Resilience in a post-Quantum world

Redefining Data Security for the Age of AI & the Quantum Era

Adam McElroy – CTO Eclypses

February 2026

“ Is the firm effectively prepared to continue delivering important business services within tolerance whilst impacted by severe and plausible risk scenarios ? ”

- CEO / Chair / INED

Keeping pace with these 'frontier' AI-cyber developments will almost certainly be critical to cyber resilience for the decade to come, as we explained in our recent assessment on the Impact of AI on cyber threat from now to 2027.

AI will almost certainly pose cyber resilience challenges to 2027 and beyond, across critical systems and economy and society.

These will range from responding to an increased volume of attacks, managing an expanded attack surface and keeping pace with unpredictable advancements and proliferation of AI-cyber capability.

The Cyber Security and Resilience (Network and Information Systems) Bill proposes new laws to improve UK cyber defences and protect our essential public services.

European Union

EUR-Lex

Access to European Union law

Official Journal of the European Union L 333/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

HM Government

70 Whitehall
London
SW1A 2AS

13 October 2025

Dear CEO / Chair,

Making cyber security a board responsibility

Hostile cyber activity in the UK is growing more intense, frequent and sophisticated. This is causing significant financial and social harm to UK businesses and citizens. There is a direct and active threat to our economic and national security which requires an urgent collective response.

The government is taking significant action to counter the cyber threat and has developed tools to help businesses to defend themselves, but we cannot do this alone. We ask you and the CEOS and chairs of other leading UK companies to take the necessary steps to protect your business and our wider economy from cyber attacks. Cyber resilience is a critical enabler of economic growth, so getting this right will promote growth and foster a stable environment for investment and innovation.

1. Make cyber risk a Board-level priority

Effective governance of cyber risk is fundamental to business resilience. Executive and non-executive directors should prioritise this and ensure it is considered in strategic decision-making. The government's ***Cyber Governance Code of Practice***, developed with industry leaders, sets out critical actions Boards and directors should take to govern cyber risk effectively. We urge you and your Board to use this Code to ensure your organisation.

2. Sign up to the NCSC's Early Warning service

Early Warning is a free service from the government's National Cyber Security Centre (NCSC) *which informs your organisation of* potential cyber attacks on your network, giving you invaluable time to detect and stop *a cyber incident before it excalates.* We strongly advise you and your suppliers to register for this *free and simple service.*

3. Require Cyber Essentials in your supply chain

Supply chain cyber attacks are increasing, yet just *14%* of UK businesses asses the cyber risks posed by their immediate suppliers. ***Cyber Essentials*** is a highly effective government-backed scheme which certifies that organisations have key cyber protections in place to prevent common cyber attacks. It is the minimum cyber security standard businesses should seek to gotain. Organisations with **Cyber Essentials** are significantly less likely to make a claim on their cyber insurance. As leaders of the nation's largest businesses, we ask you to embed the *same requirements across your supply chain.*

Time to Act

Strengthening our nation's cyber resilence requires close collaboration between government and industry. *Our forthcoming* ***Cyber Security and Resilience Bill*** will increase protections for essential and digital services. Whether or not your business is in scope, the NCSC's ***Cyber Assessment Framework*** (CAF) *can also be used to improve cyber resilence for your most critical services.*

We invite you to confirm receipt of this letter and share the senior contact we should communicate with on this issue.

Rt Hon Liz Kendall MP
Secretary of State for Science, Innovation and Technology

Rt Hon Rachel Reeves MP
Chancellor of the Exchequer

Rt Hon Peter Kyle MP
Secretary of State for Business and Trade

Dan Jarvis MBE MP
Minisser for Security

Dr Richard Horne
CEO, National Cyber Security Centre

Graeme Biggar CBE
Director General, National Crime Agency

Data (Use and Access) Act 2025

Government Bill

Originated in the House of Lords, Session 2024-26

FCA

Operational resilience

Policy paper

G7 Cyber Expert Group Statement on Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector: January 2026

Published 13 January 2026

eclypses

1977

Gartner

February 5, 2026

Postquantum Action Plans

Gartner predicts advances in quantum computing will render the asymmetric cryptography organizations rely on to secure data and systems unsafe by 2030 ..... Post quantum cryptography alternatives must be adopted now to avoid potential data breaches, legal liability and financial loss from "harvest now, decrypt later" attacks targeting long-term sensitive data.

