Crown Commercial Service *Supplier*

G-Cloud 15

Ransomware Data Protection powered by Rubrik

Atos

Table of contents

Crown Commercial Service Supplier

Atos

1. What is the Ransomware Data Protection Service powered by Rubrik?

The Atos Ransomware Data Protection (Ransomware) Managed Service uses Rubrik's zero-trust platform to deliver immutable backups, air-gapped from the production environment, along with disaster recovery workflows to ensure data resilience and minimise downtime.

Addressing NCSC guidelines for cyber-resilience, Atos hardens its hybrid infrastructure against emerging threats, such as ransomware, while enabling continuous data observability and rapid recovery of files and applications.

Backed by a 24x7 SOC, the service combines proactive monitoring to ensure backup compliance, detect anomalies, analyse risk patterns and expedite failover procedures with recovery to uphold data integrity across disruptions. This means public sector organisations can recover rapidly from outages or breaches to an operational state.

Crown Commercial Service Supplier

Atos

2. What does it deliver?

Atos' Data Security (Ransomware) Managed Service powered by Rubrik is a comprehensive, managed solution designed to safeguard public sector organisations against the growing threat of ransomware attacks.

Leveraging advanced technology from Rubrik, the service provides a multi-layered approach to data protection, enabling organisations to maintain the integrity and availability of their critical data assets in the face of increasingly sophisticated cyber threats.

Key aspects of the service include:

1. **Immutable backups:** public sector organisation data is stored in an immutable format, preventing ransomware from accessing and encrypting the backups.
2. **Rapid recovery:** in the event of an attack, the service enables fast recovery to the most recent clean state, minimising downtime.
3. **Ransomware monitoring and investigation**: using machine learning, the service determines the scope of ransomware attacks by detecting deletions, modifications and encryptions. This provides granular visibility, reducing data loss.
4. **Threat hunting:** The service analyses historical backup data to pinpoint when indicators of compromise first appeared in the environment. This helps avoid reinfection during the recovery process.
5. **Clean state restoration:** By identifying the most recent uninfected snapshots, the service facilitates the restoration of data to a clean, ransomware-free state.
6. **Sensitive data monitoring:** for the Enterprise edition, the service also discovers, classifies and reports on sensitive data to help manage exfiltration risk and comply with regulations.

The Data Security Managed service is delivered through a tiered model with Foundation, Business and Enterprise editions, each providing an increasing level of capabilities. Overall, it takes a proactive, multi-faceted approach to defending against ransomware and enabling public sector organisations to recover quickly in the event of an attack.

By combining cutting-edge technology, proactive threat detection and rapid recovery capabilities, Atos' Ransomware Data Protection service empowers organisations to defend against the ever-present threat of ransomware.

With this comprehensive, managed solution in place, public sector organisations can maintain the confidentiality, integrity and availability of their critical data assets, ensuring business continuity and resilience in the face of evolving cyber threats.

Crown Commercial Service Supplier

Atos

3. What technology does it use?

Atos' Data Security (Ransomware) Managed Service is built on the foundation of Rubrik's cutting-edge data security and management platform.

Rubrik's technology is designed from the ground up with a focus on simplicity, scalability and resilience, making it an ideal choice for organisations seeking to protect their critical data assets from the ever-growing threat of ransomware attacks.

At the core of the Data Security (Ransomware) Managed service is the creation of immutable backups. By storing public sector organisation data in an unalterable format, the service ensures that even if ransomware manages to infiltrate an organisation's primary systems, the backups remain secure and untouched. This immutability is achieved through a combination of logical air-gapping, encryption and strict access controls, preventing ransomware from accessing or encrypting the backed-up data.

In the event of a successful ransomware attack, the Data Security (Ransomware) Managed service enables rapid recovery, minimising downtime and data loss. The service leverages Rubrik's advanced data management capabilities to quickly identify and restore the most recent clean state of the data, before the ransomware infection occurred. This allows public sector organisations to resume normal operations with minimal disruption, reducing the financial and reputational impact of the attack.

To proactively detect and investigate ransomware activity, the service employs cutting-edge machine learning algorithms. These algorithms continuously monitor data across the public sector organisation's environment, identifying suspicious deletions, modifications and encryptions that may indicate a ransomware attack is in progress. By providing granular visibility into these anomalous activities, the service enables security teams to quickly investigate and respond to potential threats, reducing the scope and severity of any data loss.

In addition to real-time monitoring, the Data Security (Ransomware) Managed Service also includes powerful threat hunting capabilities. By analysing historical backup data, the service can pinpoint the exact moment when indicators of compromise (IoCs) first appeared in the environment. This intelligence is invaluable in identifying the root cause of an attack and ensuring that all traces of the ransomware are eliminated during the recovery process, preventing reinfection.

When recovering from a ransomware attack, the Data Security (Ransomware) Managed service ensures that public sector organisations are restoring their data to a clean,

malware-free state. By leveraging Rubrik's robust data management and version control capabilities, the service can identify the most recent uninfected snapshots of the data before the ransomware takes hold. This allows organisations to confidently restore their systems and data, knowing that they are not inadvertently reintroducing the malware.

