Infrastructure Reliability

Service Specification

Service Specification

Service Name:	Infrastructure Reliability
Service Level Hours:	Refer to section 1.1
Unit of Charge:	% of AWS, Azure and/or GCP Spend plus Alert Logic license fee
Prerequisites:	Refer to Deployment Documents
Supported Cloud Platforms:	AWS, Azure and GCP
Product Codes:	CO-INFRASTRUCTURE-RELIABILITY CO-INFRASTRUCTURE-RELIABILITY-OB CPA-AL-LICAL-PRO (Alert Logic Threat Management - Professional Licences)
Version Number:	3.1.1
Status:	Live
Published Date:	November 2019

The Small Print

Definitions

The definitions for all capitalised terms used throughout this Service Specification are set out in the Cloud Operations Service Definitions document which forms a part of this Service Specification and the Cloudreach Order Form to which this Service Specification relates.

Table of Contents

1. Service Overview **6**
1.1 Service Levels 7

2. Operating Systems Supported **7**
2.1 LTS version support 8

3. Onboarding **9**
3.1 Onboarding Terms 9
3.2 Deployment Strategy 9
3.3 List of VM Agents installed on Compute Resources 10
3.3.1 Agent Maintenance 10

4. Availability & Performance Management **10**
4.1 Monitoring Methodology 11
4.1.1 Data Residency 11
4.1.2 Data Collection 11
4.1.3 Data Retention 11
4.2 Scope of “Supported” and “Monitored” 11
4.2.1 Scope of “Supported” 11
4.2.1.1 Best Practice Guidance 11
4.2.1.2 Configuration Management 11
4.2.1.2.1 Out of Scope: Configuration Management 11
4.2.1.3 Service Troubleshooting 12
4.2.1.4 Out of Scope: Support Boundaries 12
4.2.2 Scope of “Monitored” 12
4.2.2.1 Service Monitoring 12
4.2.2.2 Compute Resources 13
4.3 Supported & Monitored CSP Services 13
4.3.1 AWS-native - Monitored & Managed Services 13
4.3.2 Azure-native - Monitored and Management Services 16
4.3.3 GCP-native - Monitored and Management Services 18
4.3.4 Out of Scope: Virtual Machine Hosted Applications 20

5. Patching **20**
5.1 Scope of Security Patching 20
5.2 OS Upgrades 21
5.3 Automation of Patching 21

6. Backup and Restore **21**
6.1 AWS and Azure & GCP Virtual Machine Backup / Restore 21
6.1.1 Schedule and Retention (AWS & Azure) 21
6.1.2 Schedule and Retention (GCP) 22
6.1.2 Backup Approach 22
6.1.3 Recovery Approach 22
6.2 Database Backup 23
6.3 Database Restore 24

7. Threat and Vulnerability Management **25**

7.1 Threat Management 25
7.2 Vulnerability Management 26

8. Endpoint Protection 26
8.1 File Scanning vs Kernel-based detection 27
8.2 Event Monitoring 27
8.2.1 Quarantined Infections 27
8.2.2 Non-quarantined infections 27

9 Services Management Support 27
9.1 Incident Management 27
9.1.1 Incident Management Guidelines 27
9.1.1.1 Cloudreach Responsibilities 27
9.1.2 Incident Prioritization 28
9.1.3 Incident Prioritization for Threat & Vulnerability Management service 29
9.1.4 Incident Response and Resolution Times 29
9.2 IT Change Management 29
9.2.1 Cloudreach responsibilities 29
9.2.2 Customer responsibilities 30
9.2.3 Change Catalogue 30

10. Continuous Improvement 30
10.1 Service Overview 30
10.1.1 Automation 30
10.1.2 Infrastructure Modernization 30
10.1.3 Complex Changes 31
10.2 Improvement Request Fulfillment 31
10.3 Reporting 31
10.4 Out of Scope: Continuous Improvement Exceptions 32

11. Service Delivery Management 32
11.1 Service Review Meetings 32
11.1.1 Service Reports 33
11.1.1.1 Management Summary 33
11.1.1.2 Service Management 33
11.1.1.3 Performance Management 33
11.1.1.4 Cloud Environment Management 33
11.2 Service Improvement Initiatives 34
11.3 Custom 34
11.4 Service Review Timetable 34

12. Offboarding and handling of customer data 34

Document Control

Version	Date	Author(s)	Notes
3.1.1	28-11-2019	Ben De Mora	GCP capabilities

Sign off

Version	Date	Sign-off	Job Title
3.1.1	29.11.2019	Barbara Cooke	Head of Operations Excellence
3.1.1	29.11.2019	Stephanie Leopold	Lead Regulatory Counsel
3.1.1	29.11.2019	Shanoor Hussain	Core Operations Leader
3.1.1	29.11.2019	Ben de Mora	Senior Product Architect

1. Service Overview

Infrastructure Reliability is a managed service for Amazon Web Services (AWS), Microsoft Azure Public Cloud and Google Cloud Platform (GCP). The service will manage the availability and accessibility of the Customer's environment(s) in these public clouds. It will provide operational support services of Customer's environments and support components/ resources/ instances within their cloud platform that is controllable by the Cloud Service Provider's (CSP) console or APIs. It will also support the availability and accessibility of the VMs hosting the Customer's applications.

A summary of the key features of Infrastructure Reliability are listed below:

Onboarding - Cloudreach will assign a Service Transition team member to manage the project of onboarding Customer environment into Infrastructure Reliability. During initial phase of onboarding, Cloudreach will assess the time needed to onboard the environment based on the complexity and intricacies involved with onboarding. Please note that Cloudreach will only perform onboarding of Customers Environments during Business Hours.

Availability and Performance Management - The service will monitor the availability and accessibility of the Customer's environments up to the Operating Systems. Cloudreach will monitor IAAS and PAAS services at Cloud Provider Platform level by ingesting metrics which are available by default in the corresponding CSP's monitoring service (i.e. AWS Cloudwatch, Azure Monitor, GCP Stackdriver). Cloudreach shall define alerting for these metrics based on the best practices for the corresponding CSP service and customer requirements. The performance metrics will also be collected to detect trends with defined thresholds for alerting and performance analysis.

Patching - Security patches will be applied on a monthly basis, with the ability to audit and report on the patches applied while maintaining compliance standards.

Backups and Restore - Block Level backups will be taken for Operating Systems and Database Engines with restore of backups performed via Service Requests.

Threat and Vulnerability Management - as part of Infrastructure Reliability, Cloudreach will deploy Alert Logic Professional bundle. The service includes the implementation, tuning, incident and change management e.g. configuration and rules changes, and reporting. This is, in addition to the security operations performed by Alert Logic in providing security monitoring, responding to intrusions and vulnerabilities that the service provides.

Endpoint Protection - as part of managing any Virtual Machine (VM)s in the Customer's environment(s), Cloudreach includes Endpoint Protection software to provide Anti-Virus and Anti-Malware protection. The supply, configuration, tuning, ongoing maintenance and reporting are part of the service.

Services Management Support - the Customer's public cloud environment(s) will be maintained as part of the service including configuration management and any trouble-shooting that may be required to address issues with availability and accessibility of the environment(s). Incidents and Change will be managed using the corresponding ticketing and procedures in accordance with runbooks and/or process(es) documented.

Continuous Improvement (*available if the Customer's Monthly Spend ≥ amount specified in applicable order form*) - This service provides with remote access to Improvement Engineers on an adhoc basis to deliver improved and increased automation, modernization of architecture and tools, KPI improvements and reporting, and Customer experience improvements through Site Reliability Engineering. In addition, the Continuous Improvement can be used for a complex change, modification or creation of resources outside of the configuration of the environment from the time onboarding was completed.

