



Service Definition

Table of Contents

Summary of capability 3

 How the system works.....3

 How the system is differentiated4

 Key Castlepoint capabilities5

Hosting services 8

 Technical requirements.....8

 Backup and restore8

 Business continuity and disaster recovery8

 Maintenance and updates8

 Service levels.....9

Support services..... 9

 Customer success and training9

 SLA management10

 Security management.....11

Pricing 11

The Castlepoint service

Summary of capability

Castlepoint is a modern, innovative solution used and trusted by international Defence, government, critical industry, financial services, and regulated enterprises to apply cutting-edge technology to resolve the long-standing, intractable challenges of effective eDiscovery, security and records management, and the limitations of traditional records systems.

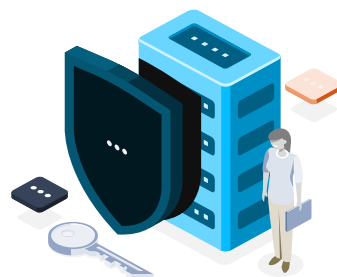
Castlepoint is a true manage-in-place solution, which does not move or modify source data, but also does not affect source systems with any customisations, agents, or connectors. Its operation is invisible to users and employs true Explainable Artificial Intelligence (XAI) automation via rules-as-code to accurately classify content, sentence it, make it discoverable, and flag its sensitivity, risk, and value. It is also a decision support tool which provides insights to support investigations, intelligence, audits, and compliance.

Users work as normal in any system. They do not change their behavior. Compliance is invisible and automated.



Castlepoint is rapidly deployed inside the secure environment. It authenticates to every system and registers, indexes, and automatically classifies every item (and event).

- NLP
- Rules as Code
- Containerized
- Manage in Place
- Agentless integration
- Cloud and on premises



Enterprise command and control without traditional impacts.

How the system works

Castlepoint **automatically registers** every information asset in a network in the central Castlepoint database. Castlepoint records the name, location, context, and metadata of the item, whether structured or unstructured. It captures the audit trail of the item, and monitors, tracks, and updates its status each time the item is modified or moved.

Castlepoint can alert on data changes relating to these entities, and can relate them together to be classified, sentenced, and managed as a single 'virtual record', even where the relevant items are in different systems.

Castlepoint then **reads** every word in every item and uses Natural Language Processing to extract key phrases and named entities from the content. These are registered in the Castlepoint database, and used for search and discovery, as well as to classify content against applicable rules and regulations.

Castlepoint uses AI to apply **rules-as-code** to all data holdings, **automatically classifying** them against any policy, rule, or regulation, including Records Authorities. It then adds metadata to its information asset register to classify the content as being related to a certain Function, business unit, key project, or topic for example, and **tracks its retention period**, triggering an alert for disposal when it comes due. **Disposal** can then be managed via Castlepoint, capturing a disposal certificate. Castlepoint also automatically determines the correct **security classification** for every item, and can **push the correct label** to the source system. This process is fully automated and does not require any user action or input, or any specific behaviour by users (such as only saving certain files in certain locations).

Castlepoint provides record-based out-of-the-box **reporting** across date and time, disposition, ontology, and user groupings. Castlepoint provides much more comprehensive reporting on records, sentencing, users, classified records, sensitive content, and audit events than is available via most source system interfaces. The system also shows activity on records, and systems, over time. Castlepoint records and maintains extensive audit information on all actions on documents and records from standard events such as Adding and Updating, to extended events like changing security markings and sharing documents.

All data within Castlepoint is exportable and can be downloaded for additional processing.

How the system is differentiated

Castlepoint is fast to deploy on premises or in any cloud, and does not create technical debt through integration, customisation, or data duplication or modification. It is a secure, manage-in-place SaaS solution, which is invisible to general users, has no impacts on source systems, source data, or the governance team, and achieves compliance across any line of business system without using agents or connectors.

Full coverage of all data

Castlepoint manages the whole information security and GRC domain (discovery, audit, privacy, cyber, GenAI governance, and records management) in a single platform. It manages all systems, including legacy and bespoke applications, and all data formats, on premises and in the cloud (and we can deploy on premises or airgapped if required).

