# UK MoD adopts Castlepoint’s AI to curb human error after Afghan data breach



Britain's Ministry of Defence (MoD) has selected Australian cybersecurity firm Castlepoint Systems to automate data classification and reduce risks associated with human error in handling sensitive information. This marks Castlepoint’s inaugural contract in the UK, coinciding with heightened concerns over data security, particularly following the 2022 Afghan data breach which compromised nearly 19,000 personal records and generated widespread public scrutiny.

Castlepoint, now headquartered in London, brings its explainable artificial intelligence (AI) technology to bear on the MoD’s vast and complex data environment. The system automatically classifies data such as emails, reports, and documents at the point of creation, based on content and context, while offering traceable justifications for each classification decision. This transparency is crucial for meeting the UK’s stringent ethical and legal standards around AI deployment. By significantly minimising reliance on manual processes, Castlepoint addresses a known vulnerability in national security protocols—human error in labelling and managing unstructured data.

Rachael Greaves, CEO of Castlepoint Systems, described securing the MoD contract as a critical milestone for the company, emphasising the broader importance of sophisticated data control across organisations beyond national security. She highlighted Castlepoint’s explainable AI and true autoclassification capabilities as instrumental in improving labelling accuracy and coverage, while ensuring minimal disruption to MoD personnel.

The agreement signals Castlepoint’s formal entry into the UK and European markets, which are witnessing growing demand for AI-driven solutions in public sector data governance. The company is already well-established in Australia and New Zealand, where it serves two-thirds of the Australian Federal Government, overseeing more than 286.5 million records across over 1.6 million systems. This extensive footprint underscores the effectiveness of Castlepoint’s technology in managing the surge of digital records—Australian government data volume increased from 51 terabytes in 2013 to more than 314,000 terabytes in 2022.

Castlepoint’s founding vision, shaped by co-founders Greaves and Gavin McKay during years of government and corporate audits, was to tackle the escalating challenges of data storage, compliance, and security through ethical AI. Their platform integrates discovery, audit, privacy, cybersecurity, and records management, a holistic approach designed to address the escalating cyber and privacy risks posed by insecure data retention and management practices. Traditional enterprise document and records management systems have struggled to keep pace, leaving a vast quantity of sensitive information inadequately controlled, widening potential vulnerabilities.

The company’s market recognition extends beyond government contracts. Castlepoint has been named among Australia’s top 100 innovators in cybersecurity for three consecutive years, reflecting ongoing advancements in ethical AI and information governance. It has also been included in the CyberTech100 list, highlighting its impact in bolstering cybersecurity resilience, particularly for financial institutions.

Castlepoint’s approach is characterised by its emphasis on transparency and ethical considerations, ensuring AI-driven decisions do not inadvertently increase risks to citizens or organisations. Its innovation has been identified as strategically important for national security, offering governments clarity and control over their data environments while alleviating pressures on public sector resources.

This development comes amidst broader efforts within allied defence sectors to enhance data security frameworks. For instance, South Australian cybersecurity company Secure State recently launched a pioneering cloud solution tailored to defence needs under the AUKUS partnership, aiming to protect classified and sensitive information in compliance with complex international security standards. Such innovations underscore an increasing recognition of the vital role advanced cybersecurity solutions play in national and allied defence strategies.

Castlepoint’s MoD contract represents a significant step in evolving the UK’s data governance capabilities, equipping the MoD with advanced tools to mitigate risk, safeguard sensitive information, and uphold accountability in an era where the volume, variety, and velocity of data present enormous challenges to legacy security models.

