TECHOIL
YOUR TRUSTED PARTNER EMPOWERING WITH AI

IF YOUR EMAIL GOES DOWN, YOUR PLANT GOES DOWN.

When email fails, the plant can’t keep running. Can you afford an operational interruption lasting hours or days?

THREATS ARE EVOLVING

Ransomware and extortion appear in a significant share of breaches and cause critical downtime. The cost per incident and the loss of IP (drawings, drilling data) can easily exceed any preventive investment. In addition, recent reports show that ransomware/extortion appears in 32% of breaches, and BEC losses are measured in the billions.

THE SEVERE RISKS OF UNSECURE EMAIL

83% OF BREACHES
INVOLVE EMAIL

48% OF THREATS
COME FROM PHISHING ATTACKS

91% OF ATTACKS START WITH
A PHISHING EMAIL

71% OF TARGETED ATTACKS
INFECT OT ENVIRONMENTS

Without robust security, your company is exposed to potentially devastating cyberattacks. Phishing, spear phising, and Business Email Compromise (BEC) can lead to operational disruptions, safety risks and more. And one click is enough: Under 60 seconds to take the bait; 68% of breaches involve people.

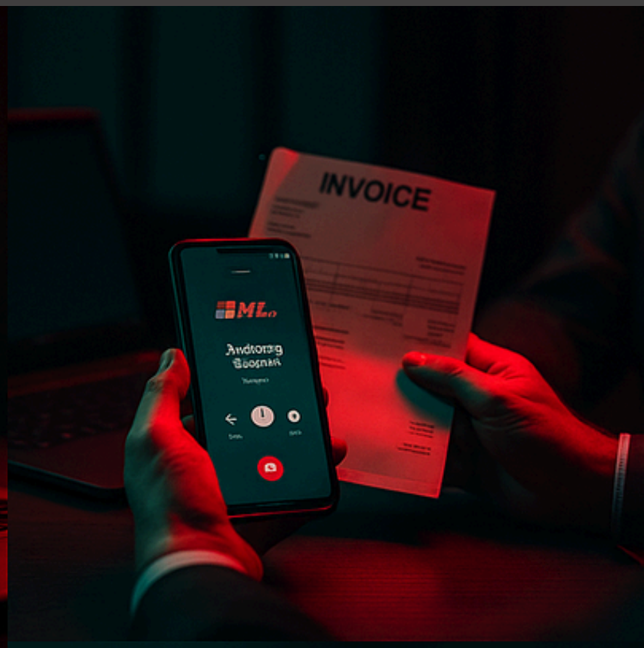
Unsecure email can lead to massive financial loss.

$4.4 MILLION IS THE AVERAGE
DATA BREACH COST

$2.8 BILLION IN LOSSES TO BEC
SCAMS IN 2023

TECHOIL
YOUR TRUSTED PARTNER EMPOWERING WITH AI

THE MOST DANGEROUS CYBERATTACKS AGAINST YOUR CORPORATE EMAIL



Phishing / spear-phishing
Look-alike emails from Microsoft, partners, or logistics that harvest credentials or drop malware.
Risk: Account compromise, theft of IP (field data, drawings), and spread into critical systems.

BEC (executive/vendor impersonation)
Convincing payment-change requests or urgent wire instructions.
Risk: Seven-figure, irreversible transfers tied to your real vendor flows.

Ransomware via email
Booby-trapped links/attachments encrypt servers and leak data.
Risk: Production downtime, extortion, and regulatory fallout (ransomware in 30% of breaches).

Zero-day via attachments/links
Unknown exploits slipping past basic filters.
Risk: Footholds in mailboxes → jump to systems you actually care about.

E-MAIL SECURITY

FOR HOUSTON OIL & GAS

TECHOIL

OBTAIN THE BEST MANAGED EMAIL SECURITY SERVICE FOR HOUSTON OIL & GAS OPERATIONS

OT aware, bilingual, and locally managed.

Oil & Gas specialization

Rules and detections tailored to typical sector flows (vendors, contracts, loading orders, payment instructions).

Local response + CST hours

Team in the Houston time zone with response SLAs coordinated with operations.

Onboarding + managed DMARC in 5 days

Technical validation/PoC and governance, with audit-ready reporting.

