Clearedin

SOLUTION BRIEF

A Smarter Way for Email Security + Cloud Collaboration Compliance

"Clearedin's solution has consistently, dramatically reduced our risk and amount of time we've spent on phishing defense."

Christine Ray
CISO at Unqork

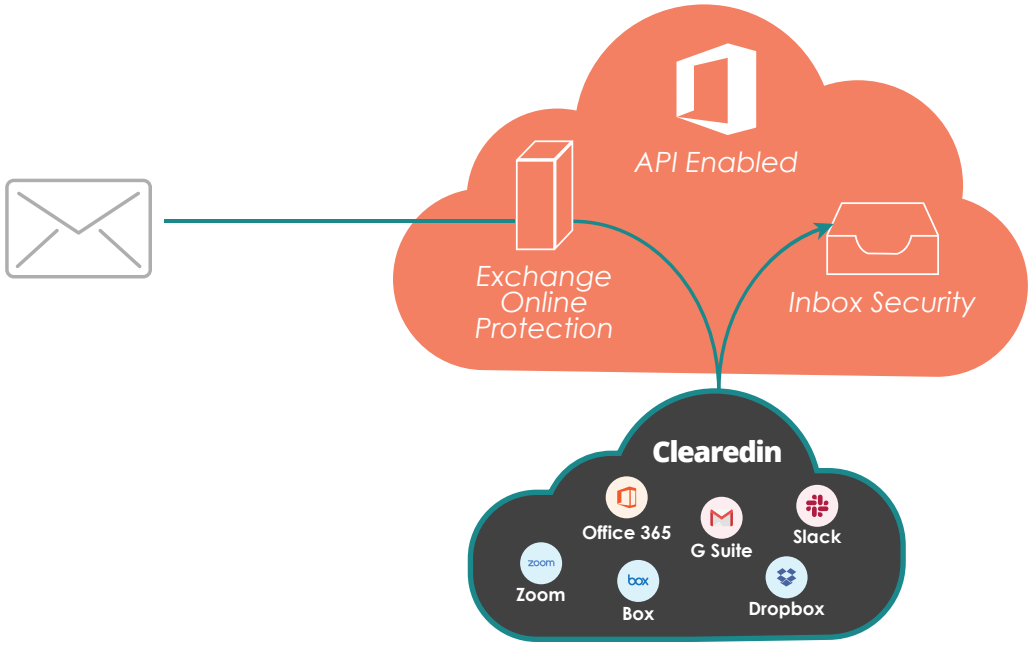
unqork

Protection for All Targeted Cloud Collaboration and Email Attacks

During any business day, the average worker connects more than 100 times with colleagues, customers, and business partners over digital communication collaboration and email channels. This pattern repeats itself across millions of business workers worldwide. Armed with malicious exploits to gain unique personal information, hackers aggressively try to phish bits of personal data through these channels to steal bank accounts, business partner data, personal identity, or anything else of value.

First generation phishing defenses helped reduce email-based information theft. But today, valuable privileged business digital channels expose a large compliance hole often overlooked by the CISO and IT staff. Personal and corporate chat, video and file share unknowingly expose confidential information to malicious exploits, bad actors, and social engineering through accidental employee actions. The growing volume (numbering in the billions per year) of collaboration messages for chat, video and file sharing vastly exceeds email. Phishing exploits are far beyond the current corporate focus on Email Security. Hackers easily trick users to share sensitive information on collaboration channels. Malicious exploits capitalize on this collaboration shift beyond email and are adapting their illicit phishing activities.

Businesses and their auditors find it increasingly difficult to maintain compliance across these collaboration channels and meet strict industry standards. Compliance standards are evolving to ask the critical questions around all channels that hold Personal Identifiable information (PII) as paramount. This is true in multiple verticals including healthcare, financial services, government, or energy services. Failure to meet these compliance baselines is increasingly common due to collaboration and email phishing, resulting in lost business and costly fines. Business partner reputation is also at risk, any company located throughout the world doing business in Europe places the CFO wholly responsible for ensuring secure data according to GDPR.



Achieve Industry-Specific Compliance Across Enterprise Cloud Applications and Email

The popularity of chat, video, and file collaboration suites (all alongside email channels) is a time saver and productivity boost for many businesses. Pairing positive gains with compliance requirements is essential. Clearedin offers customers a server-side phishing solution with an API-based approach that is deployed in minutes. This active defense helps customers in nearly every industry establish a customizable anti-phishing solution to automate compliance in FINRA, SEC, Bank Secrecy Act, GLBA, FERC, DOE, California Consumer Privacy Act (CCPA), FDA, HIPAA, GDPR and NIST. Automating, documenting, and achieving business protection across these industries for multiple digital collaboration channels is difficult but not impossible.

