LOGICALIS
Architects of Change

Rubrik Cloud Data Protection, Security & Management

Service Description

May 2024

G-Cloud 14

Table of Contents

Rubrik Cloud Data Protection, Security & Management

Logicalis and our partner Rubrik provide a single software platform that delivers backup, instant recovery, archival, search, analytics, compliance, and copy data management in one secure fabric across data centers and clouds.

Clients are able to deploy one or more components, layering on additional features as and when required, the CDM platform is broken down into a number of solution areas.

Cloud Data Protection

Modern Data Protection for the Cloud

A native data protection solution to automatically discover, protect, organize, and manage all your data and apps on multiple clouds through a singular, easy-to-use view. Rubrik delivers SaaS backup and recovery to keep your cloud data safe, enhancing data availability for greater resilience and recovery confidence.

HOW IT WORKS AUTHORIZE

AUTHORIZE Rubrik with your cloud in a few clicks using the automated setup workflow. Requiring only the minimal set of permissions needed, Rubrik will auto-discover all VMs in configured accounts, allowing users to specify which accounts and regions to manage.

CONFIGURE Use our single SLA policy engine to automatically create and expire snapshots to suit your backup and replication requirements. If file recovery is needed, Rubrik automatically spins up a single lightweight node in the cloud which is powered down once complete, minimizing consumption of cloud compute resources.

PROTECT Backups are automatically stored in elastic cloud storage so that users can efficiently scale protection in-line with cloud service consumption. Use incremental forever backups to drive capacity and network savings. All cloud-native data can be automatically indexed, delivering instant access and fast recovery with global predictive search. Users simplify management across hybrid cloud with a single Rubrik UI for cloud-native and on-premises applications. Use Rubrik on-premises or in the cloud to automatically backup and recover cloud-native VMs. With global predictive search, perform file-level restores in the event of a corrupt or missing config file without rolling back your entire system

Office 365

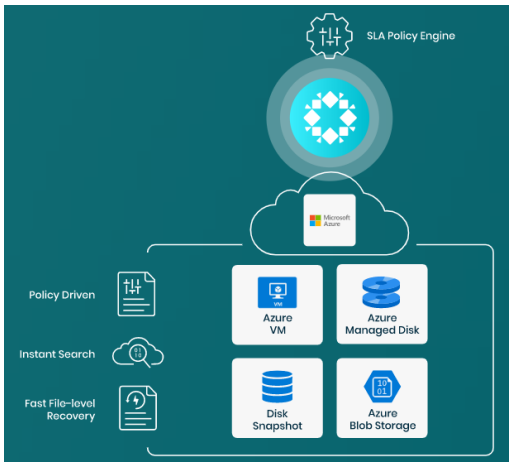
https://www.rubrik.com/en/solutions/office-365

AWS

https://www.rubrik.com/en/solutions/aws-native-protection

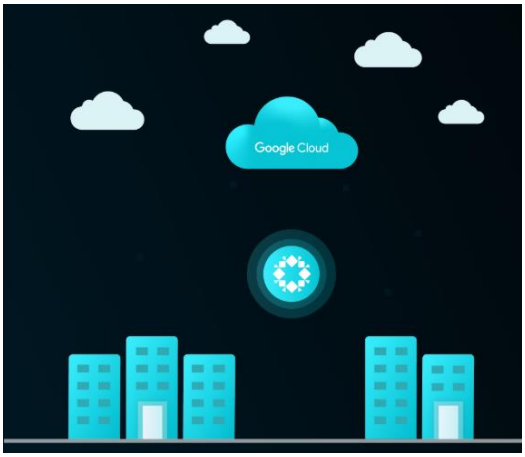
Azure

https://www.rubrik.com/en/solutions/Azure-Native-Protection



Google Cloud Platform

https://www.rubrik.com/en/partners/technology-partners/google-cloud-platform



Polaris Radar (Ransomware protection)

Polaris Radar uses data analysis to diagnose threat impacts quickly by using historical data trends and

filesystem behavioural models to perform anomaly detection. A data lake is used to store the results for further analytics and analysis by custom trained machine learning models developed uniquely for each customer over time. By using intelligence to analyses behavioural patterns through machine learning algorithms, Radar is able to detect ransomware quickly and efficiently using a simplified KNN classifier algorithm for better intelligence instead of basic stats. This model is used to baseline behaviour specifically for each device by looking at patterns to find behaviour that varies significantly from that baseline therefore detecting an anomaly that warrants further analysis.

