COMPLETE EMAIL & IDENTITY SECURITY

90% of breaches start with an email or a stolen login.

Not with exotic zero-days. With a convincing login page, a plausible invoice, a helpful-sounding voice on the phone. The hardest part of enterprise security isn't the perimeter — it's the inbox, the identity, and the person clicking.

$4.45M
Avg. cost of a single breach (IBM, 2024)

277 days
Median time to identify and contain

2 / 3
Orgs hit by ransomware in the last 24 months

82%
Of breaches involve the human element

WHERE MODERN ATTACKS ACTUALLY LAND

Email
Phishing, BEC, and malware delivered straight to the inbox.

Identity
Stolen credentials used to take over a single account.

Cloud storage
Ransomware and silent data exfiltration in shared drives.

Collaboration
Teams, Slack, and shared workspaces traditional tools miss.

Employee
Human error remains the most exploited surface in any org.

THE ARCHITECTURE

Four integrated layers. One security posture.

Most orgs buy four separate tools from four separate vendors and hope the gaps line up. We deploy one integrated platform where each layer covers the others' blind spots.

LAYER 01

Email & collaboration protection

Stops phishing, impersonation, malicious links, and malware before they reach a user. Extends from inbox to Teams, Slack, and shared file repos.

- Phishing / BEC
- Malware
- Impersonation
- Malicious links

LAYER 02

Identity threat detection

Every account monitored 24/7 for unusual login locations, impossible-travel patterns, and unauthorised access. Compromised accounts are contained in minutes.

- Account takeover
- Credential stuffing
- MFA fatigue
- Insider abuse

LAYER 03

Security awareness training

Ongoing, targeted training and realistic simulated phishing. Human error drives most breaches — this layer converts your team into the first line of defense.

- Clicks on phish
- Weak passwords
- Data handling
- Social eng.

LAYER 04

Microsoft 365 data protection

Continuous backup of Mail, Teams, OneDrive, and SharePoint. Recover from ransomware or accidental deletion in minutes, not days.

- Ransomware
- Accidental deletion
- Malicious insider
- Data corruption

WHAT GETS PROTECTED

- All inbound, outbound, and internal mail traffic
- Every user identity and login event, continuously
- Microsoft Teams, Slack, and shared workspaces
- SharePoint, OneDrive, and shared document libraries
- Human behaviour, through ongoing training

WHAT GETS STOPPED

Phishing — intercepted before it reaches users.

Account takeover — detected and contained in real time.

Data loss — prevented through backup and access controls.

Malware — blocked at the point of entry across channels.

Fraudulent wire requests — stopped through BEC detection and training.

THE CASE

What changes when you deploy this.

WITHOUT THIS PROTECTION

Average breach. $4.45M per incident, before lost customers.

Downtime. Days to weeks of operational disruption.

Reputation. Customer trust eroded, often permanently.

Regulatory. GDPR, HIPAA, and SOC 2 exposure compound the cost.

Ransomware. Data encrypted, ransom demands mounting.

Leadership. Board scrutiny. Personal liability for CISOs..

WITH OUR PLATFORM

Email threats. Blocked before they reach a single user.

Account takeover. Detected and contained in real time.

Human risk. Continuously reduced through training.

Critical data. Backed up and recoverable within minutes.

Audit readiness. Security posture documented at all times.

Business continuity. Maintained even under active attack.

4	24 / 7	100%	15 min
Security layers, one platform	Continuous identity monitoring	Microsoft 365 data coverage	Typical containment on ATO events

NEXT STEP

A 30-minute risk assessment. No obligation, no slide pitch.

We'll review your current email and identity posture, flag the gaps this platform closes for you specifically, and leave you with a written summary either way.

hello@methodologyit.tech 800-270-0016 methodologyit.tech

SCAN TO SCHEDULE