Service Delivery Manager (SDM) - Appointed Service Delivery Manager responsible for owning the Customer experience and delivering the service management outcomes associated with Managed Services provided by Cloudreach. The SDM provides strategic business alignment, business critical IT service management, chaired proactive service reviews and continuous service improvement. The SDM delivered remotely is included as part of Infrastructure Reliability. If the Customer is requesting that the SDM is on-site and/or has specific dedicated number of hours or days a month, additional charges, including travel and expenses shall be applied. Customer's specific requirements will be captured during pre-sales and associated additional charges will be priced on application and reflected accordingly in the order form.

1.1 Service Levels

Services	Service Level Hours
Onboarding Continuous Improvement Service Management Support (Changes)	Business Hours (9x5) (*PDT time zone if the Customer is based in NA and GMT time zone if the Customer is based in EEA*)
Service Delivery Manager	Business Hours (9x5) (*applicable time zone where the SDM is located*)
Availability and Performance Management Backup and Restore Threat and Vulnerability Management Endpoint Protection Service Management Support (P1 and P2 Incidents)	24x7
Patching Service Management Support (P3 and P4 Incidents)	24x5 (*PDT time zone if the Customer is based in NA and GMT time zone if the Customer is based in EEA*)

2. Operating Systems Supported

Cloudreach supports the following Operating System versions:

Operating System Version	Comment
Windows Server 2008 R2 Service Pack 1/2- 2016	On January 14, 2020, Microsoft will be officially ending its support for Windows Server 2008 R2 editions. Cloudreach shall stop support of this version on January 14, 2020.

	Windows 2016 Nano is not supported at this time.
Ubuntu	Only the LTS editions are supported at this time. Cloudreach will support any LTS (Long Term Support) versions which are currently within vendor support. For a list of supported LTS versions and their end-of-life date please visit https://wiki.ubuntu.com/Releases Please note that within an LTS version of Ubuntu, Canonical releases multiple "patch versions" of the LTS distribution. Different patch versions may contain different kernel revisions, with varying support (and security patching availability), which may end before the end of life of the LTS distribution. Cloudreach recommends that customers always opt in for the patch version that uses a kernel version which is supported throughout the lifecycle of the LTS distribution, as otherwise customer may miss out on some security patches until the kernel is upgraded. Kernel upgrades are not part of the monthly patching schedule performed by Cloudreach. For further information please see https://wiki.ubuntu.com/Kernel/Support
Debian	Cloudreach will support any LTS versions which are currently within vendor support. For a list of supported LTS versions and their end-of-life date please visit https://wiki.debian.org/LTS/
Amazon Linux	Cloudreach will support any LTS versions which are currently within vendor support. For a list of supported versions and their end-of-life date please visit https://aws.amazon.com/amazon-linux-ami/faqs/
CentOS	Cloudreach will support any major version which are currently within vendor support. For a list of the currently supported versions and their end-of-life date please visit https://wiki.centos.org/About/Product
RedHat Enterprise	Cloudreach will support any RHEL version which is currently within vendor's Full Support. For a list of the currently supported versions and their end-of-life date please visit https://access.redhat.com/support/policy/updates/errata

2.1 LTS version support

Cloudreach may require to update & test the set of tooling to ensure that it works as expected with new versions of Operating Systems. For that reason, at times, Cloudreach may not be able to support new LTS versions of Operating Systems as soon as they are released.

In the case of OS vendors making changes that require Cloudreach to adjust the tooling, Cloudreach reserves the right to take up to 6 months to make all necessary changes to support new LTS release.

With regards to Operating Systems end of support, Cloudreach will provide support until such date or extension thereof, from the OS vendors.

3. Onboarding

3.1 Onboarding Terms

Once the service is ready for onboarding, Cloudreach will assign a Service Transition team member to manage the project of onboarding Customer environment into Infrastructure Reliability. Cloudreach will also allocate Service Delivery Manager, who will be the main point of contact between Customer and Cloudreach during the onboarding phase.

During initial phase of onboarding, Cloudreach will assess the time needed to onboard the environment based on the complexity and intricacies involved with onboarding.

Please note that Cloudreach will only perform onboarding of Customers Environments during Business Hours.

3.2 Deployment Strategy

In order to deliver the Infrastructure Reliability service, Cloudreach needs to have access to the Customer's Environment(s) in the form of network, API and system level access. This enables Cloudreach's operational teams to provide the various management services within the Customer's Environment where configuration, maintenance, troubleshooting and service management are required. For example, in the case of configuration and service management, Cloudreach needs to deploy its monitoring and management tools.

The Deployment Strategy Document also details the policies that the Customer needs to comply with for the duration of the contract.

A separate Deployment Document details the access information required for the customer's chosen public cloud platform such as network address(es), accounts/subscriptions and logins, authentication and permissions. This is a prerequisite for Cloudreach to deliver Infrastructure Reliability to the Customer. The necessary documentation will be made available before and at the time of onboarding the environments to be taken under Cloudreach management.

Here's an example:

If AWS ASG or Azure Scale Sets exist within Customer's Cloud Platform, then the Customer shall provide Cloudreach with relevant access to implement the required integration and deployment tools as made available per the AWS ASG or Azure Resource Groups services. (i.e. User data for an AMI that is used with an ASG launch configuration). Customer shall be responsible for limiting Cloudreach's access to only the specific data, information or other Customer material which is required for the purposes of carrying out the implementation.

The Customer shall inform Cloudreach of any changes to the Golden AMI in use of said resources outlined above to ensure that all Cloudreach monitoring and management tools continue to function effectively upon service redeployment.

3.3 List of VM Agents installed on Compute Resources

Cloudreach, as part of delivery of Infrastructure Reliability service, may install following agents onto the compute resources:

Vendor	Agent	Notes
Chef	Chef Client	For Configuration Management of Cloudreach tooling.
SignalFX	SignalFX Smart Agent	Monitoring agent which collects telemetry data from OS level instances.
Cylance*	CylancePROTECT Agent	Kernel-based Endpoint Protection agent (applicable unless customer opts out from the service)
AlertLogic	AlertLogic Agent	Intrusion Detection System agent (applicable unless customer opts out from the service)
AWS	Simple Systems Manager (SSM) Agent	Management agent, used for the purpose of patching and running shell commands externally for customers with environments in AWS.
Azure	Log Analytics Agent	Management agent used for Patching & Backups of Azure VM's. Only for customers with environments in Azure.
Azure	Azure VM Agent	Pre-installed with marketplace images, this agent is required for various management purposes of Azure VMs.
Azure	Hybrid Worker Agent	For execution of Azure Automation runbooks on VMs (used for patching automation).

Cloudreach reserves the right to change or add agents to customer VM's. Customers will be notified of any changes made to the list above with advance notice.

**Cylance is the primary endpoint protection agent which Cloudreach installs in cases where endpoint protection is adopted by the customer. In some circumstances (environment specific), then either Alert Logic or BitDefender will be used as an alternative where applicable.*

3.3.1 Agent Maintenance

It is the responsibility of Cloudreach to install and maintain version and configuration of agents installed on Customer's Virtual Machines.

Unless otherwise agreed by Cloudreach, Customer shall not alter the agents installed and configured by Cloudreach, as any changes made may result with impact on the service that Cloudreach can provide.

4. Availability & Performance Management

Cloudreach will monitor the health of cloud resources for each mutually agreed AWS, Azure and/or GCP Account and can raise an alert based on the event conditions denoted

during Onboarding Process. Cloudreach defined AWS and Azure health check metrics are based on a subset of available AWS CloudWatch, Azure Monitor Diagnostics and GCP Stackdriver metrics.

In the event that an alert is raised, Cloudreach shall:

- Manage the response to the alert pursuant to the Incident Management Process.
- Send the alert based on the event conditions as an email to the Primary Contact as denoted during the Onboarding process.

4.1 Monitoring Methodology

4.1.1 Data Residency

All monitoring data collected by Cloudreach will be stored on servers hosted in the EU region.