Global event tracking and detection of all VMware hybrid cloud environments makes it easy to combat ransomware enterprise wide. Detection includes monitoring unexpected changes so that administrators can rapidly diagnose and recover. Accelerating detection helps to minimize and prevent data loss.

DETECTION

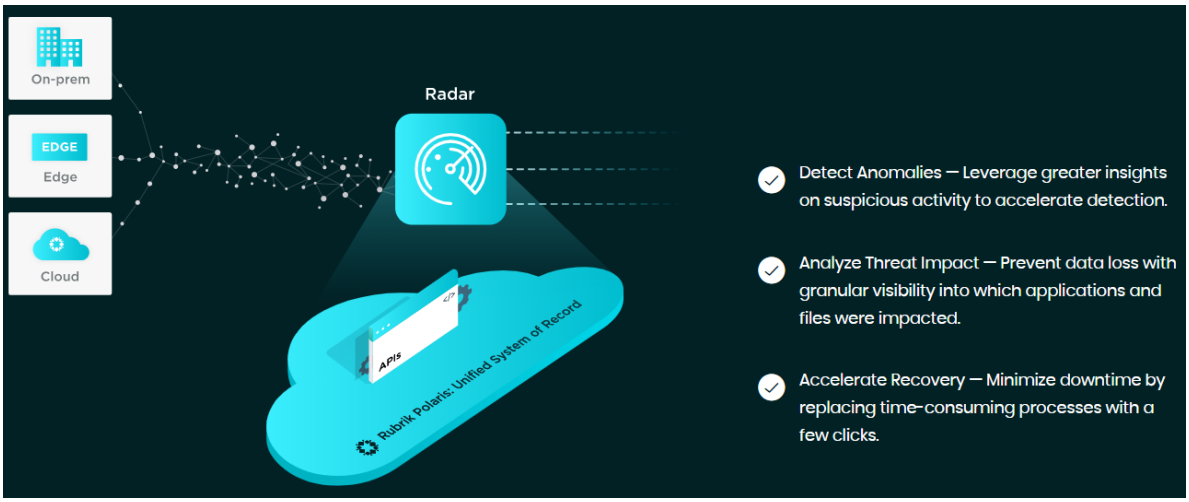
Radar performs analysis on each snapshot indexed inside the Rubrik Polaris platform. The analysis is largely based off of file system behaviour and content analysis. The detection pipeline has two parts:

File System Analysis – Performs behavioural analysis on the file system metadata information looking at items like # files added, # files deleted, etc. This creates a historical baseline that gets refined over time through machine learning algorithms. This information is used to detect anomalies in behaviour for future scans and compares for encryption performed by ransomware.

File Content Analysis – Once outlier behaviour is detected then further analysis can be performed on that snapshot. The content analysis will begin to detect ransomware. The method of the analysis is a light weight process and is designed to efficiently use CPU cycles to lower compute overhead.

EVENT TRACKING AND ALERTING

Once the detection threshold is met in the file system analysis, a filesystem anomaly alert indicates to the user that anomalous behavior has been detected. An alert is generated and is followed by a content analysis letting the user know if there is a high or low number of encryption indicators. This alerting can be configured to send email notifications along with notifications in the UI.



https://www.rubrik.com/en/lp/white-papers/19/Polaris-Radar-Monitor-Detect-Recover?utm_medium=website&utm_source=internal-link

Polaris Sonar (Data Search, Governance & Compliance)

As businesses adopt cloud, they grapple with massive data fragmentation, making it impossible to know where sensitive data resides. At the same time, the increasing risk of data privacy breaches and non-

compliance with regulations impose serious financial penalties. Polaris Sonar is a new SaaS application that applies machine learning to discover, classify, and report on sensitive data without any impact to production. By leveraging your existing Rubrik deployments, users get up and running in just a few minutes with zero additional infrastructure required.