The Data Security (Ransomware) Managed service is delivered through a tiered model, offering three distinct editions to meet the diverse needs and budgets of organisations:

1. Foundation Edition: provides the core data protection and recovery capabilities, including immutable backups and rapid restore functionality
2. Business Edition: builds upon the Foundation Edition, adding ransomware monitoring and investigation features, as well as expanded recovery options
3. Enterprise Edition: offers the full suite of capabilities, including sensitive data monitoring, advanced threat hunting and additional data recovery features.

		Platform	Security	Enhanced Security
		Foundation Edition (FE)	Business Edition (BE)	Enterprise Edition (EE)
Data Resilience	**Enterprise, Cloud and SaaS Protection** Cyberproof your enterprise data with air-gapped, immutable, access-controlled backups	✓	✓	✓
	Rubrik Cloud Vault Secure and archive your most valuable data with a cloud data vault with the next level of immutability	10TB (Backup Tier)	10TB (Backup Tier)	200TB (Backup Tier)
	M365 Protection-as-a-Service Where MSP manages the backup process for the customer - M365 based on a pre-determined set of retention periods and SLAs	Option	Option	Option
	Archival-as-a-Service Where MSP helps organisations unlock cost-effective, scalable data archiving across hybrid cloud environments. (cold storage for long-term storage)	Option	Option	Option
Data Observability	**Ransomware Monitoring and Investigation** Determine the scope of the ransomware attacks, using high fidelity machine learning to detect deletions, modifications and encryptions		✓	✓
	Sensitive Data Monitoring and Remediation Reduce sensitive data exposure and manage exfiltration risk by discovering what types of sensitive data you have, where it lives and who has access to it			✓
	Threat Monitoring and Hunting Reduce sensitive data exposure and manage exfiltration risk by discovering what types of sensitive data you have, where it lives and who has access to it			✓

		Platform	Security	Enhanced Security
		Foundation Edition (FE)	Business Edition (BE)	Enterprise Edition (EE)
Data Recovery	**Mass Recovery** Restore business operations quickly by recovering apps, files or users at scale.	✓	✓	✓
	Threat Containment Ensure safe and quick data recovery by quarantining data infected by malware.			✓
	Orchestrated Application Recovery Recover applications quickly with pre-built workflows and disaster recovery blueprints			✓
	Data Security Command Centre Identify Security gaps, quantify data risk, and provide actionable recommendations to improve data security posture	✓	✓	✓
	Cloud Data Protection Cyberproof your cloud data with air-gapped, immutable, access-controlled backups	Universal Cloud Licences		

For public sector organisations subscribing to the Enterprise Edition of the Data Security (Ransomware) Managed service, Atos also provides advanced capabilities for monitoring sensitive data. The service can discover, classify and report on an organisation's sensitive data assets, such as personally identifiable information (PII), protected health information (PHI) and financial data.

This visibility is critical in managing exfiltration risk, as it allows organisations to understand where their most valuable data resides and who has access to it. Additionally, the sensitive data monitoring capabilities help organisations maintain compliance with relevant data protection regulations, such as NCSC, GDPR, and PCI-DSS.

By combining cutting-edge technology, proactive threat detection and rapid recovery capabilities, Atos' Data Security (Ransomware) Managed service empowers public sector organisations to defend against the ever-present threat of ransomware. With this comprehensive, managed solution in place, organisations can maintain the confidentiality, integrity and availability of their critical data assets, ensuring business continuity and resilience in the face of evolving cyber threats.

Service Benefits

Atos' Data Security (Ransomware) Managed service provides public sector organisations with several key benefits to enhance their ransomware defence and ensure data resilience:

- Enhanced data protection through immutable backups
- Rapid recovery and minimised downtime in case of an attack
- Proactive threat detection using advanced machine learning algorithms
- Comprehensive threat intelligence through powerful threat hunting capabilities
- Restoration to a clean state by identifying uninfected data snapshots
- Sensitive data visibility and compliance (Enterprise Edition)
- Scalability and flexibility to maintain protection as data volumes grow
- Expert support and management from Atos' security professionals
- Improved overall security posture by addressing ransomware threats head-on
- Peace of mind and ensure business continuity in the face of cyber attacks.

This service empowers organisations to strengthen their cybersecurity defences, safeguard valuable data assets and maintain resilience in today's challenging business landscape.

Business Benefits

Atos' Data Security (Ransomware) Managed service delivers key business benefits and outcomes that help organisations operate effectively, maintain customer trust and drive growth while facing cyber threats. By implementing this ransomware defence solution, businesses can:

- Ensure business continuity: the service minimises downtime from ransomware attacks, allowing organisations to resume critical operations quickly and maintain productivity.
- Mitigate financial losses: swift restoration of systems and data helps minimise financial impacts, such as lost revenue and recovery costs.
- Protect customer trust and brand reputation: demonstrating a commitment to data security and resilience strengthens customer confidence and differentiates businesses from competitors.
- Maintain regulatory compliance: sensitive data monitoring capabilities (Enterprise Edition) help public sector organisations comply with data protection regulations, avoiding penalties and legal consequences.
- Support digital transformation: the service's cloud-native design and scalability secure digital transformation initiatives, enabling innovation and growth.