4.1.2 Data Collection

For CSP native monitoring services (i.e. AWS CloudWatch), data will be collected from an external 3rd party tooling provider via API requests to the appropriate CSP service. As part of the onboarding process, a service account role and relevant permissions will need to be created in Customer environments to allow this collection.

For OS-level collection of data, an agent will be installed on the operating system. The agent will report metrics to an external endpoint, either directly or via proxy.

Frequency of collection is configurable, with default being every 5 minutes. Over time, older data might be aggregated for performance reasons.

4.1.3 Data Retention

Monitoring data will be retained for 13 months.

4.2 Scope of “Supported” and “Monitored”

This section provides an explanation of what Cloudreach means in relation to supporting and monitoring CSP services.

4.2.1 Scope of “Supported”

4.2.1.1 Best Practice Guidance

Cloudreach holds expert level knowledge of this service and leverages this to provide guidance and advice to Customers. Engineers will be able to advise Customer on changes to the service that are inline with the best practice guidelines provided by the vendor and discuss details and intricacies of the service with customers.

4.2.1.2 Configuration Management

Cloudreach will perform changes to the service at CSP Level, using either CSP’s provided GUI or API to execute the change. The focus of any changes to be carried out will be to either maintain or improve health, availability or accessibility of the resource/service.

4.2.1.2.1 Out of Scope: Configuration Management

Please note that within the Infrastructure Reliability service, Cloudreach will only perform environment-level support and will not provide application-level administration. An

example of this is an RDS service, where Cloudreach will ensure that the database is configured correctly (i.e. Network level access, monitoring CloudWatch metrics, backups).

However, within Infrastructure Reliability, Cloudreach will not provide any service that interacts with the data inside the database (i.e. altering tables, modifying data, creating SQL users). For this level of support, Cloudreach can supply Customer with “Application Reliability” as an additional service.

4.2.1.3 Service Troubleshooting

Cloudreach will assist Customers with troubleshooting issues with the service or resource at CSP level, with the focus of providing availability and accessibility of the resource and service within customer environments.

An example of issue, where Cloudreach can assist, could be a problem with application connecting to the database. In such instance, Cloudreach would be able to review the network connectivity & health of the database to establish the cause of the connectivity issue. With this in mind, within Infrastructure Reliability service, Cloudreach would not look to investigate any issues with the data once inside the database (i.e. query performing slowly).

4.2.1.4 Out of Scope: Support Boundaries

- For services that are not “supported” in the below tables, Cloudreach will endeavour to work with the Customer and CSP Support team, leveraging CSP’s in-house skills and documentation to deliver support for this service.
- For avoidance of doubt, Infrastructure Reliability will support existing resources, rather than provision net new resources unless necessary in support of existing infrastructure.

4.2.2 Scope of “Monitored”

4.2.2.1 Service Monitoring

Cloudreach shall integrate with Cloud Service Provider native monitoring tooling to provide monitoring service to Customers. In most cases, Cloudreach will perform API calls (either directly or via 3rd party tooling) to collect various metrics from CSP Monitoring service (i.e. AWS CloudWatch) and will ingest those metrics into a monitoring platform, where further analysis will be performed to identify problems and patterns within Customer environments.

Cloudreach is utilising the following API services to collect Metrics Data:

- AWS Cloudwatch
- Azure Monitor
- GCP StackDriver

During onboarding, Cloudreach will discuss and agree on monitoring methodology with the Customer. Cloudreach will configure the monitoring alerts to the needs of the Customer environment(s), focusing on monitoring key components which indicate that the platform is available and accessible. Cloudreach will only perform monitoring of the services which are critical for the health & availability of the Environment, in line with the Environment usage patterns.

Once onboarding is completed, Cloudreach monitoring software will monitor the Customer environment(s). Cloudreach will receive notifications and investigate events in accordance with the defined monitoring alerting. If appropriate, Cloudreach will raise a

support case and contact the Customer primary contact(s) to inform them of the details of the support case.

Cloudreach reserves the right to disable or modify a specific monitoring or alerting configuration on notice to the Customer, if deemed necessary by Cloudreach in order to preserve an accurate and effective alerting signal.

4.2.2.2 Compute Resources

For additional level of monitoring for compute resources, Cloudreach will require to perform an installation of agent software on every Compute Resource which is to be supported. Further details about the agent installation will be provided within "Access Requirements" document supplied during onboarding.

4.3 Supported & Monitored CSP Services

The list of Supported and Monitored CPS services shall be amended to reflect changes that the CSPs make to their services. Cloudreach will reflect these changes accordingly.

4.3.1 AWS-native - Monitored & Managed Services

In the table below is a list of AWS services which publish metrics to CloudWatch, with indication of support and monitoring capabilities within Infrastructure Reliability.

Service	Namespace	Supported	Monitored
Amazon API Gateway	AWS/ApiGateway		✔
AppStream 2.0	AWS/AppStream		✔
AWS Billing and Cost Management	AWS/Billing		✔
Amazon CloudFront	AWS/CloudFront	✔	✔
Amazon CloudSearch	AWS/CloudSearch		✔
Amazon CloudWatch Events	AWS/Events	✔	✔
Amazon CloudWatch Logs	AWS/Logs	✔	✔
AWS CodeBuild	AWS/CodeBuild		✔
Amazon Cognito	AWS/Cognito		✔
Amazon Connect	AWS/Connect		✔
AWS Database Migration Service	AWS/DMS		✔
AWS Direct Connect	AWS/DX	✔	✔
Amazon DynamoDB	AWS/DynamoDB	✔	✔
Amazon EC2	AWS/EC2	✔	✔
Amazon EC2 Spot Fleet	AWS/EC2Spot	✔	✔
Amazon EC2 Auto Scaling	AWS/AutoScaling	✔	✔
AWS Elastic Beanstalk	AWS/ElasticBeanstalk	✔	✔

Amazon Elastic Block Store	AWS/EBS	✔	✔
Amazon Elastic Container Service	AWS/ECS	✔	✔
Amazon Elastic File System	AWS/EFS	✔	✔
Amazon Elastic Inference	AWS/ElasticInference		✔
Elastic Load Balancing	AWS/ApplicationELB	✔	✔
Elastic Load Balancing	AWS/ELB	✔	✔
Elastic Load Balancing	AWS/NetworkELB	✔	✔
Amazon Elastic Transcoder	AWS/ElasticTranscoder		✔
Amazon ElastiCache for Memcached	AWS/ElastiCache	✔	✔
Amazon ElastiCache for Redis	AWS/ElastiCache	✔	✔
Amazon Elasticsearch Service	AWS/ES		✔
Amazon EMR	AWS/ElasticMapReduce		✔
AWS Elemental MediaConnect	AWS/MediaConnect		✔
AWS Elemental MediaConvert	AWS/MediaConvert		✔
AWS Elemental MediaPackage	AWS/MediaPackage		✔
AWS Elemental MediaTailor	AWS/MediaTailor		✔
Amazon FSx for Lustre	AWS/FSx		✔
Amazon GameLift	AWS/GameLift		✔
AWS Glue	AWS/Glue		✔
AWS CloudHSM	AWS/CloudHSM		✔
Amazon Inspector	AWS/Inspector		✔
AWS IoT	AWS/IoT		✔
AWS IoT Analytics	AWS/IoTAnalytics		✔
AWS IoT Things Graph	AWS/ThingsGraph		✔
AWS Key Management Service	AWS/KMS	✔	✔
Amazon Kinesis Data Analytics	AWS/KinesisAnalytics		✔
Amazon Kinesis Data Firehose	AWS/Firehose		✔
Amazon Kinesis Data Streams	AWS/Kinesis		✔
Amazon Kinesis Video Streams	AWS/KinesisVideo		✔
AWS Lambda	AWS/Lambda	✔	✔
Amazon Lex	AWS/Lex		✔