Executive simulations & training

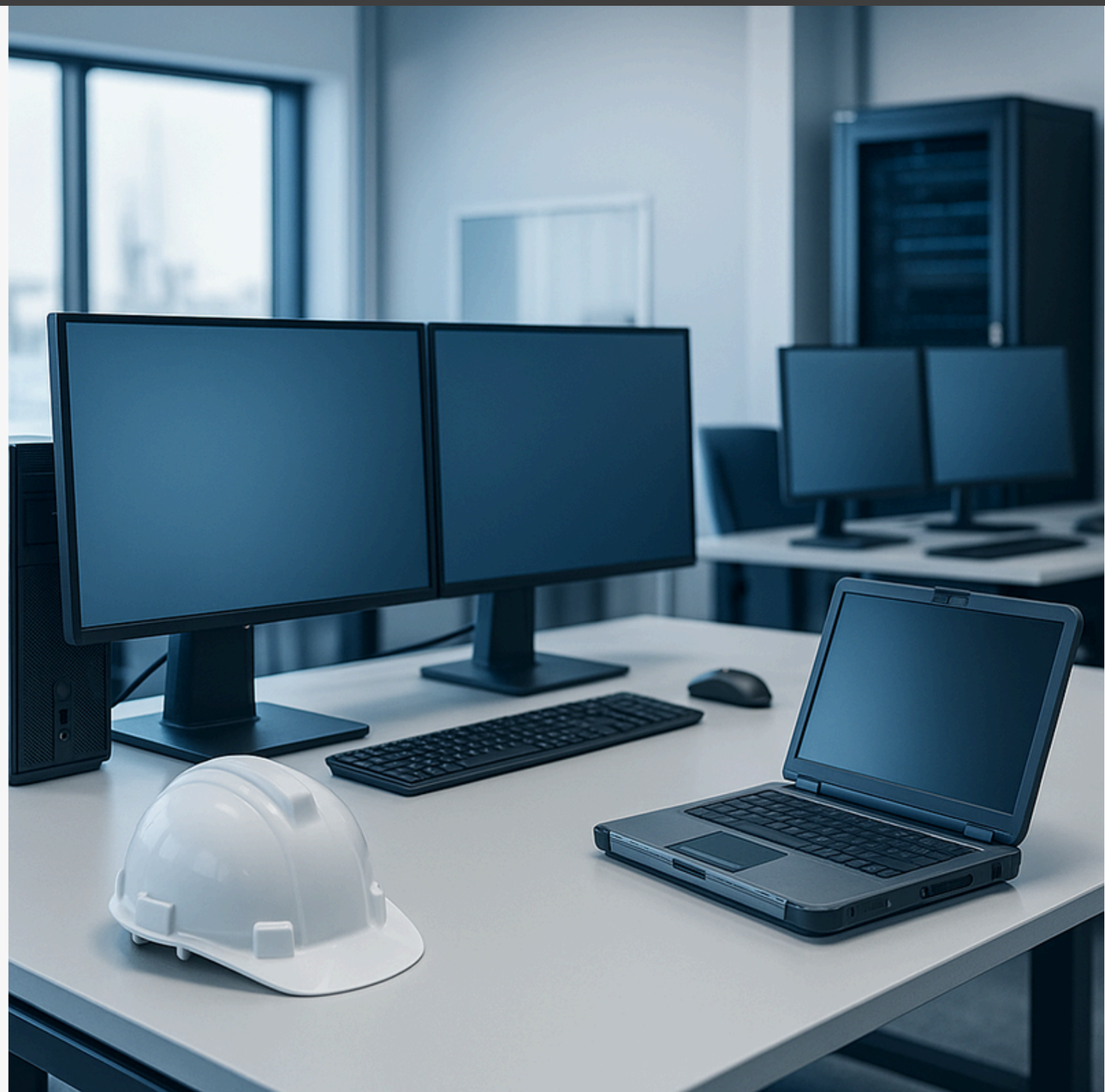
Phishing simulations targeted at critical roles (CFO, VP Ops, logistics).