Here are a few examples:

- **FINRA, SEC, Bank Secrecy Act, and GLBA**
  Phishing attacks easily move laterally across cloud-connected collaboration apps and email. Clearedin automates whitelists and blacklists to help achieve FINRA or SEC compliance, isolate valuable PII, and prevent dangerous access to the corporate staff, operations, partners, and suppliers, regardless of location or device.
- **FERC, DOE, California Consumer Privacy Act (CCPA) and NIST**
  For Federal agencies requiring NIST or FERC compliance, Clearedin proactively manages and documents risk assessment, awareness and training, data security, anomalies and events, security-continuous monitoring, detection processes, analysis and mitigation.
- **FDA and HIPAA**
  Business partners and patients alike need to avoid Business Email Compromise (BEC) and falsified account takeovers (ATO). They must deliver enforceable templates to minimize compromise. Clearedin helps customers follow U.S. Department of Health and Human Services cybersecurity preparedness guidelines for HIPAA. This includes protecting clinicians from collaboration messaging and email attacks while keeping patient data safe.

Proactive Security Compliance for financial services, healthcare, government, and energy or utilities requires automation, AI, and machine learning innovation.

Cloud Email and Collaboration Compliance means that phishing must be blocked across the four most popular cloud collaboration applications: chat (slack), video (zoom), file share (box) applications and email (office 365).

Clearedin provides compliance with Trust Graph and Trust Profiles to automate the benefits of pattern recognition across enterprise workflows.

Why Clearedin?

Clearedin's patented Trust Graph technology offers a unique anti-phishing approach using machine learning (ML). ML rapidly compiles a unique fingerprint of each organization's typical communication and collaboration patterns.

Every collaboration message and email adds valuable human intelligence to the Trust Graph. Combined with the Clearedin platform, customers gain nearly limitless artificial intelligence (AI) insight for every employee communication across chat, video, file sharing or email, along with other professional B2B digital collaboration channels. Clearedin Trustgraph applies this AI to whitelists and blacklists to avoid previously manual knowledge gaps and eliminate social engineering and intimidation techniques common in phishing attacks. This approach simplifies and streamlines compliance requirements. Server-based Trust Profiles quickly grow for each sender without manually scanning private documents, email, and other communications. Trust Profiles grow more powerful with every communications interaction. Our AI applies ML and other techniques to solve modern-day phishing attack surfaces at work including ingestion of crucial trust factors such as the updated reputation scores of senders and collaborators.

Third-party compliance experts including Accenture recommend clients consider AI and deep-learning applications in natural-language processing essential. Clearedin agrees: *our approach helps companies manipulate algorithms that determine sentiment, gather intelligence, or filter for spam and phishing.* The recent surge in remote workers scales this approach to automatically block phishing-based attachments that install parasites and illegally siphon personal data, logins, and passwords.

AI and ML Deliver Highest Trust Collaboration Scores

Analyst firms including Gartner state that Zero-trust networks "create an identity- and context-based, logical-access boundary encompassing a user and an application or set of applications." Clearedin applies zero-trust security across multiple collaboration digital channels from video, voice, email, and chat. Clearedin's TrustGraph assumes no implicit trust is granted to assets or user accounts based on physical or network location, or asset ownership.

Authentication and authorization (both subject and device) are discrete functions performed before session permissions are granted to an enterprise resource. Through AI and ML, our solution helps customers achieve adaptive Zero-trust compliance by learning to always deliver a higher collaboration trust score across all users and digital channels.

INDUSTRY HIGHLIGHT

Purplesec, a cybersecurity firm specializing in offensive and defensive strategies, reported that 98 percent of cyberattacks rely on social engineering. Collaboration applications are especially vulnerable, since gaining access to one application often exposes the entire suite—and all the workers who use it—to malicious exploits. Clearedin eliminates social engineering gaps between voice, video, and collaboration applications.

www.purplesec.us

Learn more about Clearedin, Compliance, Zero-Trust Security and automating anti-phishing with no SoC overhead. Visit us at *www.clearedin.com* today.

Clearedin

Clearedin learns the unique cadences and rhythms of how your organization communicates and collaborates and uses that knowledge to engage and educate your employees while keeping them safe. Clearedin customers span cloud-native start-ups Global 2000 enterprises, and government agencies. Contact us at info@clearedin.com.