No impacts on the organisation

Castlepoint is invisible to general users and does not require any change in behaviour (such as using labels, metadata, naming conventions, or file plans), or cause any changes in their normal experience in their own source systems such as M365. Compliance is invisible and automated.

Castlepoint does not move, modify, or copy data. It is a manage-in-place solution that does not affect data integrity or security.

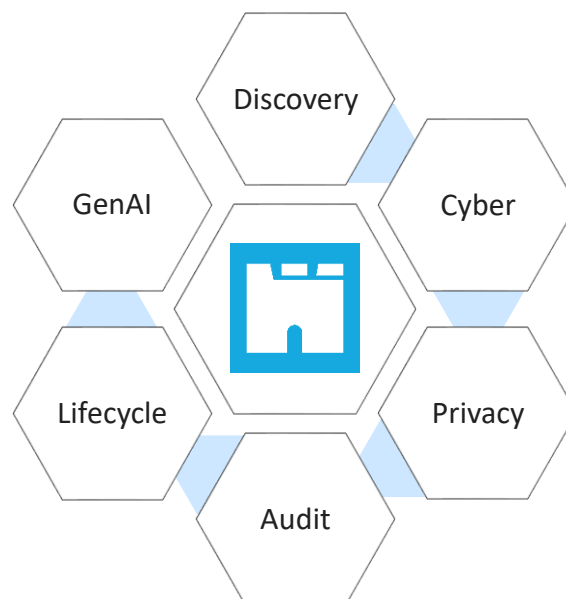
Castlepoint does not hamper network performance, and it does not require agents or connectors to be installed on source systems in order to manage them. This mitigates the key cascading technology risk of tightly coupled systems integration, ensuring that source system supportability, sustainability, user experience, and security are not affected.

Castlepoint does not place a burden on governance teams, as it does not require them to curate training data, supervise a Machine Learning system, write rules or rules engines, or create and maintain file plans.

Autoclassification with Ethical AI

New regulation requires decisions made or recommended by machines to be fully transparent and auditable. Unlike closed-box AI systems such as traditional Machine Learning, Castlepoint is an Ethical AI. The classification is accurate, transparent, explainable, and contestable, and shows exactly why a decision was reached.

Key Castlepoint capabilities



Castlepoint includes the following capabilities as part of the standard license:

- **eDiscovery**

Castlepoint's powerful eDiscovery gives you visibility of all your data in all your systems through a single pane of glass. Search content and metadata of any file or database, in any system, on-premises or in the cloud, with no business or system impacts. Castlepoint registers billions of data points and facets from your network in its own, secure database. It captures all the properties of your documents, database entries, mail, social, and web content, as well as all the topics and people discussed in them. Search includes metadata, properties, full text, key phrase, named entity, topic and taxonomy, function, security classification, sensitive data, trends, events, formats, date, and location, for example. Castlepoint includes compliant ESI controls for legal hold and export for subject and data access requests.

- **Privacy Management**

Castlepoint's privacy management capability helps you to effectively minimise your sensitive personal information holdings, respond rapidly and accurately to information requests, and properly protect PII, PCI, and PHI. Castlepoint rapidly returns results from billions of data points to find every mention of an individual, in documents, databases, mailboxes, personal drives, and chats. It also shows audit events on personal information, and alerts to potential non-conformances.

Castlepoint automatically detects identifying information, including names, contact details, and government-issued IDs, and sensitive personal information such as criminal history, medical conditions, and other protected characteristics. It alerts when this information is captured into the environment and triages the risk, with a tracking interface to manage remediation. Castlepoint audits all events on the information, and automatically sentences it, so that you know when it needs to be disposed of to meet your data minimisation obligations.

- **Security Management**

Castlepoint is a command and control AI that gives you the high ground over your risk. Castlepoint brings together the full story of an operation, asset or individual across the whole enterprise and over all time, so you can see what you have, where it is, and who is doing what to it. Castlepoint can determine whether something is sensitive, risky, classified, or subject to secrecy provisions under law, without needing to rely on metadata or labels. Castlepoint detects and alerts on risky data, anywhere it is stored, including risk specific to your context such Intellectual Property or controversial work streams. Castlepoint recommends the appropriate security marking, and can push this label to Purview, for example, to apply DLP controls in downstream systems.