### 📌 Reference Map:

* Paragraph 1 – [[1]](https://tech.eu/2025/08/06/uk-mod-taps-australian-cybersecurity-startup-castlepoint-after-afghan-breach/), [[2]](https://tech.eu/2025/08/06/uk-mod-taps-australian-cybersecurity-startup-castlepoint-after-afghan-breach/)
* Paragraph 2 – [[1]](https://tech.eu/2025/08/06/uk-mod-taps-australian-cybersecurity-startup-castlepoint-after-afghan-breach/), [[2]](https://tech.eu/2025/08/06/uk-mod-taps-australian-cybersecurity-startup-castlepoint-after-afghan-breach/)
* Paragraph 3 – [[1]](https://tech.eu/2025/08/06/uk-mod-taps-australian-cybersecurity-startup-castlepoint-after-afghan-breach/), [[2]](https://tech.eu/2025/08/06/uk-mod-taps-australian-cybersecurity-startup-castlepoint-after-afghan-breach/), [[5]](https://www.castlepoint.systems/blog/castlepoint-government-momentum-media-release)
* Paragraph 4 – [[3]](https://idm.net.au/article/0014966-castlepoint-systems-named-top-100-cyber-innovator), [[5]](https://www.castlepoint.systems/blog/castlepoint-government-momentum-media-release)
* Paragraph 5 – [[3]](https://idm.net.au/article/0014966-castlepoint-systems-named-top-100-cyber-innovator), [[6]](https://australianfintech.com.au/castlepoint-systems-celebrates-inclusion-in-fourth-annual-cybertech100-list/), [[5]](https://www.castlepoint.systems/blog/castlepoint-government-momentum-media-release)
* Paragraph 6 – [[3]](https://idm.net.au/article/0014966-castlepoint-systems-named-top-100-cyber-innovator), [[5]](https://www.castlepoint.systems/blog/castlepoint-government-momentum-media-release)
* Paragraph 7 – [[4]](https://defencesa.com/news-events-and-media/news/secure-state-launches-nation-first-cybersecurity-defence-solution/)
* Paragraph 8 – [[1]](https://tech.eu/2025/08/06/uk-mod-taps-australian-cybersecurity-startup-castlepoint-after-afghan-breach/), [[2]](https://tech.eu/2025/08/06/uk-mod-taps-australian-cybersecurity-startup-castlepoint-after-afghan-breach/), [[5]](https://www.castlepoint.systems/blog/castlepoint-government-momentum-media-release)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://tech.eu/2025/08/06/uk-mod-taps-australian-cybersecurity-startup-castlepoint-after-afghan-breach/> - Please view link - unable to able to access data
2. <https://tech.eu/2025/08/06/uk-mod-taps-australian-cybersecurity-startup-castlepoint-after-afghan-breach/> - Britain's Ministry of Defence (MoD) has selected Australian firm Castlepoint Systems to provide services for automating data classification and reducing the risk of human error. The company is now headquartered in London. The selection marks Castlepoint’s first UK contract and comes on the heels of growing concern over the risks of mishandled sensitive information, most notably the 2022 Afghan data breach, which exposed nearly 19,000 personal records and drew sharp public criticism. Castlepoint’s technology alleviates the reliance on manual data classification by personnel operating across high-stakes environments. Human error, particularly in labelling and handling unstructured data, has been cited as a weak link in national security. In Castlepoint’s system, data such as emails, reports, and documents are automatically assessed and given the correct security marking at the point of creation, based on both content and context. Importantly, the system is explainable, providing traceable justifications for each classification decision, an essential feature in meeting the UK’s ethical and legal standards for AI deployment. This contract signals Castlepoint’s formal entry into the UK and European markets, where demand for AI solutions in public sector data governance is intensifying. The company is already established in Australia and New Zealand, where its technology is used by two-thirds of the Australian Federal Government. Castlepoint's CEO, Rachael Greaves, stated, “Castlepoint, with Explainable AI and true autoclassification at its core, can increase labelling accuracy and coverage without disrupting the essential work of MoD personnel.”
3. <https://idm.net.au/article/0014966-castlepoint-systems-named-top-100-cyber-innovator> - Castlepoint Systems has been recognised as one of Australia’s Top 100 Innovators in the Cyber Category for the third year running. This recognition highlights the company’s efforts in advancing information management and security through ethical AI solutions. Castlepoint was founded by Rachael Greaves and Gavin McKay, who identified a need for better data storage and compliance practices during their years of working on government and corporate audits. They developed a platform that uses ethical AI to discover, classify, and control all types of data within an organisation’s network. This includes documents, emails, chat messages, databases, and web pages, helping organisations manage rogue data and comply with regulatory requirements. Castlepoint defined a new category of information governance technology, as the founders recognised the importance of integrating the discovery, audit, privacy, and cyber functions for enterprises directly with records management. Records governance was being set aside as too difficult, and many organisations were not investing in lifecycle management. Legacy EDRMS systems could not handle the volume, variety, and velocity of record content, and most records were going completely unsentenced. This was not just an issue for the records team. Long term retention of sensitive data with no continuing business use has been resulting in an enormous threat surface from a cyber and privacy perspective. Organisations were being breached regularly, and spilling data they should no longer have even had on the network. Castlepoint’s novel approach to Explainable AI autoclassification meant that, for the first time, all content in the enterprise could be registered, classified, sentenced, and compliantly disposed, no matter where it was stored, or how it was labelled. This capability has transformed the cyber posture of its clients and has been identified as a strategic national security solution as a result. “We’re honoured to be recognised among Australia’s top innovators,” said Rachael Greaves, co-founder of Castlepoint Systems. “Our goal has always been to help organisations manage their data securely, compliantly, and ethically, without the downside risk inherent in legacy approaches.” Gavin McKay added, “As we grow globally, we remain focused on providing solutions that prioritise security and compliance. Explainability and Transparency are crucial for creating a safer digital environment, as both the threats and opportunities of AI boom.” Castlepoint Systems continues to drive innovation in cybersecurity and remains committed to transforming data management practices. It has recently launched its Generative AI Governance capability, enabling organisations to properly prepare for, and manage, Copilot adoption.