Amazon Machine Learning	AWS/ML		✔
Amazon Managed Streaming for Kafka	AWS/Kafka		✔
Amazon MQ	AWS/AmazonMQ		✔
Amazon Neptune	AWS/Neptune		✔
AWS OpsWorks	AWS/OpsWorks	✔	✔
Amazon Polly	AWS/Polly		✔
Amazon Redshift	AWS/Redshift		✔
Amazon Relational Database Service	AWS/RDS	✔	✔
Amazon Route 53	AWS/Route53	✔	✔
Amazon SageMaker	AWS/SageMaker		✔
AWS Shield Advanced	AWS/DDoSProtection	✔	
Amazon Simple Email Service	AWS/SES	✔	✔
Amazon Simple Notification Service	AWS/SNS	✔	✔
Amazon Simple Queue Service	AWS/SQS	✔	✔
Amazon Simple Storage Service	AWS/S3	✔	✔
Amazon Simple Workflow Service	AWS/SWF	✔	✔
AWS Step Functions	AWS/States	✔	✔
AWS Storage Gateway	AWS/StorageGateway	✔	✔
Amazon Textract	AWS/Textract		✔
Amazon Translate	AWS/Translate		✔
AWS Trusted Advisor	AWS/TrustedAdvisor	✔	✔
Amazon VPC	AWS/NATGateway	✔	✔
Amazon VPC	AWS/TransitGateway	✔	✔
Amazon VPC	AWS/VPN	✔	✔
AWS WAF	AWS/WAF	✔	✔
Amazon WorkSpaces	AWS/WorkSpaces	✔	✔
Glacier	N/A*	✔	N/A*
VPC	N/A*	✔	N/A*
CloudFormation	N/A*	✔	N/A*
CloudTrail	N/A*	✔	N/A*
Config	N/A*	✔	N/A*

Systems Manager	N/A*	✔	N/A*
Trusted Advisor	N/A*	✔	N/A*
Personal Health Dashboard	N/A*	✔	N/A*
IAM	N/A*	✔	N/A*
Organizations	N/A*	✔	N/A*
Key Management Service	N/A*	✔	N/A*
Certificate Manager	N/A*	✔	N/A*

* Services marked with N/A under monitoring are already managed-natively by the CSP and monitoring of these services is either not possible or not necessary.

4.3.2 Azure-native - Monitored and Management Services

In the table below is a list of Azure services that publish metrics to Azure Monitor service, with indication of support and monitoring capabilities within Infrastructure Reliability. Where there are no metrics to collect and therefore no monitoring performed, Cloudreach provides best practice, configuration and troubleshooting services.

Namespace	Supported	Monitored
Microsoft.AnalysisServices/servers		✔
Microsoft.ApiManagement/service	✔	✔
Microsoft.Automation/automationAccounts	✔	✔
Microsoft.Batch/batchAccounts		✔
Microsoft.Cache/redis	✔	✔
Microsoft.CognitiveServices/accounts		✔
Microsoft.Compute/virtualMachines	✔	✔
Microsoft.Compute/virtualMachineScaleSets	✔	✔
Microsoft.Compute/virtualMachineScaleSets/virtualMachines	✔	✔
Microsoft.ContainerInstance/containerGroups	✔	✔
Microsoft.ContainerService/managedClusters	✔	✔
Microsoft.CustomerInsights/hubs		✔
Microsoft.DataFactory/datafactories		✔
Microsoft.DataFactory/factories		✔
Microsoft.DataLakeAnalytics/accounts		✔
Microsoft.DataLakeStore/accounts		✔
Microsoft.DBforMariaDB/servers	✔	✔
Microsoft.DBforMySQL/servers	✔	✔
Microsoft.DBforPostgreSQL/servers	✔	✔

Microsoft.Devices/IotHubs		✔
Microsoft.Devices/provisioningServices		✔
Microsoft.DocumentDB/databaseAccounts	✔	✔
Microsoft.EventGrid/topics	✔	✔
Microsoft.EventGrid/eventSubscriptions	✔	✔
Microsoft.EventGrid/extensionTopics	✔	✔
Microsoft.EventHub/namespaces	✔	✔
Microsoft.EventHub/clusters	✔	✔
Microsoft.HDInsight/clusters		✔
Microsoft.Insights/AutoscaleSettings		✔
Microsoft.Insights/Components		✔
Microsoft.KeyVault/vaults	✔	✔
Microsoft.Kusto/Clusters		✔
Microsoft.LocationBasedServices/accounts		✔
Microsoft.Logic/workflows	✔	✔
Microsoft.NetApp/netAppAccounts/capacityPools/Volumes		✔
Microsoft.NetApp/netAppAccounts/capacityPools		✔
Microsoft.Network/networkInterfaces	✔	✔
Microsoft.Network/loadBalancers	✔	✔
Microsoft.Network/dnszones	✔	✔
Microsoft.Network/publicIPAddresses	✔	✔
Microsoft.Network/applicationGateways	✔	✔
Microsoft.Network/virtualNetworkGateways	✔	✔
Microsoft.Network/expressRouteCircuits	✔	✔
Microsoft.Network/expressRouteCircuits/peerings	✔	✔
Microsoft.Network/connections	✔	✔
Microsoft.Network/trafficManagerProfiles	✔	✔
Microsoft.Network/networkWatchers/connectionMonitors	✔	✔
Microsoft.Network/frontdoors	✔	✔
Microsoft.NotificationHubs/Namespaces/NotificationHubs	✔	✔
Microsoft.OperationalInsights/workspaces	✔	✔
Microsoft.PowerBIDedicated/capacities		✔
Microsoft.Relay/namespaces		✔

Microsoft.Search/searchServices		✔
Microsoft.ServiceBus/namespaces	✔	✔
Microsoft.SignalRService/SignalR		✔
Microsoft.Sql/servers/databases	✔	✔
Microsoft.Sql/servers/elasticPools	✔	✔
Microsoft.Sql/managedInstances	✔	✔
Microsoft.Storage/storageAccounts	✔	✔
Microsoft.Storage/storageAccounts/blobServices	✔	✔
Microsoft.Storage/storageAccounts/fileServices	✔	✔
Microsoft.Storage/storageAccounts/queueServices	✔	✔
Microsoft.Storage/storageAccounts/tableServices	✔	✔
Microsoft.StreamAnalytics/streamingjobs		✔
Microsoft.TimeSeriesInsights/environments		✔
Microsoft.TimeSeriesInsights/environments/eventsources		✔
Microsoft.Web/serverfarms		✔
Microsoft.Web/sites (excluding functions)		✔
Microsoft.Web/sites (functions)		✔
Microsoft.Web/sites/slots		✔
Microsoft.Web/hostingEnvironments/multiRolePools		✔
Microsoft.Web/hostingEnvironments/workerPools		✔

Within Azure CSP, Cloudreach is not able to support or monitor “Classic” Azure services from previous generation of Azure Platform.

For resources that offer different service tiers, Cloudreach requires that Customers opt in for a tier that supports Azure Monitor metrics. For example: Load Balancer, “Basic” tier does not report health metrics to Azure Monitor

4.3.3 GCP-native - Monitored and Management Services

In the table below is a list of GCP services with indication of support and monitoring capabilities within Infrastructure Reliability. Where there are no metrics to collect and therefore no monitoring performed, Cloudreach provides best practice, configuration and troubleshooting services.