TOTAL THREAT DEFENSE

ANTIPHISHING: SPOTS FAKE PAGES AND VISUAL TRICKS BEFORE THE CLICK. **ANTISPAM:** REMOVES NOISE AND REDUCES DAILY ATTACK SURFACE. **EMAIL ANTIVIRUS:** BLOCKS KNOWN-BAD ATTACHMENTS AT THE GATEWAY. **SANDBOXING:** DETONATES LINKS/FILES IN ISOLATION TO CATCH UNKNOWNS (YOUR BEST FRIEND AGAINST ZERO-DAY). **BEC PROTECTION:** FLAGS IMPOSTOR DOMAINS, ANOMALOUS WIRE REQUESTS, AND SENDER-BEHAVIOR RED FLAGS. **ADVANCED AI BEHAVIOR ANALYTICS + ZERO-DAY DETECTION:** LEARNS NORMAL PATTERNS (WHO EMAILS WHOM, WHEN, HOW) TO CATCH NEVER-SEEN-BEFORE ATTACKS FAST. **EMAIL AUTHENTICATION** (WE IMPLEMENT & MANAGE IT). **DMARC, DKIM, SPF:** STOP OTHERS FROM SENDING MAIL AS YOUR DOMAIN, SHUT DOWN SPOOFING, AND IMPROVE LEGITIMATE DELIVERABILITY. A CORE ANTIDOTE TO BEC. **SEAMLESS INTEGRATION MICROSOFT 365 & GOOGLE WORKSPACE:** FAST ROLLOUT, POLICY MAPPING, GROUPS, AND COMPLIANCE ALIGNMENT WITHOUT BREAKING WORKFLOWS. **VISIBILITY & EXPERT CONTROL:** REAL-TIME ALERTS AND REPORTING, QUARANTINE MANAGEMENT, AND FULL TRACEABILITY FOR AUDITS AND EXECUTIVE DECISIONS.

SYSTEM REQUIREMENTS

- Microsoft O365 + Defender
- Microsoft O365 + Email Security Gateway (brand-agnostic)
- Any email service (SaaS) + Email Security Gateway (brand-agnostic)



DELIVERABLES

Quarantine management

Tickets/reports will be handled for reviewing and/or releasing emails placed in quarantine by the security system. Prior to release, the corresponding analysis will be performed to identify potential threats, and you will be notified if there is any possible security risk or if it is a false positive.

Proactive monitoring

Continuos quarantine reviews will be performed throughtout the day, releasing potential false positives across up to 5% of the contracted mailboxes (as designated by you). The goal is to maintain business continuity for mailboxes critical to operations or key personnel.

Handling reports of suspicious email

Messages reported by users as unsolicited or containing suspicious information will be reviewed, and you will be notified if any specific action is required based on the analysis.

Blocklist management

If supported by the current solution, blocklists (blacklists) will be managed to add any sender or domain identified as malicious.

Identification of IoCs

Based on the capabilities of the current security solution, Indicators of Compromise identified from user reports and/or the solution's security telemetry will be analyzed, and a notification with recommendations will be sent to your appropriate team.

Weekly report delivery

Depending on the capabilities of the current security solution, weekly reports on email activity will be generated and delivered according to your areas of interest.

Awareness campaigns

Additional cost; quote required.

NOTES

Please take the following points into account:

1. The security configuration of the current platform remains the responsibility of the vendor/manufacturer.
2. User accounts on the current security platform must be provided with a monitoring role that has privileges to:
-Manage quarantine and add/remove domains/senders from the blocklist (blacklist).
-If an analysis module is available, extract the findings identified by the solution.
-Access the reporting module to generate reports.
-Access the logs and/or auditing module.
3. Knowledge transfer for the current security tool will cover only the modules mentioned above.

E-MAIL SECURITY
FOR HOUSTON OIL & GAS
TECHOIL

- Quarantine management
- Proactive monitoring
- Handling reports of suspicious email
- Blacklist (blocklist) management
- Identification of IoCs (Indicators of Compromise)
- Delivery of weekly reports
- Awareness campaigns (additional cost; quote required)

Transparent pricing:

US$19.99

Mailbox / month.

Onboarding and integration included.

RELEASE DATE:
September 18, 2025.

ONE CLICK IS ALL IT TAKES:
UNDER 60 SECONDS TO TAKE THE BAIT;
68% OF BREACHES INVOLVE PEOPLE.

IF YOUR EMAIL GOES DOWN, YOUR PLANT GOES DOWN.
EVERY DAY WITHOUT PROTECTION IS AN OPEN WINDOW.

REQUEST A POC TODAY

001-1000-001

techoil.io

SOURCES

FBI Internet Crime Complaint Center (IC3) — 2024 Internet Crime Report (BEC figures).
Verizon — 2024 Data Breach Investigations Report (DBIR) (human element and extortion/ransomware statistics).
IBM — Cost of a Data Breach Report (2024/2025 summaries on average breach cost).

TECHOIL
YOUR TRUSTED PARTNER EMPOWERING WITH AI