings

OUT-OF-BAND VIDEO CONFERENCING

BreachRx Meetings provides out-of-band video conferencing for the live, synchronous coordination that high-severity incidents demand when the normal meeting stack may be unavailable or untrusted.

Incident commanders, cross-functional stakeholders, leadership, counsel, and response partners can continue real-time crisis coordination outside the affected collaboration environment. Bridge gives teams a trusted place for live discussion while the broader response remains managed in Rex.

- **Out-of-band crisis coordination.** Keep high-urgency discussions moving without depending on the normal conferencing stack.
- **Privileged meetings.** Flag sensitive meetings as privileged to help protect associated recordings and meeting artifacts as part of the privileged response.
- **Recording and transcription.** Capture critical discussions and create transcripts that preserve important context, decisions, and next steps from the live response.



Scratch Pad

REAL-TIME INCIDENT RESPONSE COLLABORATION

BreachRx Scratch Pad gives response teams a protected, collaborative document workspace built directly into incidents and exercises in the Rex Platform.

Teams can capture findings, hypotheses, handoffs, decisions, remediation details, and draft communications together in real time instead of scattering notes across standalone docs and chat. Multiple contributors can edit at once, use images, and video, and bring teammates in with mentions and comments while Rex AI Maestro helps connect the work back to structured workflows.

- **Shared source of truth.** Keep findings, decisions, tasks, and drafts in one central place tied to the active incident.
- **Real-time collaboration.** Write together, see changes live, use mentions and comments, and stop chasing the latest version.
- **Protected incident context.** Keep sensitive collaboration inside the incident with support for legal privilege protections and the governed Rex response environment.



Integrated with the Rex Platform

Out-of-Band Comms is part of the broader Rex Platform – the agentic AI-powered CIRM environment used to orchestrate cyber incidents across security, legal, privacy, communications, IT, and leadership.

Unlike a standalone backup chat or conferencing tool, BreachRx Out-of-Band Comms keeps communication connected to the response itself. Teams can coordinate actions, manage obligations, capture critical decisions, involve approved external stakeholders, and maintain a trusted record of what happened, who acted, and why.



Don't just move the conversation out-of-band. Move the entire response.

Key Capabilities

Out-of-Band Communication & Continuity

Capability	Description	Business Value
Mail	Secure messaging and email-replacement channel for incident communications outside the corporate inbox.	Keeps message-based coordination moving when email is unavailable or untrusted.
Chat	Secure incident, leadership, and action chats connected to the active response.	Reduces fragmented side channels and keeps conversations aligned with incident efforts.
Meetings	Secure video conferencing for synchronous incident coordination.	Maintains live coordination without depending on the normal meeting stack.
Scratch Pad	Protected collaborative document workspace for real-time notes, findings, decisions, and drafts tied to the active incident.	Keeps collaboration in one governed source of truth while reducing scattered documents and version confusion.
Mobile Command™	Secure mobile view into live incident status, changes, and decision-ready context.	Keeps leadership informed without constant manual status reporting
Familiar Interfaces	Mail, Chat, Meetings, Scratch Pad, and Mobile Command use familiar interaction patterns modeled on the standard tools users already know.	Reduces training and helps teams shift to out-of-band operations quickly during an incident.
Identity Provider (IdP) Integrations	Integrates with leading IdPs such as Okta and Microsoft Entra ID so customers can manage BreachRx access through existing enterprise identity tools.	Lets administrators add or remove users quickly while keeping access management centralized.

Legally Privileged Communications

Capability	Description	Business Value
Privileged Workstreams	Separates sensitive legal discussions from routine incident communications while keeping them connected to the active response.	Helps preserve privilege and sensitive legal analysis without sacrificing response context or coordination.
Controlled Counsel Access	Role-based access brings outside counsel and approved external parties into protected incident workstreams.	Enables faster legal collaboration while limiting exposure and maintaining clear privilege boundaries.
Defensible Incident Record	Facts, decisions, ownership, and supporting evidence remain connected to the governed Rex system of record.	Supports accountability and a more defensible response under executive, regulatory, and legal scrutiny.



SOC 2 Type II

About Us

BreachRx's Rex Platform uses agentic AI to orchestrate enterprise-wide incident response, enabling organizations to manage high-volume attacks, reduce chaos, and make fast, coordinated, defensible decisions across teams.

Contact Us

info@breachrx.com

linkedin.com/company/breachrx

breachrx.com