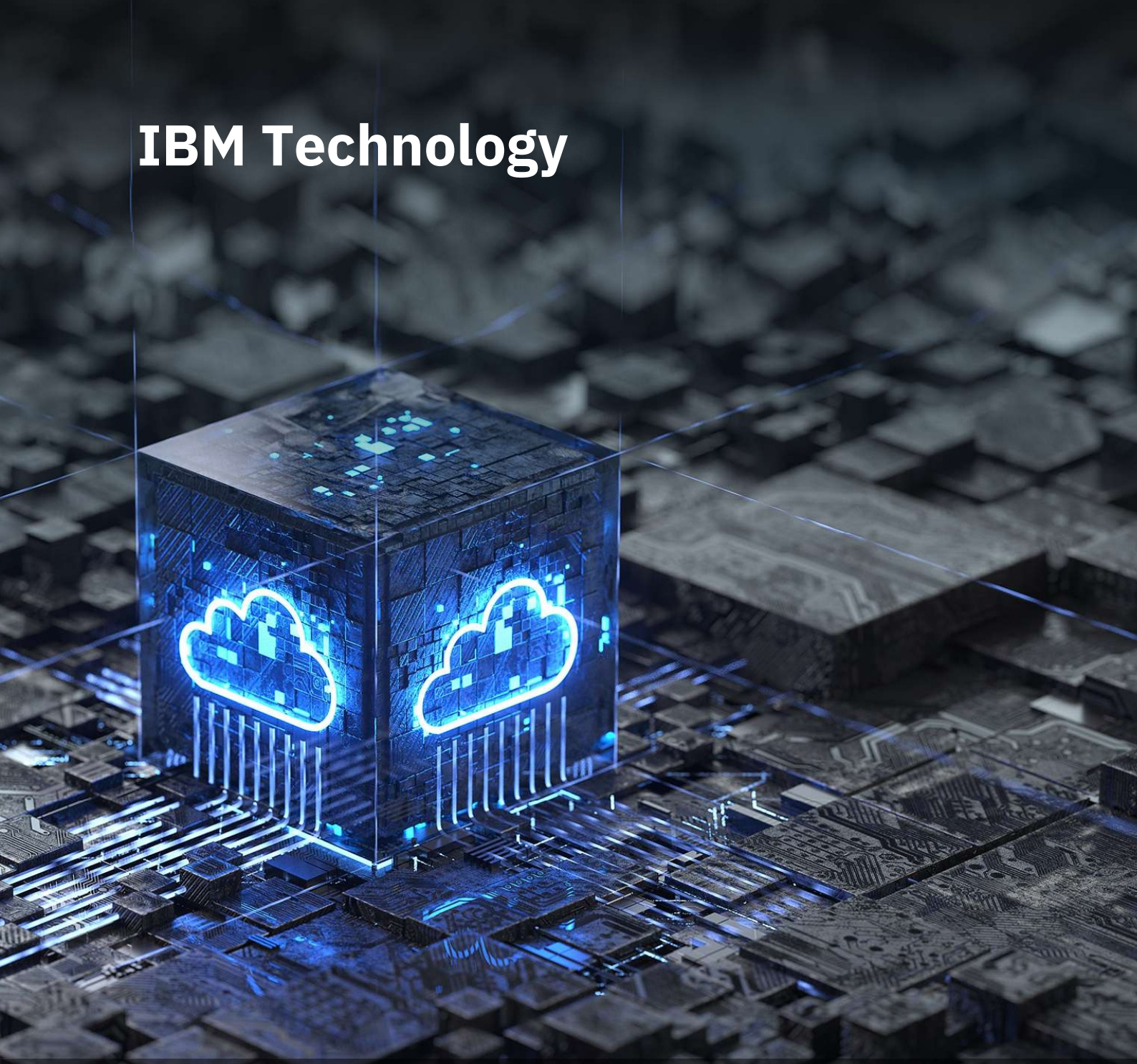
IBM Technology



G-Cloud 15
IBM – Verify Identity Protection

Service Definition Document

Email: ukcat@uk.ibm.com
Contact: Anne-Marie Wheeler

IBM Verify Identity Protection

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order. Upon acceptance of Client's order, this Service Description and the Cloud Services Agreement found at http://www.ibm.com/terms/csa (or equivalent agreement for Cloud Services between the parties) applies to Client's use of the Cloud Services.

1. Cloud Service

IBM Verify Identity Protection is a cloud-based service that helps to protect the identity fabric of an organization against identity-focused attacks, by providing end-to-end visibility into security gaps and potentially risky user accesses across identity systems in a hybrid-cloud environment. The identity fabric consists of all cloud and local systems used in managing human and non-human identities and their access to the organization's resources, including user directories, application gateways, identity access providers and entitlement management systems.

The service employs both identity security posture management (ISPM) and identity threat detection and response (ITDR) methodologies to identify and alert on system blind spots, misconfigurations, and access-based attacks as they unfold.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM Verify Identity Protection

This Cloud Service helps organizations identify and remediate identity posture issues and threats for managed and unmanaged identities across multi-cloud, SaaS and on-premise environments. The solution helps provide visibility, contextual observability, end-to-end identity security posture management (ISPM) functionality, and real-time identity threat detection and response (ITDR) capabilities. It contains over 70 risk logics ("playbooks") for detecting various identity risk postures such as absence of multifactor authentication (MFA), bypassing of critical security controls like Zero Trust Network Access (ZTNA), or the use of shadow identity systems such as unapproved password managers.

Available ISPM features include, but are not limited to:

- Identity activity observability, for all service and human accounts
- Identity & access blind spots
- Identity infrastructure exposures

Available ITDR features include, but are not limited to:

- Identity infrastructure threats,
- Suspicious identity accesses
- Threat investigations and response with identity context

Entitlements for the Cloud Service are calculated based on Entity IDs across the company which will be tracked on a monthly basis.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below applies to IBM's processing of personal data on behalf of Client.

https://www.ibm.com/terms/?id=6EAFCBAC38014EAFA3BABF75AC43A7FF

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides the Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total

number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/support/pages/node/731179.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at https://www.ibm.com/support/home/pages/support-guide/.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Entity ID is a unique identifier for any entity identified within the Cloud Services.

  For the purposes of this Cloud Service, an Entity ID is defined as a human user accessing the systems of the company, for example, an employee, a contract, or a business partner. Each Entity ID may have up to 10 assigned identities, such as user accounts or service accounts. In the event an Entity ID has more than 10 assigned identities, Client must purchase additional Entity ID entitlements to cover the additional identities.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at https://www.ibm.com/acs apply.

5.1 Enabling Software

The Cloud Service contains the following Enabling Software:

- Network Access Flow Collector
- Directory Collector

6. Overriding Terms

6.1 Data Use

The following prevails over anything to the contrary in the Content and Data Protection section of the base Cloud Service terms between the parties: IBM will not use or disclose the results arising from Client's use of the Cloud Service that are unique to Client's Content or that otherwise identify Client. IBM and IBM's supplier Authmind, Inc. may however use Content and other information that result from Content as part of the Cloud Service for the purpose of managing and improving the Cloud Service and other Cloud Services that utilize the same underlying technology. IBM may share (including to IBM's supplier Authmind Inc.) threat identifiers and other security information embedded in Client personal data for threat detection and protection purposes. The provisions of this section will survive the termination or expiration of the transaction.