- Enhance decision-making and risk management: proactive threat detection and intelligence provide insights for informed decision-making and effective risk management strategies.
- Reduce the burden on IT and security teams: Atos' managed services allow internal teams to focus on strategic initiatives and core business objectives.
- Enable scalability and business growth: the flexible and scalable architecture supports business growth without being constrained by security concerns.
- Improve operational efficiency: streamlined data protection and recovery processes reduce manual effort and minimise human error, driving productivity gains.
- Strengthen overall security posture: implementing a comprehensive ransomware defence solution elevates the overall security posture, protecting against threats and demonstrating a commitment to data security.

By delivering these benefits and outcomes, Atos' Data Security (Ransomware) Managed service empowers organisations to operate confidently in the face of ransomware threats, ensuring business continuity, mitigating losses, protecting customer trust and supporting growth and innovation.

Crown Commercial Service *Supplier*

Atos

4. What terms apply?

To the fullest extent permitted under G-Cloud 15 Framework Agreement and the Call-Off Contract, Atos will provide the Services in accordance with the Atos Supplier Terms (which will include, but may not be limited to , the Supplier Acceptable Use Policy, Supplier Data Processing Agreement, Supplier Specific Shared Responsibility Model, Supplier SLAs and Supplier Licence Terms and any applicable Third-Party Terms outlined in this Service Description document and the Order Form) and this Service Description document.

For clarity:

- Atos Supplier Terms may be modified in accordance with the provisions of the Call-Off Contract, and remain effective except where expressly overridden.
- Hyperlinks included in the Atos Supplier Terms and Service Description document remain effective where they point to Atos' or the relevant Third-Party Terms or documents. Should a hyperlink cease to function, Atos will work with the client to update it through the agreed procedure.

Crown Commercial Service *Supplier*

Atos

5. Termination

Termination shall be in accordance with:

- The G-Cloud 15 Framework terms and conditions
- Any terms agreed within the Order Form of the relevant Call-Off Contract
- For this specific service, by default Atos ask for at least thirty (30) days prior written notice of termination without cause.

Atos commits to the continued provision of services for the duration of the Call-Off Contract subject to the terms and conditions of the G-Cloud 15 Framework Agreement, the Call-Off Contract, the Atos Supplier Terms and the applicable Third Party Agreements (as defined in the Atos Supplier Terms and indicated in the Order Form) related thereto.

Crown Commercial Service *Supplier*

Atos

6. How do I order?

Please contact our team at: gcloud@atos.net

- We will prepare a quotation for your review, including any applicable volume discounts.
- Once the quotation is agreed, we will issue the necessary documentation (as required by the G-Cloud Framework) and request a purchase order from you.
- Upon receipt of your purchase order, we will configure the services in line with the agreed requirements. Where applicable, you will also receive access to our self-service portal to begin provisioning services.
- If you are a new customer, you may need to complete additional 'new supplier' forms.
- Invoices will be issued to you and to Crown Commercial Service (CCS), quoting the purchase order number, for the services procured.
- We will also submit the required monthly management information reports to Government Procurement.

Crown Commercial Service *Supplier*

Atos

7. Glossary

Term	Definition
CAF	Cyber Assessment Framework
GDPR	General Data Protection Regulation
IOC	Indicators of Compromise
NCSC	National Cyber Security Centre
MCSS	Minimum Cyber Security Standards
PCS-DSS	Payment Card Industry Data Security Standard
PHI	Protected Health Information
PII	Personally Identifiable Information

Crown Commercial Service *Supplier*

Atos

8. Why Atos

Atos has been a trusted partner on every G-Cloud iteration since the framework began, helping public sector organisations modernise with confidence. We combine global expertise with deep UK experience, delivering secure, scalable cloud solutions that meet the highest government standards.

As Europe's leading provider of cloud and cybersecurity services, Atos offers end-to-end capabilities - from migration and hosting to SaaS and consultancy - supported by UK delivery centres and strategic partnerships with hyperscalers.

Our focus on innovation, sustainability, and social value ensures that customers not only achieve operational excellence but also contribute to a greener, fairer future. With Atos, you gain a proven partner committed to driving efficiency, resilience, and transformation across public service.

About Atos

Atos Group is a global leader in digital transformation with c. 67,000 employees and annual revenue of c. €10 billion, operating in 61 countries under two brands — Atos for services and Eviden for products. European number one in cybersecurity, cloud and high-performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is the brand under which Atos SE (Societas Europaea) operates. Atos SE is listed on Euronext Paris.

The purpose of Atos Group is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Learn more at: atos.net

105043-RR