ServiceNamespace	Supported	Monitored
Compute Products		
Compute Engine: Virtual Machines, Disks, Network	✔	✔
App Engine: Managed App Platform	✔	✔

Kubernetes Engine: Managed Kubernetes/Containers (GCP platform level)	✔	✔
Cloud Functions: Event-driven serverless functions	✔	✔
Storage Products		
Cloud Storage: Object Storage and Serving	✔	✔
Nearline: Archival Occasional Access Storage	✔	
Coldline: Archival Rare Access Storage	✔	
Persistent Disk: VM-attached Disks	✔	
Cloud Filestore: Managed NFS Server	✔	✔
Database Products		
Cloud Bigtable: Petabyte-scale, low-latency nonrelational		✔
Cloud Datastore: Horizontally Scalable Document DB	✔	✔
Cloud Firestore: Strongly-consistent Serverless Document DB	✔	✔
Cloud Memorystore: Managed Redis	✔	✔
Cloud Spanner: Horizontally Scalable Relational DB		✔
Cloud SQL: Managed MySQL and PostgreSQL	✔	✔
Data and Analytics Products		
Cloud Dataflow: Stream/batch data processing		✔
Cloud Pub/Sub: Global Real-time Messaging	✔	✔
Google BigQuery: Data Warehouse/Analytics		✔
Networking Products		
Carrier Peering: Peer through a carrier	✔	
Direct Peering: Peer with GCP	✔	
Dedicated Interconnect: Dedicated private network connection	✔	✔
Partner Interconnect: Connect on-premises network to VPC	✔	
Cloud CDN: Content Delivery Network	✔	
Cloud DNS: Programmable DNS Serving	✔	
Cloud Load Balancing: Multi-region Load Distribution	✔	✔
Cloud NAT: Network Address Translation Service	✔	
Cloud Router	✔	✔
IPsec VPN: Virtual private network connection	✔	✔
Internet of Things Products		
Cloud IoT Core: Device Management and ingest data		✔

Identity and Security Products		
Access Transparency: Audit Cloud Provider Access	✔	
Cloud IAM: Resource Access Control	✔	
Cloud Key Management Service: Hosted Key Management Service	✔	
Management Tools Products		
Cloud APIs: APIs for Cloud Services		✔
Stackdriver Logging: Centralized Logging	✔	✔
Stackdriver Monitoring: Infrastructure and Application Monitoring	✔	✔
Mobile Products (Firebase)		
Firebase database		✔

4.3.4 Out of Scope: Virtual Machine Hosted Applications

Customer hosted applications such as databases, network and web servers will only be monitored for health and performance of underlying VM infrastructure that they are running on.

For application level monitoring and reporting, the Customer must subscribe to the Cloudreach's Managed Application service additionally.

5. Patching

Cloudreach shall perform the following Operating System patching where patches are made available by the Operating System provider.

Type	Frequency
Critical and Security Patching	Monthly, within mutually agreed maintenance window with customer during onboarding.

If Customer makes use of Golden Amazon Machine Imagines (AMIs) or Azure Gold Image as a source for infrastructure deployment Cloudreach will hold temporary Snapshots as a roll-back mechanism if required during critical/security patching periods.

5.1 Scope of Security Patching

For Windows VMs, Cloudreach will configure Windows VM's with Cloudreach-managed WSUS server. Cloudreach will then only whitelist patches classified as "Critical Updates" and "Security updates". No other patches will be applied to those virtual machines by Cloudreach.

For Linux VM's, with example of Amazon Linux or RHEL distributions, Cloudreach will only install patches marked as "security" patches, for example by using the "yum security" plugin (https://linux.die.net/man/8/yum-security).

Cloudreach will install minor kernel security patches during patching activity, however, within the scope of regular patching, Cloudreach will not upgrade kernel version of the underlying OS.

For avoidance of doubt, Infrastructure Reliability will not perform any application-level patching on Customer workloads.

Exception:

- Due to the nature of security and non-security related updates in CentOS, patching will always include non-security related updates for this distribution.

5.2 OS Upgrades

Cloudreach considers this type of activity Service Packs (Windows) or Distribution Upgrades (Linux)) as more complex, with higher risk to application stability. For this reason, Cloudreach does not perform this type of upgrade by default within the Infrastructure Reliability service.

Type	Notes
Service Packs (Windows) or Distribution Upgrades (Linux)	Cloudreach is able to perform and assist the customer with this as a complex change request
Kernel Upgrades (Linux)	Cloudreach can perform kernel version upgrades as a complex change request

5.3 Automation of Patching

As part of efficient delivery of service to Customer, Cloudreach will deploy tooling which allows for automated patching of Customer virtual machines, including deployment of CSP native tool on the OS level (SSM agent for AWS, OMS agent for Azure). Further details and requirements will be provided to Customer within “Access Requirements” document, supplied during onboarding.

Due to complexities and intricacies of patching activity, Cloudreach will assess the ability to automate the patching activity for each environment and will implement the right level of automation to ensure the stability of customer environment.

6. Backup and Restore

6.1 AWS and Azure & GCP Virtual Machine Backup / Restore

6.1.1 Schedule and Retention (AWS & Azure)

Cloudreach shall perform daily, weekly and monthly backups of the AWS EC2 and Azure Virtual Machine operating system Instances based on the default schedule and retention periods defined in the table below:

Backup	Schedule	Retention Period
Daily	02:00 UTC Monday to Sunday	7 days
Weekly	03:00 UTC every Sunday	4 weeks
Monthly	04:00 UTC on the first of every month	2 months

Customer may request alternative backup schedule and/or retention period during Onboarding of the Customer's services which shall be subject to approval by Cloudreach.

Instances are backed up based on the approach defined in the table below:

- All Incidents raised by the Cloudreach backup monitoring and configuration platform pertaining to 'backup failure' will automatically be assigned as an Incident request and actioned by the Cloudreach CSD.

6.1.2 Schedule and Retention (GCP)

Cloudreach shall perform daily backups of the GCP Virtual Machines based on the default schedule and retention periods defined in the table below:

Backup	Schedule	Retention Period
Daily	02:00 UTC Monday to Sunday	30 days

OR

Backup	Schedule	Retention Period
Weekly	02:00 UTC Sunday	52 weeks

Currently Cloudreach is only able to offer Daily OR Weekly backup policy for GCP VM's.

6.1.2 Backup Approach

Cloud Platform	Backup Approach
AWS	Backups are performed by taking a Snapshot of AWS EC2 EBS volumes on a regular schedule as specified in the preceding table.
Azure	Backups are performed by taking full backups of each Azure Virtual Machine against a regular schedule defined by the Customer. By default the preceding table sets out the backup and retention periods.
GCP	Backups are performed by configuring a "Scheduled Snapshots" functionality in GCP

Instances of Operating Systems can be restored upon request by the Customer based on the approach defined in the table below:

- If required by the Customer, Cloudreach shall invoke an Operating System recovery approach against the Azure VMs, AWS EC2 instances or GCP VMs within the supported account. The restore will be treated with P2 priority if it is service impacting.

- All requests raised by the Customer that are not identified as service impacting will be treated as P4 Service Requests.

6.1.3 Recovery Approach

Cloud Platform	Type	Recovery Approach

AWS	Instance or Full Volume	Root Volumes: Cloudreach shall create a new volume from a previous Snapshot depending on the date requested by Customer. Cloudreach shall remove the current volume and replace with the newly created volume. Additional Drives: Cloudreach shall create a volume from a previous Snapshot depending on the date requested by Customer. Cloudreach shall remove the volume and replace with the newly created volume or if requested attach the new volume at a different mount point. Time: Time scales depend on the size of the volume and any other file system factors such as encrypted file system implementations (e.g. BitLocker and ProtectV).
Azure	Instance or Full Volume	Virtual Machine: Cloudreach shall recover a chosen Azure Virtual Machine against an existing or retained application consistent backup from a previous recovery point as chosen by Customer. Upon system restore this will also restore all previous system dependent Azure services, installed applications, pre existing files and/or folders. Cloudreach shall re-assign any pre existing Azure endpoints to the newly created Azure Virtual Machines to ensure continued connectivity upon successful restore. Time The time to execute a restore action is variable and dependent on the volume of data to be recovered from a backup.
GCP	Instance or Full Volume	Root Volumes: Cloudreach shall create a new volume from a previous Snapshot depending on the date requested by Customer. Cloudreach shall remove the current volume and replace with the newly created volume. Additional Drives: Cloudreach shall create a volume from a previous Snapshot depending on the date requested by Customer. Cloudreach shall remove the volume and replace with the newly created volume or if requested attach the new volume at a different mount point. Time: Time scales depend on the size of the volume and any other file system factors such as encrypted file system implementations (e.g. BitLocker and ProtectV).