4. <https://defencesa.com/news-events-and-media/news/secure-state-launches-nation-first-cybersecurity-defence-solution/> - South Australian-based cybersecurity company, Secure State, has launched a national-first cloud solution for the defence industry to store and manage highly sensitive information related to AUKUS and other Defence programs. xClave will be the only secure sovereign platform in Australia that can meet the complex security regulations for handling information such as the Australian PROTECTED classified, US Controlled Unclassified Information (CUI) required by the Cybersecurity Maturity Model Certification (CMMC) and the UK Ministry of Defence Identifiable Information (MODII). This critical business enabler will support the secure communication and collaborative efforts between AUKUS partners, whilst also ensuring information is protected from ever-changing threats and espionage. Founder and Creator of Secure State, Luke Smith, explained this value of the platform to the defence industry. “By providing a secure, compliant, and cost-effective sovereign solution, xClave makes it easier for SMEs to meet their strict obligations within the AUKUS framework, enabling them to participate in critical projects and securely collaborate with partners, contributing to the security and technological advancement of Australia, the United States and the United Kingdom,” Mr Smith said. “This not only provides important peace of mind, but it also allows businesses to focus on innovation and growth – both in Australia and internationally – and unlocking lucrative opportunities within this vital sector.” South Australian Minister for Defence and Space Industries Stephen Mullighan highlighted that local companies are once again leading the way in the sector. “Addressing the cybersecurity challenges surrounding the AUKUS framework is crucial and it’s fantastic to see a South Australian-based company stepping up to deliver a leading solution that will support companies to protect sensitive information in a secure environment,” said Minister Mullighan. “This Australian-first innovation opens up opportunities for collaboration and broader participation by local industry in AUKUS program projects. It is a testament to our state’s continued commitment to advancing technologies in support of Defence initiatives.”
5. <https://www.castlepoint.systems/blog/castlepoint-government-momentum-media-release> - Castlepoint Systems has achieved over 100% year-on-year growth in FY23, with two-thirds of Australian federal government portfolios now using its ethical AI-driven platform to manage, protect, and govern sensitive data, ensuring compliance and cybersecurity across over 286.5 million records. Castlepoint now manages over 286.5 million records for its clients, equating more than ten records per Australian citizen, in over 1.6 million separate systems. The company has identified more than a quarter of a billion sensitive and high-risk records in enterprises that require protection, and applied records retention rules to these so they can be appropriately preserved or lawfully destroyed, reducing the potential harm of any future data spill. “Government has significant obligations for compliant information management,” said Rachael Greaves, CEO and Co-Founder at Castlepoint. “The volume of digital records held by Commonwealth entities has jumped from 51 terabytes in 2013, to more than 314,000 TB in 2022. There is just too much volume, variety, and velocity of data for legacy control methods to be effective. Castlepoint has disrupted these traditional models that have failed the test of time, and helped keep the Australian public service at the forefront of accountability and responsibility. By making discovery, audit, privacy, cyber security, and records management part of one enterprise capability, we have joined the hands of compliance and cyber teams united against a common threat environment. This has amplified their ability to mitigate the risk of losing our nation’s records which results from a lack of effective command and control,” said Greaves. Castlepoint supports agencies to discover, audit, and protect high risk and high value information from any system in a single interface with Explainable AI (XAI), and enables them to ease cost pressures and relieve strain on the nation’s public service. This allows governance teams to have a complete view across the whole environment, and quickly and easily apply security, discovery, and compliance processes. Castlepoint’s XAI is also architected with ethical considerations to ensure decisions about records and their automated management do not pose risks to citizens. Government customers like the Commonwealth Treasury are using the Castlepoint compliance system for more than just tactical management. "Castlepoint has given Treasury’s information management team the ability to confidently provide metrics and insights to senior leadership, and to support strategies and plans for improving information management capability,” said a Treasury spokesperson. “Having full control of information doesn’t need to cause unwanted impacts. With Castlepoint’s AI capabilities, we can know what data we have, where it is, and who is doing what to it. We can determine what inherent risk and value it has, what rules apply to it, and whether they are being met. And we can do this without the impacts we see on users, source systems, source data, or the regulatory team that we have all experienced before with other types of GRC solutions.”
6. <https://australianfintech.com.au/castlepoint-systems-celebrates-inclusion-in-fourth-annual-cybertech100-list/> - Castlepoint Systems, experts in data management and ethical AI for cybersecurity, has been listed in the fourth annual CyberTech100 list. The list highlights those organisations having a significant impact in the growing cybersecurity space for financial services, and celebrates the most innovative CyberTech companies across the globe that are improving the cyber defences of financial institutions. Founded by CEO Rachael Greaves and CTO Gavin McKay – and based on their direct experience working in public sector data management – Castlepoint Systems is the only company in the world that can give complex enterprises complete visibility of all the information in their environment, making it easier for them to know what they have, where it is, and who is doing what to it. Castlepoint Systems works with a global cross-section of leading financial organisations including the Australian Government Treasury to ensure that their cybersecurity is not only compliant right now, but ready to scale for the future. In a market that is evolving due to the digital challenges being increasingly posed by companies and individuals alike, such as generative AI, the CyberTech sector is proving to be an area of considerable future growth. Between 2023 and 2030, the industry is predicted to grow a CAGR of 13.8% from $172.3 billion to $424.9 billion. This year’s CyberTech100 includes some of the widest and most diverse businesses in the sector. A longlist of over 1,000 firms was produced by FinTech Global, with a panel of analysts and industry experts voting on the finalists. Castlepoint Systems was one of the companies selected based on their innovative