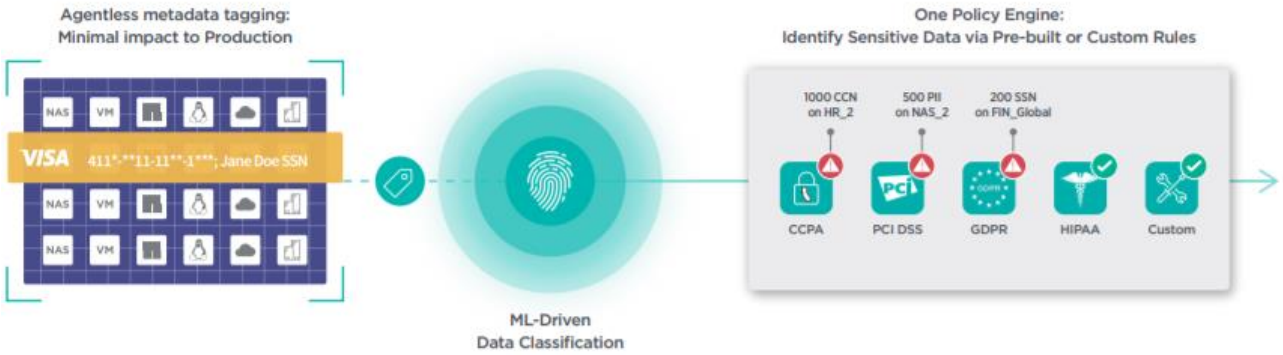
Polaris Sonar applies machine learning to scan and classify sensitive data without agents or impact to production. Leverage pre-built policy templates to identify common data types from regulations and standards such as GDPR, PCI-DSS, HIPAA, and GLBA, or define custom dictionaries, expressions, and policies. We employ various NLP techniques to minimize false positives.

Reduce Sensitive Data Exposure

With intensifying data breaches and non-compliance penalties, manual data governance increases risk and consumes valuable resources. Polaris Sonar applies machine learning to automate sensitive data classification for common data types, such as personally identifiable information (PII), without impacting production.

HOW POLARIS SONAR WORKS

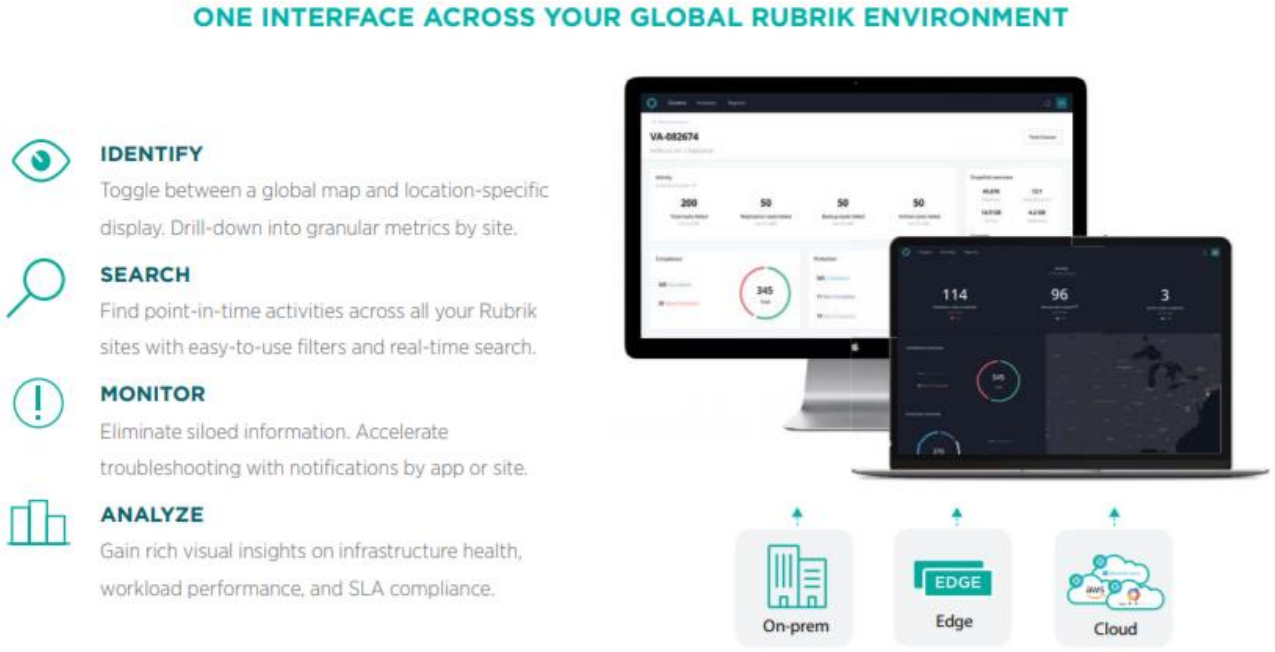
1. Configure role-based access controls to assign user permissions on data access.
2. Create a compliance policy from a custom or pre-defined template, which specifies what protected objects and types of sensitive information to search for, such as social security number, healthcare NPI, credit card number, or ITIN. Sonar then performs an initial scan to surface sensitive data aligned with the policy. Users can whitelist locations where sensitive information is allowed to minimize false alerts.
3. Use agentless, incremental scanning to quickly classify new and modified data for performance efficiencies and without impact to production.
4. Search on-demand for information at any point in time via on-demand search to satisfy access requests (e.g. “Where are all locations with John Smith’s PII?”)
5. Sonar will automatically notify you on policy violations and when sensitive data resides in wrong locations.
6. Report on policy violations, track compliance progress, and help identify at-risk data.



