SOLUTIONS BRIEF

Mission-Critical Security and Compliance-Ready Collaboration

Mattermost
MISSION IN MOTION

The High-Stakes Reality of Mission-Critical Disruptions

Incidents—whether cyberattacks, system failures, compliance-driven disruptions, or infrastructure outages—can occur at any moment, threatening operations and business continuity. When a breach occurs, every second matters. Yet, traditional collaboration tools like Microsoft Teams and Slack are built for general business communication—not mission-critical security workflows. These tools lack the granular security controls, isolation capabilities, and compliance readiness needed to manage high-stakes incidents effectively. Organizations relying solely on these platforms risk prolonged downtime, data exposure, and compliance violations. Radware's 2025 Global Threat Analysis Report reveals a staggering increase in web DDoS attacks, soaring by 550% in 2024, largely driven by geopolitical tensions and the rise of AI technologies.

Without a dedicated, secure communication platform, response teams—whether in cybersecurity, IT operations, or critical infrastructure—struggle to coordinate effectively, delaying resolution and increasing risk. Mattermost ensures continuous, protected communication during an incident, keeping defenders connected and operational no matter the circumstances.

A global media company relies on internal tooling for essential IT communications, but **during a Sev0 outage, bringing critical operations to a halt and costing an estimated $100,000 per minute.** To ensure that critical operations aren't disrupted by future outages, the organization has implemented Mattermost as their backup communication system.

Mattermost provides the team of 15,000 developers at the organization with a **secure, self-hosted collaboration environment to ensure that they can respond to and resolve incidents quickly and effectively.**

The Mattermost Advantage:

Control, Security, and Resilience

Mattermost eliminates communication gaps that slow incident response, giving security, IT, and operations teams complete control over critical situations. It provides a secure, resilient, and compliant environment for coordination when it matters most.

- Reliable Connectivity: When primary systems are compromised, Mattermost keeps security teams connected through dedicated, isolated communication channels.
- Pre-Built Playbooks & Automation: Streamline incident response with structured workflows, reducing human error and improving response efficiency.
- Self-Hosted & Compliance-Driven: Maintain full data ownership while ensuring compliance with FedRAMP, HIPAA, GDPR, NERC CIP, and other security frameworks and standards.
- Seamless Tool Integration: Connect with existing security stacks, SIEMs, and orchestration platforms for an optimized incident response process.

Trusted by Industry Leaders:

Mattermost is the Secure Choice for Critical Operations

When cyber threats escalate, your communication shouldn't be a liability**.** Mattermost gives you the control, security, and resilience needed to act fast, mitigate threats, and stay compliant.

- Prevent Lateral Movement: Isolate defenders from breached assets to contain threats and mitigate damage.
- Real-Time, Secure Coordination: Keep teams operational with end-to-end encrypted, fully auditable communication that withstands any disruption.
- Data Sovereignty & Deployment Flexibility: Choose self-hosted, private cloud, or air-gapped deployments for maximum control over sensitive data.
- Purpose-Built for High-Security Environments: Trusted by Fortune 500 enterprises, global financial institutions, and defense organizations for their most critical communication needs.

Organizations operating in high-stakes environments require a solution that ensures business continuity, security, and compliance—especially when traditional collaboration tools fail. Mattermost excels in two critical areas: Out-of-Band Incident Response and Secure Collaboration for Regulated Industries. Whether responding to cyber threats or ensuring compliance-driven communication, Mattermost delivers the control, security, and resilience required for mission-critical operations.

Use Case 1: Out-of-Band Incident Response

When cyberattacks, IT failures, or infrastructure outages take down primary communication systems, organizations need a secure, resilient way to coordinate a rapid response. Traditional collaboration tools can become attack vectors, exposing security teams to lateral movement risks and limiting their ability to contain and respond to incidents in real-time.

Why Mattermost Leads in Secure Incident Response

- Isolated, Secure Communication: Dedicated out-of-band (OOB) channels keep defenders separate from breached assets, preventing lateral movement and ensuring response coordination remains uncompromised. Mattermost also supports real-time audio and screensharing, enabling faster decision-making and collaboration during incidents.
- Structured, Playbook-Driven Incident Management: Pre-built workflows and Mattermost Boards help teams track tasks, assign responsibilities, and standardize IR protocols, reducing errors and accelerating resolution. Task tracking ensures all response steps are documented and auditable for compliance.
- Deployment Flexibility: Deploy on-premises, private cloud, dedicated SaaS, or air-gapped environments for uncompromised data control and security, tailored to enterprise compliance requirements.
- Proven Response Acceleration: Customers have seen up to 90% faster incident response, cutting resolution times from 20 minutes to just 2 minutes.

“Mattermost is our sole Out-of-Band communication platform for threat hunting and cyber response.”

– Associate Director, Threat Response Operations,
Fortune 100 Insurance Company

Use Case 2: Secure Collaboration in Regulated Industries

Regulated industries such as finance, healthcare, defense, and critical infrastructure face heightened security risks and strict compliance mandates. Traditional cloud-based collaboration tools introduce compliance gaps, data sovereignty risks, and security vulnerabilities.

Why Mattermost Leads in Secure Collaboration

- Self-Hosted & Compliance-Driven: Enforce compliance with FedRAMP, HIPAA, GDPR, CMMC, NERC CIP, and other security frameworks and standards. Mattermost ensures audit logs, granular access controls, and end-to-end encryption to protect sensitive data. Organizations can easily manage compliance audits with automated reporting and traceable activity logs.
- End-to-End Security & Access Control: Enterprise-grade encryption, role-based permissions, and automated audit logs prevent insider threats and unauthorized data exposure.
- Seamless External Collaboration: Securely communicate with vendors, contractors, and partners while preventing shadow IT and compliance violations.
- Reliability for Mission-Critical Operations: Designed to support 24/7 availability, disaster recovery, and operational resilience.

"If you value your data and privacy and aim for high reliability and general ease of use, then self-hosted Mattermost is by far the best option out there."

– Head of IT, *National Telecomm Infrastructure Provider*

Seamless Integration for Security & Compliance

Mattermost integrates seamlessly with SIEMs, ITSM systems (e.g., ServiceNow, Splunk), identity providers (SSO/MFA), workflow automation tools, and IR platforms to enhance security monitoring, enforce role-based access, and enable automated compliance reporting for audits. Real-time alerts and automated workflow integrations ensure faster threat response, continuous system oversight, and seamless handoffs between security and compliance teams.

When security, compliance, and operational resilience are non-negotiable, Mattermost is the **proven solution for secure, compliant incident response and enterprise collaboration**—ensuring teams stay connected and in control.

Discover how Mattermost can empower your mission

Schedule a Demo

Mattermost
MISSION IN MOTION