6.2 Database Backup

Cloudreach can provide following backup strategy for specified cloud-native database technologies. There are two types of database backups supported:

1. A differential backup is based on the most recent, previous full data backup. A differential backup captures only the data that has changed since that full backup. The full backup upon which a differential backup is based is known as the base of the differential.
2. The transaction log is a serial record of all the transactions that have been performed against the database since the transaction log was last backed up. With transaction log backups, you can recover the database to a specific point in time (for example, prior to entering unwanted data), or to the point of failure.

Database Technology	Differential	Transactional	RPO	Default

				Retention
AWS				
RDS (MySQL)	✔	✔	5 minutes	1 week
RDS (Aurora)	✔	✔	5 minutes	1 week
RDS (PostgreSQL)	✔	✔	5 minutes	1 week
RDS (Oracle)	✔	✔	5 minutes	1 week
RDS (MS SQL)	✔	✔	5 minutes	1 week
Azure				
Azure SQL (Basic Service)	✔	✔	10 minutes	1 week
Azure SQL (Standard Service)	✔	✔	10 minutes	5 weeks
Azure SQL (Premium Service)	✔	✔	10 minutes	5 weeks
GCP				
Cloud SQL (MySQL)	✔	✔	5 minutes	1 week*
Cloud SQL (PostgreSQL)	✔	X	5 minutes	1 week*

**Last 7 automated backups are retained as standard. Data shown assumes a daily automated backup.*

Cloudreach utilises cloud-native backup features of database hosting platforms (i.e. AWS RDS, Azure SQL, GCP Cloud SQL). Cloudreach does not actually perform or maintain backups, however, within the service, Cloudreach, upon customer request, will perform configuration changes to backup configuration, and will perform a restore operation, when requested by Customer (see section 6.3 for further details). Cloudreach is limited by the technology limitations of the respective CSP services and may not be able to fulfil requests for changes that are not possible.

With regards to Recovery Time Objective (RTO), Cloudreach is unable to provide generic assertion of how long it will take to restore a database. This is due to a number of factors which are unique to each application and environment (i.e. database size, application intricacies).

6.3 Database Restore

As part of the service, Cloudreach is able to perform a restore of the database (supported restore databases needs to be defined in table in section 6.2).

Cloudreach will only perform the restore of the database using the CSP generated backups. Cloudreach will only perform the restore as an emergency action, upon agreement with the customer, when application has become unavailable due to an issue with the database. Cloudreach reserves the right to first investigate and decide if restore is an appropriate action to take. Cloudreach will always take the quickest path to restoring the database.

During this operation, additional maintenance tasks (for example, update of Customer's "Infrastructure-as-code" template) may be required. If requested by the Customer, such

tasks may be performed by Cloudreach under Infrastructure Reliability Continuous Improvement.

7. Threat and Vulnerability Management

The successful provision of the Threat and Vulnerability Management feature of Infrastructure Reliability by Cloudreach is conditional upon Customer subscribing to Alert Logic's Threat Management - Professional. Cloudreach will manage this security service as part of Infrastructure Reliability.

7.1 Threat Management

As part of Threat Management, Cloudreach shall:

1. Respond to the intrusion types generated by the Alert Logic's Threat Management - Professional's Intrusion Detection System (IDS) monitoring and log collections, as defined in the table below, by raising an Incident via the Cloudreach Incident Management Process;
2. In response to identified Incidents, Cloudreach shall implement mutually agreed actions to the Customer's Cloud Platform where these actions are within the overall scope of this Service Specification and purchased by the Customer. Where actions are outside the overall scope of this Service Specification, Cloudreach shall notify the Customer in writing and no action will be taken at the time until Customer provides it's consent;
3. Provide a weekly review and monthly report with analysis to the Customer using data from Alert Logic

Intrusion Type	Description
Brute force	This Incident identifies repeated authentication attempts and related activities. Alert Logic triggers a brute force incident when sufficient events indicate attempts to systematically compromise a system by brute-force guessing valid username and password combinations.
Information leak	This Incident identifies generally successful reconnaissance attempts. Alert Logic creates an information leak incident when events indicate attempts at reconnaissance activities such as port scans used to identify open and closed ports, or obtaining information from a secure system.
Log policy	This Incident uses the Log Management log correlation policies to identify potential issues. Log Management can create a log policy incident automatically based on selected correlated log messages and specifically defined conditions.
Misconfiguration	This Incident identifies a possible system misconfiguration. Alert Logic triggers a misconfiguration incident when events indicate that a system is incorrectly configured. Attackers can utilize the misconfiguration to compromise the system.
Policy violation	This Incident identifies activities that violate the acceptable use policies of most companies. These activities include viewing inappropriate material, peer-to-peer activity, and firewall policy changes.
Recon	This Incident identifies attempts to evaluate a target. Alert Logic creates a recon incident when events indicate reconnaissance activities against a network or set

	of hosts. The activities that trigger this Incident include gathering information about a server operating system, software versions, or the existence of debugging or demonstration scripts.
Suspicious activity	This Incident identifies activity not included in another category as set out in this table, and that requires further research. Alert Logic creates a suspicious activity incident when anomalous activities, which could indicate a compromise, occur.
Trojan activity	This Incident identifies activity that indicates a host is infected by a Trojan horse or other backdoor malware. Alert Logic creates a Trojan activity incident when events indicate a Trojan in the network. This type of malware acts as a legitimate program, but steals information or harms the system.
Worm activity	This Incident identifies hosts that display signs of worm infection. Alert Logic creates a worm activity incident when events indicate the traversing of a network worm.
Application attack	This Incident identifies attacks that target application-specific vulnerabilities. Alert Logic creates an application attack incident when an attacker attempts to compromise an application with a buffer overflow, race condition, directory traversal, SQL injection, cross-site scripting, /usr/bin/perl or other UNIX command attempts. This feature can also be set in Blocking mode and is only available as part of Alert Logic Threat Management - Enterprise. This an additional chargeable licence in addition to the Professional licence.

Cloudreach shall respond to the Intrusions Types in accordance with the service levels outlined in the section 9.1.3

Cloudreach will not provide resolution times as part of Threat Management due to the varied nature of threats and the potential complexity of threat resolution.

7.2 Vulnerability Management

Cloudreach shall monitor the vulnerabilities generated by Alert Logic Threat Management and report any such vulnerabilities and configuration issues on a monthly basis as part of monthly reporting.

In response to identified vulnerabilities and/or configuration issues, Cloudreach shall implement mutually agreed actions to the Customer's Cloud Platform where these actions are within the overall scope of this Service Specification and purchased by the Customer. Where the actions fall outside of the overall scope of this Service Specification, Cloudreach shall inform the Customer in writing.

8. Endpoint Protection

Cloudreach installs, configures and manages endpoint protection software to provide anti-virus and anti-malware protection on virtual machines that it manages on behalf of Customers' environments. The Endpoint Protection software to deliver this service is provided as-is and is subject to compatibility with the OS (Operating System) type and/or version.

8.1 File Scanning vs Kernel-based detection

Cloudreach has selected a next-generation anti-virus software capable of performing detection of intrusion at kernel level of Operating Systems. Due to the intricacies of providing such protection, at current time Cloudreach is only able to provide this level of protection for selected number of OS distributions and kernel versions.