Polaris GPS (Central Management)

Rubrik Polaris GPS delivers centralized management for your global, distributed Rubrik environment. Designed for a seamless user experience, Polaris GPS provides a comprehensive view of your physical, virtual, and cloud topologies while making management tasks elegantly simple and intuitive. Search for a point-in-time activity by application or location. Determine SLA compliant applications at-a-glance.

Optimize costs and performance with on-demand insights on infrastructure health and behavior. Powered by an automated visualization engine, Polaris GPS enables filtering as-you-go to generate rich custom dashboards in minutes.



Benefits of the Cloud Data Platform

Instant Search

Deliver near-zero RTOs with predictive search. Locate VMs, physical databases, applications, or files, whether the data resides on-premises or in the cloud.

Policy-Driven

Rubrik wipes out management complexity with just a few clicks through a single policy engine that orchestrates service level agreements (SLAs) across the entire data lifecycle. Automate management across hybrid and multi-cloud environments with one programmatic interface.

Self-Service & Orchestration

At the core of Rubrik lies a powerful suite of APIs that can orchestrate data from data center to cloud. Integrate Rubrik into your ideal automation stack to accelerate service delivery. Deliver self-service and automated custom lifecycle management workflows that play well with third party services.

Analytics & Reporting

Rubrik Envision unlocks actionable insights across the hybrid cloud with customized visual reporting.

Deliver platform analytics across your entire environment on operational efficiency, compliance, and capacity utilization. Create and share rich data visualizations to drive business acceleration at scale.

Security & Compliance

Data is secured in-transit and at-rest throughout its lifecycle, regardless of location. Rubrik delivers granular role-based access control while automating compliance reporting to successfully complete various industry and internal audits. Recover quickly from ransomware from immutable backups native to the platform.

API-First and Cloud-Scale Architecture

Rubrik is a vendor-agnostic platform that is built on an API-first architecture. Leverage our powerful suite of APIs to integrate seamlessly with third party services. Rubrik is purpose-built for cloud integration and infinite scale to enable hybrid cloud for all enterprises.

Common Service Scope - Modernisation & Consolidation

Often, as part of cloud adoption, support or services, clients require a comprehensive Review, Modernisation and Consolidation of Applications and Workloads prior to onboarding to the cloud service this is scoped on a case by case basis, using the SFIA rate card as attached to the G-Cloud entry. Dependent on the exacting client requirements, one or more of the following stages would be performed, ensuring a successful onboarding of the service.

Stage 1 - Discovery & Initial Scope

Logicalis follow a mature solution design methodology, and the first stage of this methodology is the Discovery & Initial Scope Stage. During this stage we capture and understand the clients business objectives, workloads (applications and databases) to be supported, functional requirements, constraints (technical, such as re-use or key integration points, organisational & budgetary), security, operational and wider integration requirements, this information is then used to identify suitable solutions in the evaluation stage.

During the Discovery Stages of this process, we firstly look to understand the business outcomes expected of the solution, any constraints as well as analysing the Clients existing environment.

This process captures and analyses information such as:

- understanding application capacity and performance requirements (compute, memory, storage capacities, bandwidth, latency, performance, etc),
- Application Software & Database types
- network links
- security protocols
- key integration points
- operational processes
- Personnel skill levels
- other functional requirements
- constraints (budgetary, environmentally, re-use of components, strategically, organisationally, geographically)

Typical outputs from this stage would be

- Documented list of Inputs
- Documented list of Technical and Business Outcomes Required
- Initial assessment of data gathered and issues to be addresses in Stage 2 – Assess Define
- Outline scope of effort & Activities
- High level list of Solution Options

Stage 2 – Assess, Evaluate, Refine & Scope of Work

Information gathered during the Discovery & Scoping stage, along with any information that the client has available about the proposed systems. will be assessed allowing us to have a good understanding of the current operating model (COM), allowing us to define what options could be available for the Target Operating Model (TOM).