2030

End-to-End data protection for AI

AI platforms might encrypt data at rest on industry-standard cloud infrastructure.
External key-management (EKM) options may allow Enterprise customers to use their own encryption keys but not every AI model or agent currently supports EKM and it requires that customers take responsibility for control of their key lifecycle.

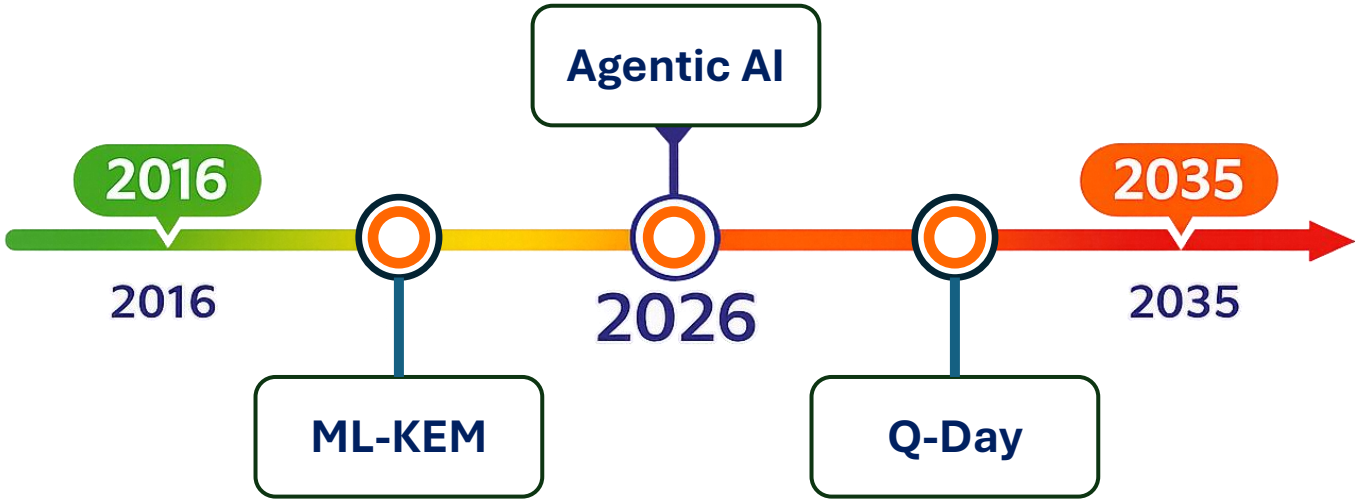
Adopting Eclypses for data protection for AI :

- Simplifies & accelerates AI adoption.
- Enables robust data protection for agents & models.
- Encrypts the agentic payload itself, before it hits the network layer.
- Adds a Quantum safe cryptographic enforcement layer for all products and endpoints.
- Removes any dependencies on network security controls and needs no back-end changes.
- Encryption and decryption happens within your estate — keys and data remain invisible, everywhere.
- Delivers agile, programmatic, polymorphic encryption + removes all client requirements for key management.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

FIPS 140-3™ (#4690)

eclypses



“ Is the firm effectively prepared to continue delivering important business services within tolerance whilst impacted by severe and plausible risk scenarios ? ”


eclypses

FIPS 140-3

Validated Inside
(#4690) by NIST

Offices

Colorado Springs, CO
Boston, MA

U.S. Patents

12 issued
1 pending

Best Security Solution

2022 & 2023
FTF News Technology
Innovation Awards

Data Protection Solution

2023 CyberNews
Best Choice

Hot Vendor

2024 & 2025 HFS OneEcosystem™
Hot Vendor

Adam McElroy, CTO

Adam.McElroy@eclypses.com

eclypses.com