Cloudreach will always prefer to install kernel based Endpoint Protection solution, however if Customer OS distribution or kernel version is not compatible with the software, file-level Endpoint Protection software will be installed on the OS instead.

8.2 Event Monitoring

Cloudreach shall proactively monitor the anti malware software for alerts and respond to such alerts based on the severity of the alert.

8.2.1 Quarantined Infections

If the infection has been quarantined, Cloudreach will simply inform the Customer of the event, and as the incident has been contained, no further action will be taken.

8.2.2 Non-quarantined infections

If the infection has not been quarantined, Cloudreach will investigate and manually contain the infection. Cloudreach will communicate all the details of the security incident to the Customer.

9 Services Management Support

Cloudreach will provide maintenance, troubleshooting, support and service management to ensure the availability and accessibility of the Customer's environment(s) in the Public Cloud. This section covers the service management Cloudreach will provide to the Customers as part of Infrastructure Reliability.

9.1 Incident Management

9.1.1 Incident Management Guidelines

9.1.1.1 Cloudreach Responsibilities

Cloudreach shall adhere to the following guidelines as part of the Incident Management Process:

- All Incidents raised by Customer will be logged with Cloudreach and will be categorised as per the Priority table above (see "Incident Prioritisation" tables above)
    - The CSD can be accessed on a 24/7 basis to assist with P1 and P2 Incidents relating to the Customer Cloud Platform and troubleshooting issues in the manner set out below. An Incident can be logged by the Customer or Cloudreach either through:
        - (i) emailing Cloudreach at support@cloudreach.com;

    - (ii) calling [UK] 0800 612 2966, [Overseas] +44 207 183 3991 or [US/Canada] (212) 335-0700;
    - (iii) the web by logging in to support.cloudreach.com using login details provided by Cloudreach during the onboarding process; or
    - (iv) mutually agreed automated event process.

  - For P1 Incidents specifically, the CSD can be accessed on a 24/7 basis only by telephone through the numbers as set out above. For the avoidance of doubt, P1 Incidents cannot be raised by email or through the CSD web portal.
- Customer can access CSD only by a designated Customer employee ("Support Engineer") raising an Incident.
- Cloudreach is under no obligation to respond to Incidents made in a manner which does not comply with this section.
  - CSD will use reasonable endeavours to find a work-around or solution to the Incident.

9.1.1.2 Customer Responsibilities

- Incidents must be logged by Customer in accordance with this section.
- When logging an Incident, Customer will provide to Cloudreach the following diagnostic information:
  - Detailed description of the issue
  - Customer Incident number
  - If available and reproducible, step by step instructions to reproduce the reported Incident
  - If available, date and time (and timezone) when Incident occurred
- Following the logging of an Incident, Customer shall be available via email or telephone to answer questions and assist the CSD as appropriate.
- Customer shall provide telephone or email access to the End User to facilitate troubleshooting Incidents.
- Customer shall provide access to End User support tools or permit Cloudreach to use their support tools to facilitate troubleshooting Incidents.
- Customer shall, within 5 working days of a request from Cloudreach, provide CSD staff access to all required Customer systems in order to enable Cloudreach to provide the Services detailed in the Order Form.

9.1.2 Incident Prioritization

The following tables outline the prioritization of Incidents and the description of each Priority Level.

Priority Level	Type of issue
P1 - Critical Impact	Total loss of service, no workaround available.
P2 - High Impact	Functional but degraded critical service or total loss for a service which supports a critical service. No work around available.
P3 - Medium Impact	Non critical service which is partially impacted and not functioning as intended.

P4 - Low Impact	Minor issue contained to a small group. A work around or alternative service is available.

9.1.3 Incident Prioritization for Threat & Vulnerability Management service

The following tables outline the prioritization of Incidents and the description of each Priority Level for Threat & Vulnerability Management.

Threat Level	Examples	Incident Priority
Critical	Successful data leakage; worm propagation; requires immediate remediation, or other post-compromise activity.	P1
High	Aggressive penetration tests, large scale or long duration brute force attacks.	P2
Medium	Brute-force or dictionary attacks; reconnaissance; failed web attack such as SQL injection, Apache Struts.	P3
Low	No threat, policy violation, authorised scans.	P4

9.1.4 Incident Response and Resolution Times

The table below show the response and resolution times for each Incident Priority. For the purpose of this clause:

- "Response" is defined as Cloudreach acknowledging the Incident by (i) providing a Cloudreach reference number either electronically or verbally to the Customer and (ii) assigning a priority to the Incident.
- "Resolution" is defined as Cloudreach providing a reasonable workaround or solution to the Incident.
- The time for Resolution starts at the same time as the Response time.
- SLA for Response and Resolution times start ticking when an Incident is logged by a Customer (either by phone, email or through the CSD web portal) or when Cloudreach is alerted of a service impact via its monitoring system.

Priority	Target Response Time	Target Resolution Time
P1	15 mins (24x7)	4 hours (24x7)
P2	30 mins (24x7)	8 hours (24x7)
P3	1 hour (24x5)	24 hours (24x5)
P4	4 hours (24x5)	3 Business Days (24x5)
P5	1 Business Day	Reasonable endeavours

9.2 IT Change Management

9.2.1 Cloudreach responsibilities

- Cloudreach shall use reasonable endeavours to agree the IT Change Management process with the Customer;

- Cloudreach will only implement Change Requests to the Customer Cloud Platform which are in accordance with the IT Change Management process;
- Cloudreach shall only provide Customer with the credentials required to access the Customer Cloud Platform to complete work authorised through the IT Change Management process

9.2.2 Customer responsibilities

- Customer shall log all required changes made to the Customer Cloud Platform with Cloudreach using the mutually agreed IT Change Management Process;
- Customer shall provide Cloudreach with all necessary Public Cloud Environment and Private Cloud Environment services requested by Cloudreach in order to effect the Change Requests in accordance with the IT Change Management Process

9.2.3 Change Catalogue

Cloudreach will provide a change catalogue upon request from Customer. This will be a separate document that will contain details and specifics of the available changes for the Customer.

10. Continuous Improvement

10.1 Service Overview

Infrastructure Reliability Continuous Improvement provides the customer with remote access to Improvement Engineers every month where the Customer's Monthly Spend equals or exceeds the amount specified in the order form. The Continuous Improvement is available during Business Hours only (9x5). The time available will be defined in the order form.

The areas of improvement include, but are not limited to:

10.1.1 Automation

Within Continuous Improvement, Cloudreach can undertake additional work that focuses on introducing or improving an element of automation within the Customer environment, with the aim of improving reliability and/or efficiency of the service. Improvement Engineers use an SRE-led approach and work closely with the Cloud Operations team during development and deployment of automation.

An example of such improvement could be an implementation of Infrastructure-as-Code template, where Cloudreach could undertake the task of moving management of resources into source code.

10.1.2 Infrastructure Modernization

Cloudreach has capability to perform a review of customer use of cloud environments against industry best practices and is able to provide customers with recommendations on changes to their environments, focusing on the areas of Reliability, Security, Cost Optimisation and Operational Excellence. Following such a review, Cloudreach will produce a report and recommend further implementation actions to remediate any

issues found. Within this service, Cloudreach can also execute on the identified areas of improvement.

Within AWS Environments, Cloudreach, as an AWS Well-Architected partner, will follow the official methodology of AWS Well-Architected reviews. For Azure and GCP, Cloudreach will take a similar approach and best practice.

10.1.3 Complex Changes

Infrastructure Reliability Continuous Improvement should be used for a complex change, modification, removal or creation of resources outside of the configuration of the environment from the time onboarding was completed.

The examples of complex change are:

- Non critical or non-urgent Operating System updates;
- Adding new or removing resources e.g. VMs during the life of the service;
- Create & Update AWS CloudFormation templates;
- Create or update Chef cookbooks and recipes;
- Create & Update Azure Resource Manager templates;
- Implementation of financial optimisation recommendations / actions;
- Deployment cycle auditing and;
- Operational task automation.