- Detailed assessment of Servers, Storage, Network, Locations & Workloads (Applications & Databases) in Scope
    - Review currently available documentation
    - Further Analyse and consider Information gathered during discovery Phase
    - Arrange technical workshops involving lines of business owners as appropriate to gather client specific knowledge and capability that needs to be factored
    - Identify Workload incompatibilities, Physical IP addresses, External Dependencies, version support, and other constraints that might impact solution design
- Detailed Hardware & OS analysis and gathering existing workload/resource utilisation

Outputs from this stage would include:

- Design Options, including recommended Solution
- Scope of Services
- Agreement on Solution to take forward to Stage 3

Stage 3 - Architecture & Design

This stage typically provides a Mid &/or Low-level design, outlining hardware, software and other components required to meet the full requirements gathered in stages 1 and 2, as well as validating the services outlined in Stage 2.

Typically, our designs would consider:

- Hardware choice Scale Up, Scale Out, Physical Service Isolation
- Operating System scope and function
- Network Layout Physical, Virtual, intra/xtra DC locations
- Specific workload Profile requirements such as placement/affinity, memory, CPU, i/o, performance, latency etc
- I/O and connectivity requirements for number and type of workloads consolidated
- Physical Isolation of workloads, security, and sensitivity
- Resilience and availability such as replication, clustering, cold/warm migration
- Backup and Recovery of the new environments

The outputs from this stage would include:

- Detailed design, allowing efficient implementation and configuration
- Proposed Migration options
- Detailed and agreed level of effort
- Identified Risks and associated mitigations
- Detailed components list
- Integration to other areas of business, facility, networks, operations, and change.

Stage 4 - Installation & Integration

The installation stage involves integration into existing environment, hardware, OS setup and System Acceptance Testing based on Mid/Low Level Designs provided in Stage 3. This would provide a production ready platform to perform migration and transition to production activities. This would include activities such as

- Rack each new physical server, according to agreed locations and layout
- Interconnects, integration with existing ethernet and fibre switches, labelling and documentation, according to design
- Installation of Additional H/W components
- Power on, basic Boot tests
- Install & update Firmware & O/S to agreed levels
- Setup i/o domains, LDOMs, Zones and other elements required for Migration
- Integration with other components per Low Level Designs
- Detailed System configuration changes to support technical objectives based on Low Level Design
- Installation, configuration, and testing of Storage infrastructure
- Basic Installation and configuration of Oracle monitoring & Management elements
- System and Acceptance testing as defined and agreed
- Testing of any replication features to be deployed host based and/or array based.
- Detailed build documentation

The outputs from this stage would be:

1. Production Ready Platform ready for stage 5 migration and transition to production
2. Detailed system build documentation
3. Acceptance tests sign off documentation
4. Site Specific configuration details
5. System specific vendor documentation

Stage 5 – Migration & Transition to Production

This stage is typically dependent on the nature of the project, complexity, timelines, client capability and transition requirements. This would typically include:

- Agreed Migration Services
- Training & Knowledge Transfer Sessions
- Service on-boarding
- System Handover and final signoff

Outputs from this phase, will include:

1. Migration plans & Failback documentation
2. Final Signoff and acceptance
3. Service operation and support procedures

About Logicalis

Overview

Logicalis UK is a leading IT solutions and managed services provider specialising in delivering technology solutions to help organisations leverage the power of digital transformation. As a global technology service provider, we deliver next-generation digital managed services, to provide our clients with real-time visibility and actionable insights across the performance of their digital ecosystem including availability, user experience, security, economic performance, and sustainability.

Our 7000+ 'Architects of Change' are based in 30 territories around the globe, helping our 10,000+ clients across a range of industry sectors, create sustainable outcomes through technology.

Our extensive range of services encompasses the entire IT lifecycle, from consulting and design to implementation and ongoing managed services. Whether we are helping clients navigate the complexities of networking and cloud computing, bolstering cybersecurity measures, optimising data centre infrastructure, or enabling digital collaboration and communication, we bring deep expertise and a customer-centric approach to every project.

We have cultivated strong partnerships with leading technology vendors such as Cisco (1 of 6 Global Gold partners), NetApp, Microsoft, IBM, Lenovo, HP, and VMWare, granting us access to the latest tools and solutions. These partnerships, combined with our in-house expertise, allow us to deliver cutting-edge IT solutions that empower organisations to stay competitive in a rapidly evolving digital landscape.

Responsible and Sustainable Company

Our agenda is shaped by who we are as a business, and which social and environmental challenges are important to our people and in the regions that we operate in. Everything we do is underpinned by one key principle: that **at Logicalis we are dedicated to conducting our business in a responsible and sustainable way**.