- **Records Management**

With automatic registration, classification, sentencing, and compliant disposition of records across the enterprise, Castlepoint makes any information system fully compliant with all parts of ISO 16175 (2 and 3), ISO 15489, ISO 230811 and additional policies and standards recommended by Archives.

Records stay in their source system, with no duplication or modification. Accuracy is benchmarked over 98%, and our AI is fully transparent and traceable (with no 'closed box' hiding the reasoning for the classification). Disposition options include export for compliant long-term archiving or transfer, as well as compliant destruction. Castlepoint supports use of 'Virtual Records' that span different locations, bringing different items across the network together into one virtual aggregation for appraisal and sentencing.

- **Audit and monitoring**

As well as capturing all the properties of items and records across the network, and analysing and classifying their content, Castlepoint also captures their event history. Available events are captured on all managed data, by all users, and across all systems, tracking and alerting when high-risk or high-value content is created, modified, or moved. Castlepoint's sensitive data signaling helps prevent breaches and spills, and respond better and faster to incidents.

- **Generative AI Governance**

Castlepoint helps prepare for Copilot and other GenAI, protect your sensitive content from surfacing, and monitor and report on outputs of AI use in your organisation.

Castlepoint knows your data, so that you can control the quality and security of content ingested and used in your Generative AI rollout. Castlepoint reviews and assigns an accurate legal retention period to all your legacy content, so that you can dispose of outdated information that's no longer valid, or otherwise exclude it from your GenAI scope.

Castlepoint finds and flags risky and controversial information in your data set, both before deploying GenAI and throughout its use, so that you can clean up or automatically apply accurate security labels to sensitive information before it ends up in a GenAI search result.

And Castlepoint audits who is using GenAI, and where their results are coming from, so that you can maintain effective oversight.

Hosting services

Castlepoint is a containerised solution and can be deployed in a customer-owned and managed cloud, on customer premises, airgapped, or in our SaaS platform.

Technical requirements

Castlepoint is deployed and available to you via a supported web browser. In the SaaS Hosting model, we deploy and manage the platform. You are required to provide:

- Software service account(s) with Read-Only access to system(s) in scope
- If connecting to a non-OOTB supported system, any available documentation
- Network connectivity between your data and the SaaS environment

Castlepoint integrates with TLS v1.2 or TLS v1.3 certificates between your environment and Castlepoint. Your network security configuration must support TLS v1.2 or TLS v1.3 to access Castlepoint.

Backup and restore

Castlepoint hosts on globally recognised tier-one hosting service provider platforms. When hosting, Castlepoint develops the back-up schedule, performs scheduled back-ups, provides routine and emergency data recovery, and manage the archiving process. In the event of data loss, Castlepoint provides recovery services to try to restore the most recent back-up.

Business continuity and disaster recovery

Castlepoint maintains a Business Continuity Plan and Disaster Recovery Procedure. The BCP and DRP are regularly tested.

Maintenance and updates

The technologies underpinning the Castlepoint solution require a schedule of maintenance to ensure they are operating effectively, securely and meeting client requirements. As such, we provide regular support and maintenance as part of our licensing model.

Castlepoint licensing includes regular maintenance and updates, including security patches, product updates, and continuous enhancements. Castlepoint manages software upgrades/patching according to the maintenance processes within the constraints of your change freezes as required. New releases are deployed frequently, including new features. The schedule for upgrades is planned with your Change Advisory Board and follows your

change control processes. Note that critical vulnerabilities in the operating system are patched within 48 hours.

Maintenance and support hours are included in the Castlepoint license fee. Support and maintenance requested in addition to the capped amounts is charged at hourly rates.

There is no license charge for use on development, test, and DR networks if the production license is current and active. Support and maintenance are not included for development and test networks but can be provided if requested at our agreed rates.

Service levels

Castlepoint uses all commercially reasonable efforts to provide 99.9% availability for the Castlepoint Software.

Availability is measured monthly as a monthly uptime percentage, in which uptime is service availability and downtime is periods where the system is not available, outside a planned outage window.

