SOLUTION BRIEF

UK Cyber Assessment Framework (CAF)

Building cyber resilience that goes beyond the checkbox

If your organisation keeps the lights on, the water running, the trains moving, or emergency services responding, a cyber attack is a public safety problem. The NCSC's Cyber Assessment Framework (CAF) exists for this reason: to help organisations running essential services find out whether their defences are truly up to the job. But its rigorous, outcomes-based approach has proven useful well beyond critical infrastructure—to the NHS, telecoms, central government, and a growing number of organisations that want a credible benchmark for cyber resilience.

The CAF organises cyber resilience into four objectives and 14 principles, each assessed against specific evidence of what good looks like in practice. What matters is not what tools you have, but whether your security capabilities can deliver the right results—and Mimecast solutions are built to do exactly that across all four objectives.

The Mimecast Advantage

Objective A: Managing Security Risk

Effective risk management under the CAF requires a dynamic understanding of where risk sits—and for most organisations the greatest concentration of risk isn't in their systems. It sits with their people. Mimecast Mihra AI (Mimecast Intelligent Human Risk Agent) builds an individualised risk profile for each of your users by aggregating signals from across our own tools and the third-party security tools across your stack.

Objective B: Protecting Against Cyber Attack

Threats follow people wherever they work—across email, messaging platforms, file sharing, and document collaboration—and Mimecast's protection spans that entire surface, extending detection, data security, and adaptive response to the full scope of how organisations operate. And as AI reshapes both how attacks are crafted and how employees work, Mimecast's protection extends to guarding against AI-generated threats and securing the sensitive data that flows to and from the AI tools your people use every day.

Key Benefits

- **All CAF objectives addressed**
  From governance and risk management to incident recovery and lessons learned.
- **Evidence-based outcomes**
  Individual risk scoring, behavioural data, and forensic logging give assessors what they need.
- **Protection where people work**
  Email, collaboration tools, insider risk, and sensitive data in motion—secured.
- **A connected security ecosystem**
  Integrations enrich risk intelligence and extend response capabilities across the stack.

Objective C: Detecting Cyber Security Events

CAF v4.0 recognises that reactive monitoring is not enough—and Mimecast goes further, combining post-delivery threat hunting, AI-assisted investigation, and bidirectional integration with SIEM, SOAR, and XDR platforms to detect and investigate threats across the wider security stack.

Objective D: Minimising the Impact of Cyber Security Incidents

When incidents occur, Mimecast ensures organisations can respond quickly with automated workflows that trigger response actions across every layer of your defences. Resilient infrastructure with a 100% availability SLA, rapid data recovery, and tamper-proof archiving ensures operations are maintained and regulatory obligations are met.

Mimecast Product Mapping

The table below identifies the Mimecast products that address each CAF principle.

CAF Principle	Mimecast Products
Objective A: Managing Security Risk	
A1: Governance	HRCC*, Aware, Engage
A2: Risk Management	HRCC*, Advanced Email Security, Engage, Incydr
A3: Asset Management	Incydr, Aware
A4: Supply Chain	Advanced Email Security, DMARC Analyzer
Objective B: Protecting Against Cyber Attack	
B1: Service Protection Policies	Advanced Email Security, HRCC*
B2: Identity & Access Control	Advanced Email Security
B3: Data Security	Incydr, Aware, Advanced Email Security
B4: System Security	Advanced Email Security, Collaboration Threat Protection
B5: Resilient Networks & Systems	Advanced Email Security, Cloud Archive
B6: Staff Awareness & Training	Engage, HRCC*
Objective C: Detecting Cyber Security Events	
C1: Security Monitoring	HRCC*, Advanced Email Security, DMARC Analyzer
C2: Threat Hunting	Advanced Email Security, HRCC*
Objective D: Minimising the Impact of Cyber Security Incidents	
D1: Response & Recovery Planning	Advanced Email Security, Cloud Archive, Aware
D2: Lessons Learned	HRCC*, Advanced Email Security, Engage

*The Human Risk Command Centre is included with Advanced Email Security and Engage licences at no additional cost.

Detailed Principle Mapping

The table maps the CAF's 14 principles to the ideal outcomes and Mimecast's capabilities.**

CAF Principle	Mimecast Products	How Mimecast Helps
Objective A: Managing Security Risk		
A1: Governance	There is board-level accountability for security. Clear roles, responsibilities, and policies govern how systems are protected.	Centralised risk dashboards give leadership the data they need for informed governance decisions. Compliance monitoring across email and collaboration platforms detects policy violations in real time, supporting adherence to GDPR, HIPAA, and sector-specific regulations.
A2: Risk Management	A dynamic, evidence-based risk management process is in place, informed by current threat intelligence and an understanding of threat actor methods.	Detection engines refined through analysis of 7-billion interactions daily (email, Teams, Slack, etc.) continuously update threat understanding. Integrated threat intelligence and security signals from 350+ partner tools inform risk decisions and enrich individual user risk profiles for more precise targeting.
A3: Asset Management	There is a complete picture of assets, including data, systems, and people. Sensitive data is classified and managed throughout its lifecycle.	Data protection capabilities monitor the movement of sensitive data—PII, PCI, and intellectual property—across endpoints, collaboration tools, and email. AI-based content inspection and configurable retention policies classify and manage collaboration data by type and sensitivity, with automated removal ensuring compliance with data protection requirements.
A4: Supply Chain	Security risks from third-party suppliers are identified and managed. Contracts include appropriate obligations. Third-party access is monitored.	Advanced BEC protection guards against supply chain fraud, using machine learning and natural language processing to detect impersonation and social engineering. DMARC enforcement provides full visibility into who is sending email on behalf of an organisation's domains, including unauthorised senders.
Objective B: Protecting Against Cyber Attack		
B1: Service Protection Policies	Policies and controls are in place, and regularly reviewed and updated, to protect systems and services, consistent with risk.	Policy-based controls govern email and collaboration security across the organisation, with configurable sensitivity levels and best-practice defaults so security teams can enforce consistent protection without operational complexity. Adaptive policy controls automatically adjust protection based on real-time user risk scores.