We are a signatory to the Task Force on Climate-Related Financial Disclosures (TCFD) (now monitored by the IFRS foundation), a member of the United Nations Global Compact (UNGC), reporting to the Carbon Disclosure Project (CDP) and have committed to the Science Based Targets initiative (SBTi) Corporate Net Zero Standard.

Logicalis has made a commitment **to become scope 1 and 2 carbon neutral across the group by 2025, halve scope 1 and 2 emissions by 2030, and eliminate 90% of our emissions by 2050.**

Certification, and compliance

Overview

We maintain and implement a documented Quality and Compliance system and are accredited to the following standards:

- ISO 9001 – Quality Management
- ISO 14001 – Environmental Management
- ISO 20000 – IT Service Management
- ISO 27001 – Information Security Management
- Cyber Essentials Plus

These certifications are re-audited on a regular basis to ensure continued compliance as well as identify areas of enhancements to compliance through our Quality & Compliance Manager.

ISO 9001 – Quality Management

Our objective is to maintain the desired quality of products at economical cost through planned and efficient utilisation of all technological, human and material resources available to us. A quality management system meeting the requirements of ISO 9001 is communicated to and understood throughout the company to meet our objectives; to meet or exceed customers highest expectations for product quality, cost and delivery, address relevant regulations and legalisation and to implement a continuous programme of improvement.

ISO 14001 – Environmental Management

As a responsible organisation, we seek to manage the direct environmental impacts from our activities on and off-site as well as the indirect impacts associated with the way that clients use the services we provide. Furthermore, we committed to raising awareness of the potential for impact our activities may have on the environment and our surroundings.

We recognise that implementing good environmental practices are integral to what we do. Our aim is to minimise our environmental footprint by focusing on the areas in which we have most impact such as reducing and recycling waste, using energy efficiently and promoting environmentally friendly policies in the workplace.

As a minimum, we manage and maintain the ISO 14001 accreditation which underpins our Environmental Management Policy.

ISO 20000 – IT Service Management

We continuously manage and maintain the ISO 20000 accreditation which underpins our IT Service Management policy.

Our teams define and develop solutions for customers in seven key areas:

- Corporate networks: to create the infrastructure to deliver content to the right place at the right time.
- IP communications: to integrate voice and data, video and mobile applications on a single, IP network to enable new ways of working and simpler management
- Security: to safeguard the integrity and privacy of shared content across the network
- Enterprise performance management: to provide 24/7, enterprise-wide performance monitoring and management
- Data management: to organise and structure content to facilitate its use by applications
- Application integration: to deliver and present content in the context of a process or task
- Enterprise computing: to deliver resilient, high availability systems to run applications

We also provide full lifecycle management of customer ICT assets – from planning, design, implementation and integration to support, management and optimisation. We have an extensive portfolio of managed services that encompass the end-to-end management of multi-vendor, multi-technology ICT system. This includes intelligent remote monitoring, operational management, co-location and full or partial outsourced partnering.

ISO 27001 – Information Security Management

We operate a number of internal policies relating to our ISO 27001 certification which staff must sign up to in order to be permitted access to systems. These cover:

- Acceptable Use Policy
- Data Classification Policy
- Information Handling Policy
- Information Security Policy
- Mobile Working Policy
- Network and Infrastructure Management Policy
- Physical Security Policy
- User Access Control Policy
- Wireless Security Policy

Cyber Essentials Plus

Logicalis UK are certified to Cyber Essentials Plus across the whole organisation, see certificate below:

CYBER ESSENTIALS PLUS

CERTIFICATE OF ASSURANCE

LOGICALIS UK Limited

Building 8 Ground Floor Foundation Park Roxborough Way Maidenhead SL63UD

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS PLUS SCHEME

NAME OF ASSESSOR : Simon Keeling

CERTIFICATE NUMBER : 48fc2030-1c99-4733-9a75-2be4c0e3f6f7

DATE OF CERTIFICATION : 2023-02-08

PROFILE VERSION : 3

RECERTIFICATION DUE : 2024-02-08

SCOPE : Whole Organisation

SCAN THIS QR CODE TO VERIFY THE AUTHENTICITY OF THIS CERTIFICATE

CERTIFICATION MARK

CERTIFICATION BODY

CYBER ESSENTIALS PARTNER

The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials Plus implementation profile and thus that, at the time of testing, the organisation's ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisation's defences will remain satisfactory against a cyber attack.