10.2 Improvement Request Fulfillment

The SDM shall collate a quarterly plan, based on the Well Architected Review (WAR) in the case of AWS, to deliver continuous improvement to the customer's infrastructure. Cloudreach will take a similar approach, reviewing architecture, operational excellence and best practices for Azure and GCP.

The SDM shall also take input from the Customer who may suggest improvement on their infrastructure.

The high level steps and activities will be as follows:

- The Service Delivery Manager shall create a request(s) for Infrastructure Reliability continuous improvement by opening a service request(s) on behalf of the customer, and informing the customer via email, phone, or self-service;
- Cloudreach will prepare a request for change (RFC) and present that to the customer to agree the improvement activity;
- If the customer decides to proceed with the RFC, the Service Delivery Manager will provide a proposed date to deliver the RFC. There is no associated SLA Resolution Target for continuous improvement RFC;
- The Service Delivery Manager will communicate via email or telephone before the actual day of implementing the RFC;
- Should the RFC not be successful, the Service Desk in conjunction with the Service Delivery Manager, will revert back to previous state prior the RFC and keep the customer informed at all times;
- If the customer decides not to proceed with the RFC, the Service Delivery Manager will not schedule the RFC and will keep it in a backlog and will be reviewed again the following quarter period

10.3 Reporting

The Service Delivery Manager will include a summary of continuous improvement RFCs during the previous month in the monthly service report.

10.4 Out of Scope: Continuous Improvement Exceptions

Customer acknowledges and understands that continuous improvement may not be used to perform tasks which are explicitly listed in the Standard Change list which will be provided upon request.

For the avoidance of doubt, Cloudreach may not be able to perform certain tasks under the following circumstances:

- Requests that are not covered within section 10.1 but will be considered on a case by case basis;
- Requests that negatively impact the security of the Customer environment;
- Changes that are unrelated to the support of components/ resources/ instances within the Customer's cloud platform;
- Large projects such as application refactoring and infrastructure modernisation

11. Service Delivery Management

The Service Delivery Manager (SDM) is responsible for owning Customer experience and delivering the service management outcomes associated with Managed Services provided by Cloudreach. The SDM provides the following services:

- Strategic business alignment - The SDM shall work with the Customer to ensure the operational services are delivered in line with the business objectives of the Customer. They shall also manage the business relations the Customer has with Cloudreach to enable delivery of services.

- Business critical IT service management – The SDM shall provide dedicated management of business-critical IT service management. They shall be the point of escalation and ensure the appropriate priority, resource, and associated governance is in place to progress to resolution.

- Proactive service reviews - Owned by your dedicated service delivery manager focusing on business as usual reporting and identifying and driving improvements recommendations.

- Continuous service improvement - The SDM shall implement a continuous service improvement plan. The plan shall cover recommendations, for example, on processes, procedures and run book improvements with action plan(s) mutually agreed with the Customer.

11.1 Service Review Meetings

The SDM will conduct and chair a monthly service review meeting with the Customer at a time and place to be mutually agreed in advance by the parties. The agenda for the service review shall include:

- Review service report management summary and discuss any points including but not limited to Cloudreach or Customer actions;
- Review Incidents, Problem(s), and Change Request(s) records, review performance and capacity issues identified (if applicable);
- Review status of existing, and any new mutually agreed, service improvement(s);
- Make recommendations for improvements of the service which have been identified by Operations team

11.1.1 Service Reports

Cloudreach shall provide Customer with a monthly service report in Google Docs format or PDF . The monthly service report shall include:

11.1.1.1 Management Summary

- Amazon Web Services (AWS) and Microsoft Azure performance summary: overall status plus availability and performance concerns, if any, on the following components: Cloud service availability, Instance CPU, memory, and network load;
- AWS and Azure security: overall status plus any security concerns, if any, for the following components: Instances in VPC, Security Groups, 2 factor authentication;
- Instance patching: overall status plus any security and compliance concerns ;
- Instance backups: overall status plus any business continuity concerns

11.1.1.2 Service Management

- Incident record summary including:
    - Current open Incident records and/or Service Requests
    - Recently closed Incident records and/or Service Requests
    - Summary of Incidents by priority and/or Service Requests
    - Summary of Incidents by component and/or Service Requests
- Problem record summary:
    - Current open problem records
    - Recently closed problem records
- Change Request record summary:
    - Pending Change Requests
    - Recently closed Change Requests
- SLA compliance summary
- Escalation Matrix
    - This lists the people and teams within Cloudreach and the customer organisation to contact and escalate an incident or an issue for example that remains unresolved at a support level

11.1.1.3 Performance Management

- Description of notable performance and/or capacity issues

- Performance charts from Cloudreach, AWS and/or Azure monitoring tools to support issues
- Information on cause of issue, if known
- Recommendations to remove or prevent future issues, if known

11.1.1.4 Cloud Environment Management

- Cloudreach will capture a view of customer cloud environment and provide the snapshot of it to customer via monthly service reviews;

- Cloudreach will provide a monthly report of the cloud environment compliance based on specified policies and criteria, for example:
    - Configuration management compliance (backups, patching)

11.2 Service Improvement Initiatives

- Cloudreach and / or Customer actions and risks aimed at improving the quality and performance of the managed service;
- The SDM shall implement a continuous service improvement plan that covers recommendations for example, on processes, procedures and run book improvements with action plan(s) to be mutually agreed with the Customer;
- Maintain and update Customer contact information;
- Cloudreach will provide Customer with trending analysis in the quarterly and bi-annual service review meetings

11.3 Custom

Any service reporting that requires additional work to customise to Customer's requirements i.e. requires additional data to be collected and/or produced will be assessed and may be subject to additional charges

11.4 Service Review Timetable

Deliverable	Frequency
Introductions and Review of the Cloudreach Escalation Matrix Guideline	Kick Off
Conduct Monthly Service Review (Onsite or Remote)	Monthly
Provide Monthly Service Reports	Monthly
Provide Quarterly Service Report (trend reports for the quarter, analysis and recommendations)	Quarterly
Provide Annual Service Report (trend reports for the year, analysis and recommendations)	Annual

12. Offboarding and handling of customer data

The table below details the type of customer information that Cloudreach requires for the provision of the services and how such information is handled upon termination of a customer service contract.

Data	Type of data	Retention Period	Format / method of transfer or deletion (if applicable)
Customer Personnel Email Address	Identity contact	Duration of contract	Deletion from internal systems
Customer Personnel Phone Number	Identity contact	Duration of contract	Deletion from internal systems
Customer Personnel Name	Identity contact	Duration of contract	Deletion from internal systems
Customer Personnel Title	Identity contact	Duration of contract	Deletion from internal systems
Chef data	Monitoring	Duration of contract	Deletion from internal systems
Performanc e data	Monitoring	13 months	Deletion from internal systems
Log data	Monitoring	13 months	Deletion from internal systems
Trace data	Monitoring	13 months	Deletion from internal systems
Access credentials to CSP	Access	Duration of contract	Deletion of Cloudreach roles from CSP
Switch role	Access	Duration of contract	Cloudreach or customer will remove switch role access and this includes any individual IAM accounts in the customer account
PEM keys	Access	10 business days after contract termination	Deletion from internal systems
AMI snapshots	Backup	Per the agreed retention policy	Deletion from AWS console, unless customer wishes to retain these
WSUS data	Monitoring	Duration of contract	Deletion from WSUS and reset of registry keys

Alert Logic data	Monitoring	13 months	Deletion of customer tenant post contract termination
Cylance data	Monitoring	13 months	Deletion of customer tenant post contract termination
Source Code	Customer IP	Duration of contract	Deletion of any customer source code from internal systems or transfer ownership of repositories if applicable