Downtime does not include outages or interruptions caused by the Customer network or systems configurations, the cloud hosting service, natural disasters or other unavoidable interruptions, security breaches not caused by Castlepoint, or by deliberate misuse of the Castlepoint System.

Support services

Castlepoint software is supported by us, remotely, and includes product updates, enhancements, and security patches. We also supply professional services as required, including for adding new systems, updating or adding ontologies, developing new specific reports or graphs, and for assistance with records management.

Castlepoint's support portal also provides a Help Centre accessible online for your staff. The Help Centre provides a comprehensive suite of knowledge articles for all capabilities we provide to your organisation. The support portal is a key resource for first, second and third level support.

All our processes conform to our ISO 9001 Certified Quality Management System (including our documented procedures), our statutory and regulatory obligations, best-practices where applicable, and the requirements of our stakeholders.

Customer success and training

All enterprise clients are assigned a dedicated Account Manager, who meets regularly with your team to ensure that your organisation is able to make full use of the system capabilities and works collaboratively to plan future enhancements and changes based on your evolving needs. The Castlepoint Customer Success Manager oversees a team of Subject Matter experts, including qualified records managers, privacy and security managers, and trainers, who provide support as needed with all aspects of information governance and system use.

We provide a range of delivery modalities including instructor-led classroom-based and virtual instructor-led classroom based for remote attendance; seminar-style for larger groups and webinars for remote groups; power user training for support staff and “champions” of new technology, as well as e-learning and pre- and post-training assessment.

SLA management

We provide full support for our clients. Following implementation, you can interact with our support resources during our support hours (standard business days 8am - 6pm) with extended support by arrangement. We also provide a Freshdesk Support portal for use by our clients, available at all times. Freshdesk provides integrated process management for:

- Incident and problem resolution
- Change control
- Configuration management
- Knowledge management

Our support portal provides multiple channels for support, including:

- Dedicated support email account
- Support Request portal
- Business hours phone support.

The support portal also provides a Help Centre accessible online for your Level 1 staff. The Help Centre provides a comprehensive suite of knowledge articles for all capabilities Castlepoint provides to your organisation. The support portal is a key resource for first, second, and third level support.

We maintain SLAS for P1, P2, and P3 tickets with documented definitions, response times, and resolution times.

Security management

Castlepoint supports role-based security, single sign on, and access models and associated systems including ADFS, Azure Active Directory, Oath 2 SAML and OIDC integration. Clients can integrate the authN/authZ flow, including onboarding and offboarding, with their own infrastructure and manage RBAC configuration via security groups. Castlepoint SaaS supports Microsoft Azure Active Directory for secured authentication and authorisation. Castlepoint can be configured to authenticate with your Microsoft Azure Active Directory, or one can be provided to you as part of the deployment.

All data is encrypted. Data in transit is TLS v1.2 or 1.3 (depending on network support). Data at rest is AES 256.

Castlepoint is developed in accordance with the Open Web Application Security Project's (OWASP) Secure Coding Practices, and we continuously scan our application images for security vulnerabilities. We adhere to applicable legal, statutory, and regulatory compliance obligations. Castlepoint's Security Management System is ISO 27001 certified.

Pricing

Castlepoint is licensed per network, so no matter how many users, systems, or records you have, Castlepoint is a flat cost to own and run. You can use it on as many systems, across as much data, and for as many users as you want to, without incurring any extra charges.

We do not charge by number of records managed, number of users, number of systems managed, number of capabilities used, or any other volume pricing. There are no extra costs for autoclassification AI or other features. Pricing is determined by your organisation's headcount, and the subscription includes support and sustainment by our expert resources, with regular meetings and monthly SLA reporting, as well as a dedicated account and contract manager. Hosting charges from Azure are passed through to you. The product is kept evergreen by us, with no charge for updates or upgrades.

Importantly, as Castlepoint is invisible to general users, and they do not have to change their processes or workflows in any way, training cost is minimal, required only for the governance team. The subscription includes:

- An enterprise license to use the software on a single production network.
- Monthly maintenance, system checks, patching, and upgrades as required
- User and administrator support as required.