

Service name

Ultima Rubrik

Edit

- **About your service**

Service description

Rubrik provides a zero trust data protection platform across all data and applications whether it be located on premises or in the public, private or hybrid cloud. Rubrik provides Ransomware detection and remediation, Sensitive Data Discovery, Incident containment and Orchestrated Application Recovery all within a single management plane.

Edit

Service categories

- Application Development and Deployment
 - Analytics and business intelligence
 - Business Intelligence
 - Business Intelligence
 - Advanced and predictive analytics
 - Advanced and predictive analytics

Edit

Multi cloud support

Yes

Edit

- **Service features and benefits**

Service features and benefits**Service features**

- Backup data on premises, across multi cloud and SaaS environments.
- Instantly recover data and applications locally or within the cloud.

Service benefits

- Assured Recoverability against ransomware via a Zero Trust immutable platform.
- Detect, Identify and Remediate against Ransomware.
- Database and Unstructured Data Protection at Scale.
- Policy Based Automation for simplicity of management.
- Rapid Recovery of services at Scale.
- Orchestrated Recovery of applications and Services.
- Single SaaS platform extending from data center to cloud.
- Provide intelligence and compliance via sensitive data discovery.
- Meet and Exceed NCSC and NIST compliant data protection strategies.
- Provide a secure by design air gapped environment.

Edit

- **Service scope**

Add-ons and extensions**Software add-on or extension**

No

Trustmarque Solutions Limited

Registered in England and Wales | Registration number: 02183240 | VAT number: GB434530809

Registered Office: Marlborough House Westminster Place, York Business Park, York. YO26 6RW

+44 (0) 845 2101 500 | info@trustmarque.com | www.trustmarque.com

Edit

Cloud deployment model

- Public cloud
- Private cloud
- Community cloud
- Hybrid cloud

Edit

Service constraints

On premises deployment requires specific hardware and/or resource configurations.

Edit

System requirements

Customer provided networking.

Edit

- **Reselling**

Supplier type

Supplier type

I'm a reseller providing extra features and support not available from the original supplier

Organisation whose services are being resold

Rubrik

Edit

- **User support**

Email or ticketing support

Email or online ticketing support

Yes

Support response times

P1 system down SLA within 30 minutes P4 query next business day SLA.

User can manage status and priority of support tickets

Yes

Online ticketing support accessibility

None or don't know

Edit

Phone support

Phone support

Yes

Phone support availability

24 hours, 7 days a week

Edit

Web chat support

Web chat support

No

Edit

Onsite support

Yes

Edit

Support levels

Premium - 24x7x365 follow the sun support Basic - Mon-Fri 8am-8pm (local time) optional Customer Experience Manager (cost uplift).

Edit

Support available to third parties

Yes

Edit

- **How users work with your service**

Browsers

Web browser interface

Yes

Supported browsers

Chrome

Edit

Installation

Application to install

No

Edit

Mobile

Designed for use on mobile devices

No

Edit

Service interface

Service interface

Yes

Description of service interface

CLI based support interface for Rubrik Support personel - enabled by customer via a secure support tunnel.

Accessibility standards

None or don't know

Description of accessibility

Via Web Browser, cli or API.

Accessibility testing

N/A

Edit

User support

User support accessibility

None or don't know

Edit

API

API

Yes

What users can and can't do using the API

Any function within Rubrik can be accessed via API's.

API documentation

Yes

API documentation formats

- Open API (also known as Swagger)
- HTML

API sandbox or test environment

Yes

Edit

Customisation

Customisation available

No

Edit

- **Onboarding and offboarding**

Getting started

Install Skills Transfer Handover via Professional Services Online Free training via Rubrik University Classroom/virtual training with certifications.

Edit

Documentation

Service documentation

Yes

Documentation formats

- HTML
- PDF

Documentation accessibility standard

None or don't know

How the documentation is accessible

Via Support portal

Edit

End-of-contract data extraction

VIA natural Expiration or manual migration via professional Services

Edit

End-of-contract process

Customer has recovery only capabilities with no support on product or services. For Rubrik hosted services, customer will have set amount of days to expire/export

Edit

- **Data importing and exporting**

Data export approach

Multiple export options available via Rubrik interface and chosen cloud storage provider.

