blueAPACHE

EMPOWER · HUMAN RISK MANAGEMENT

# Your people are the new perimeter.

Accidental insiders, malicious insiders and unsanctioned AI tools are now the single biggest risk to your data. emPOWER Human Risk Management gives you one command centre to see them, score them and stop them, in real time.

VISIBILITY & DETECTION

RESPONSE & REMEDIATION

BACKUP & COMPLIANCE

WORKFORCE RESILIENCE

blueAPACHE

# The biggest risk to your data is a human behind a keyboard.

Eighty-plus percent of breaches now involve a person, not a zero-day. A staff member clicks a lure, drags source code into a personal drive, or pastes a customer list into an AI prompt. Different intent. Same outcome: sensitive data leaves the building.

Legacy security stacks were built to defend the network. They struggle to see the people moving inside it. emPOWER closes that blind spot, connecting real behaviours to targeted intervention.

## THREE FACES OF HUMAN RISK

| | |
|---|---|
| **The accidental insider** | Well-intentioned employees mishandling data through misaddressed email, oversharing in collaboration tools or risky cloud uploads. |
| **The malicious insider** | Departing staff, disgruntled contractors and credential-borne attackers deliberately exfiltrating source code, customer lists and IP. |
| **The shadow AI vector** | Generative-AI tools and unsanctioned SaaS quietly siphoning PII, PCI and proprietary content out of the business at unprecedented speed. |

## WHERE THE RISK NOW LIVES

**82%**

of breaches involve a human element: phishing, error or misuse.

**3×**

rise in sensitive data moving to AI tools, personal cloud and removable media.

**17+**

integrations stitch email, endpoint, identity and data into one risk score.

blueAPACHE

# Four disciplines. One command centre.

emPOWER aggregates signals from across email, endpoint, data and identity, and turns them into an actionable risk score for every employee.

01
PREPAREDNESS

SECURITY BEHAVIOUR MANAGEMENT

## Transform risk into resilience

Connect real behaviours to targeted intervention, closing the gap between knowledge and action.

- Context-aware nudges at the point of risk, via email, Slack and Teams.
- Training personalised at scale, auto-assigned by individual risk score.
- Individual scorecards keep every employee accountable and engaged.

02
DETECTION

EMAIL & COLLABORATION PROTECTION

## Stop modern phishing and BEC

AI-powered protection that adapts to evolving phishing, business email compromise and impersonation.

- Adaptive AI detects advanced threats traditional gateways miss.
- Keeps malware and phishing out of Teams, Slack and OneDrive.
- Recovers mail, contacts and calendar fast, with zero downtime.

THE SHIFT

"Companies have discovered source code and customer lists being exfiltrated during a 30-day proof of value. The risk is already inside. The question is whether you can see it."

INSIDER RISK BENCHMARK · INCYDR

blueAPACHE

# Visibility, then defensible response.

The second half of the platform: see every movement of sensitive data, then evidence and act on it without slowing the business down.

03
VISIBILITY

INSIDER RISK MANAGEMENT

## See data leaving your business

Adaptive data protection with unmatched visibility across work channels, no policies required.

- AI-driven detection prioritises exfiltration risks across billions of signals.
- Dashboards for shadow AI, cloud storage and source-code movement.
- Content Inspection flags PII, PCI and custom data risks instantly.

04
RESPONSE

DATA GOVERNANCE & COMPLIANCE

## Stay ahead of regulators

Proprietary AI and ML analyse digital conversations for emerging threats and risky patterns.

- Natural-language e-discovery and case management across collaboration data.
- Mimecast Cloud Archive for legal hold and long-term preservation.
- Trustworthy alerts on employee patterns and compliance breaches.

OUTCOMES ACROSS THE FOUR DISCIPLINES

### Visibility & detection

Every risky behaviour surfaced across email, endpoint, data and identity.

### Response & remediation

Adaptive controls that intervene before data leaves the business.

### Backup & compliance

Archive, legal hold and e-discovery ready for the regulator.

### Workforce resilience

People who recognise risk and act on it, measured individually.

blueAPACHE

# The human risk command centre.

One pane of glass unifying behaviour-based signals across your stack, contextualised into actionable risk scores, from individual scorecards to enterprise dashboards.

SIGNALS, SCORE, ACTION

EMAIL | ENDPOINT | IDENTITY

DATA | CLOUD / SAAS | SHADOW AI

MIMECAST HRM CORE

## Human Risk Command Centre

Aggregates and contextualises behaviour-based signals into a single risk score per user.

### Detect

Real-time threat and behaviour analytics.

### Respond

Adaptive controls and targeted nudges.

### Resolve

Watchlists, training and e-discovery.

blueAPACHE

# Run a 30-day proof of value.

See what is really leaving your business. Most clients surface their first high-risk insider in week one, no policy writing, no lengthy deployment.

## WHAT HAPPENS IN THE 30 DAYS

WEEK 1

### Connect and observe

Signals stream in from email, endpoint, identity and cloud. No policy writing.

WEEK 2

### Score the workforce

Risk scores per user, with shadow AI and data movement surfaced by dashboard.

WEEK 4

### Review the findings

A readout of real incidents, with the intervention plan to close them.

## CONNECTED ECOSYSTEM

**17+**

INTEGRATIONS

Native integrations with the security tools you already trust, enriched with SIEM, SOAR and custom dashboard access.

- CrowdStrike
- Okta
- Netskope
- Microsoft 365
- SIEM platforms
- SOAR platforms

SPEAK WITH US

1800 248 749

WEB & EMAIL

blueapache.com

sales@blueapache.com