B2: Identity & Access Control	Access is restricted to authorised users. Privileged access is controlled. Authentication mechanisms are proportionate to risk.	Social graphing and identity analysis maps communication relationships across the organisation, detecting anomalies that indicate account compromise or impersonation. Dynamic warning banners alert users to suspicious senders in real time. Misaddressed email detection prevents accidental data exposure.
B3: Data Security	Sensitive data is identified, classified, and protected at rest and in transit. Controls prevent unauthorised access, exfiltration, or loss.	Mimecast provides continuous monitoring of data movement across endpoints, collaboration tools, and email. AI-powered content inspection detects PII, PCI, and custom-defined sensitive content. Shadow IT detection identifies when sensitive data is sent to unsanctioned applications—including generative AI tools—and prevents unauthorised exfiltration. End-to-end encryption protects data in transit; and tamper-resistant encrypted archiving of email and collaboration data ensures data integrity, chain of custody, and audit-ready retention aligned to regulatory requirements.
B4: System Security	Systems are protected from attack. Vulnerabilities are managed. Malware, phishing, and exploitation attempts are detected and blocked.	Multi-layered email threat protection combines antivirus scanning, full-emulation sandboxing, URL analysis, attachment inspection, impersonation detection via social graphing, natural language processing, and computer vision AI—catching sophisticated and AI-generated attacks before they reach users. Protection extends to collaboration platforms including messaging tools, file sharing, and document collaboration.
B5: Resilient Networks & Systems	Systems are designed to maintain availability and recover quickly from disruption. Business continuity planning is tested and maintained.	Continuity capabilities maintain uninterrupted email access during outages, backed by geographically dispersed infrastructure and a 100% availability SLA. Rapid granular recovery of mailboxes, calendars, and communications supports restoration following ransomware or other disruptive events.
B6: Staff Awareness & Training	Staff understand cyber risks relevant to their role and know how to respond. Training is ongoing, measurable, and reflects the real threat environment.	Risk scoring draws on actual user behaviour—including responses to real-world threats—not just simulated phishing. Training and behavioural nudges target individuals who need them most at the point of risk. Eight percent of users drive 80% of security incidents; this approach focuses intervention where it has the greatest impact.

Objective C: Detecting Cyber Security Events		
C1: Security Monitoring	Monitoring is in place to detect events across systems. Logs are collected and analysed. Alerts are prioritised and acted upon.	The Human Risk Command Centre aggregates and prioritises signals from email, collaboration tools, insider risk monitoring, and third-party integrations into a unified risk view, giving security teams the visibility to act on what matters most.
C2: Threat Hunting	Proactive searches take place for threats that may have evaded existing defences. Investigation capabilities identify and act on indicators of compromise.	Post-delivery scanning continuously searches for threats that bypassed initial defences, automatically removing malicious messages within seconds. AI-assisted investigation allows analysts to interrogate large volumes of communication data using natural language queries—compressing days of manual review into minutes.
Objective D: Minimising the Impact of Cyber Security Incidents		
D1: Response & Recovery Planning	Response and recovery plans are in place, tested, and understood. Critical data and communications are preserved and recoverable.	Continuity capabilities maintain full email security during incidents, preventing attackers from exploiting recovery windows. SIEM, SOAR, and XDR integrations enable automated response workflows, triggering actions such as blocking malicious senders, isolating compromised systems, and adjusting user access based on risk—reducing time to remediation from hours to minutes. Tamper-proof archiving with immutable storage preserves data in a legally defensible state, with litigation hold and eDiscovery capabilities enabling rapid response to legal and regulatory requests.
D2: Lessons Learned	Post-incident review processes are in place. Lessons are used to improve controls and reduce likelihood of recurrence.	After an incident, Mimecast's AI-assisted investigation examines communication data to identify root cause and drive targeted improvements to controls and training. Detailed forensic logging supports regulatory reporting.

**Achieving full alignment with CAF v4.0 requires the implementation of internal processes, governance structures, and organizational maturity that cannot be fully addressed by technical solutions alone.

About Mimecast

Mimecast is an AI-powered, API-enabled connected security platform purpose-built to protect organisations from the spectrum of cyber threats, with human risk at the centre of everything we do. Our platform enhances visibility, provides strategic insight, and enables decisive action—empowering organisations to secure their collaborative environments, safeguard critical data, and actively engage employees in reducing the risks that technology alone cannot solve. More than 42,000 organisations worldwide trust Mimecast to keep ahead of the ever-evolving threat landscape.