Edit

Data export formats

Data export formats

Other

Other data export formats

N/A

Edit

Data import formats

Data import formats

Other

Other data import formats

N/A

Edit

- **Analytics**

Metrics

Service usage metrics

Yes

Metrics types

SLA compliance metrics backup and restore uptime and capacity

Reporting types

- Through an API
- Real-time dashboards
- Regular reports
- Reports on request

Resource tagging

No

FOCUS resource tagging

No

Edit

- **Scaling**

Independence of resources

Through an intelligent and automated task scheduler managed via SLA policies

Edit

- **Public sector networks**

Public sector networks

Connection to public sector networks

Yes

Connected networks

- Public Services Network (PSN)
- Police National Network (PNN)
- Joint Academic Network (JANET)
- Scottish Wide Area Network (SWAN)
- Health and Social Care Network (HSCN)

Edit

- **Data-in-transit protection**

Protection between networks

Data protection between buyer and supplier networks

TLS (Version 1.2 or above)

Edit

Protection within your network

Data protection within supplier network

TLS (Version 1.2 or above)

Edit

- **Asset protection**

Data storage and processing locations

Knowledge of data storage and processing locations

Yes

Data storage and processing locations

- United Kingdom
- European Economic Area (EEA)

User control over data storage and processing locations

Yes

Edit

Datacentre security standards

Managed by a third party

Edit

Penetration testing

Penetration testing frequency

At least every 6 months

Penetration testing approach

'IT Health Check' performed by a CHECK service provider

Edit

Protection of data at rest

Protecting data at rest

Encryption of all physical media

Edit

Data sanitisation process

Data sanitisation process

Yes

Data sanitisation type

Explicit overwriting of storage before reallocation / Secure Erase

Edit

Equipment disposal approach

In-house destruction process

Edit

- **Availability and resilience**

Guaranteed availability

N/A

Edit

Approach to resilience

Various hardware and software resiliency - details available on request.

Edit

Outage reporting

Yes - public stats

Edit

- **Governance**

Named board-level person responsible for service security

Yes

Edit

Security governance

Software Security Code of Practice

Yes

Security governance certified

Yes

Security governance standards

ISO/IEC 27001

Edit

Information security policies and processes

ISO 27001 ISO 20000 EU/US Privacy Shield EU GDPR SSAE 16 SOC 2 US HIPAA US CJIS UK ICO

Edit

- **Operational security**

Configuration and change management standard

Complies with a recognised standard, for example CSA CCM v4.0 or SSAE-18 / ISAE 3402

Edit

Configuration and change management approach

Rubrik has a set standard and processes for configuration and change management which can be provided on request

Edit

Vulnerability management type

Supplier-defined controls

Edit

Vulnerability management approach

Rubrik performs ongoing and constant reviews of its infrastructure and services as well as maintaining a trained staff within InfoSec and Compliance. Details of this can be provided on request

Edit

Protective monitoring type

Supplier-defined controls

Edit

Protective monitoring approach

Rubrik provides regular and proactive monitoring processes. Details of which can be provided on request

Edit

Incident management type

Supplier-defined controls

Edit

Post-quantum cryptography secure

No

Edit

Incident management approach

Rubrik has a full set of IM and RCA processes. Details of these can be provided on request.

Edit

- **Staff security**

Staff security clearance

Staff screening performed but doesn't conform with BS7858:2019

Edit

Government security clearance

Up to Developed Vetting (DV)

Edit

- **Secure development**

Approach to secure software development best practice

Independent review of processes (for example CESG CPA Build Standard, ISO/IEC 27034, ISO/IEC 27001 or CSA CCM v4.0)

Edit

- **Identity and authentication**

User authentication

User authentication needed

Yes

User authentication

- Multi-Factor Authentication (MFA)
- Public key authentication (including by TLS client certificate)
- Identity federation with existing provider (for example Google apps)
- Limited access over government network (for example PSN)
- Dedicated link (for example VPN or bonded fibre)
- Username or password

Edit

Access restrictions in management interfaces and support channels

Rubrik uses MFA and biometric credentials for authentication to applications and baseline access is provisioned via RBAC and internal approvals (break glass) processes

Edit

Access restriction testing frequency

At least every 6 months

Edit

Management access

Management access authentication

- Multi-Factor Authentication (MFA)
- Public key authentication (including by TLS client certificate)
- Identity federation with existing provider (for example Google apps)
- Limited access over government network (for example PSN)
- Dedicated link (for example VPN or bonded fibre)
- Username or password

Edit

- **Audit information for users**

Audit for buyers' users' actions

Access to user activity audit information

Users have access to real-time audit information

How long user audit data is stored for

Between 6 months and 12 months

Edit

Audit for suppliers' users' actions

Access to supplier activity audit information

Users contact the support team to get audit information

How long supplier audit data is stored for

Between 6 months and 12 months

Edit

How long system logs are stored for

User-defined

Edit

- **Pricing**

Discount for educational organisations

Yes

Edit

Free or trial versions

Free trial available

Yes

Description of free trial

Please contact us for further information.