DARKTRACE

# Service Description: Proactive Health Optimization - Standard

## 1. Service Features

Darktrace Proactive Health Optimization - Standard provides structured technical reviews to support Customers improve outcomes from their Darktrace deployment. Our team provides reports to improve cyber security posture to address potential deployment health issues throughout the Subscription Period.

Any terms capitalized herein, shall have the meaning as defined in the Agreement.

Proactive Health Optimization - Standard consists of the following Service elements:

- Initial Technical Health Assessment;
- Monthly Data Quality and Health workshops;
- Quarterly Health Reports & Reviews;
- Focused Remediation playbooks; and
- Allocation of an Infrastructure Engineer to assist with mitigating infrastructure health challenges;
- Yearly Technical Executive Review

Proactive Health Optimization - Standard can be purchased at the beginning of the Subscription Period, or at any point during the Subscription Period when further support is required with health-related optimization. Workshops are available in English, Spanish, German, French, and Japanese. The Proactive Health Optimization - Standard Service outside of these languages is available on a best-efforts basis and is delivered by the Darktrace global professional services team. All Documentation provided as part of the service will be delivered in English.

### 1.1. Initial Technical Health Assessment

Once subscribed, an Infrastructure Engineer will undertake a remote assessment of the Customer deployment and prepare the Initial Technical Health Assessment to evaluate the health of the Customer's Darktrace environment. An active Call Home connection is required in order to perform a Health Assessment.

The Initial Technical Health Assessment will primarily focus on the following elements:

- Traffic Visibility, Quality & Load;
- Integrations; and
- Device Modelling

In collaboration with the designated Customer Success Manager, a document outlining the findings will be presented in a virtual meeting with the Customer and a remediation plan will be shared to address any identified issues. Customers should ensure that there is at least one active member of their Security team and/or user of Darktrace in attendance at the virtual meeting.

Further Technical Health Assessment reports will be generated every quarter to monitor ongoing operationality and account for any changes to the environment during that period.

Technical Health Assessments are run to validate latest deployment statistics. Every Technical Health Assessment examines Customer's Active AI deployment and includes the following elements:

1. Customer's Darktrace topology;
2. Detection health check;
3. System status Alerts;
4. Unidirectional traffic summary;
5. Deployment statistics;
6. Traffic loss;
7. Duplication review;
8. Subnet visibility;

9. Integrations summary;
10. License verification;
11. Software version verification;
12. Response Models setup
13. Response device tagging
14. Response advances configuration
15. Response reachability

For Customers that have purchased additional coverage from the AI platform such as /EMAIL, /OT, /CLOUD, /IDENTITY, /ENDPOINT, /CLOUD, and other cross platform products and services, the health assessment may also include:

1. Email verification;
2. Email flow;
3. Industrial traffic verification;
4. Endpoint traffic verification;
5. Identity modules verification;
6. Cloud security data verification
7. Attack Surface Management verification;
8. Proactive Exposure Management verifications;
9. Incidence Readiness and Recovery verifications;
10. Security Operations Support access;
11. Managed Threat Detection access;
12. Managed Detection & Response readiness.

The Darktrace engineer will schedule a Workshop with the Customer if the health assessment identifies potential improvements to the Customer's cyber security posture.

### 1.2. Monthly Data Quality and Health Services Workshops

#### 1.2.1. Overview

Following a Technical Health Assessment, a workshop between a Customer and a Darktrace Engineer will be booked in order to address the issues identified in the report. One remote workshop per month is included, and the engineer will coordinate with the Customer if the cadence needs to be adjusted. The scope of work covered in a given workshop is limited to addressing the results of the Technical Health Assessment, as set out at section 1.3.2, below.

The Workshop itself will consist of an interactive video call, wherein the Darktrace Engineer will take the Customer attendees through any observations made as a result of the Technical Health Assessment. The Engineer will make recommendations that the Customer can perform to improve the configuration of the deployment in order to help optimize performance and improve factors such as reachability, tracking and how the products act on the Customer network.

Any review and subsequent recommendations are made on a point-in-time basis that is wholly dependent on the Customer Data that the Darktrace instance has access to at the time of the Health Assessment. Any changes made by Customer based upon recommendations provided as a part of the Health Workshop are made at their own discretion. Customer acknowledges that changes made to the Customer environment after the Health Workshop may impact the accuracy of any recommendations made therein.

#### 1.2.2. Workshop composition

The focus of the Workshops is intended to be centered on the results of the Technical Health Assessment and addressing any issues that are highlighted therein. Any questions or analysis on other aspects of the Darktrace Offering are to be handled separately by Customer's account team outside of the Workshop. The length of each workshop is expected to be around 1 hour.

The Darktrace Engineer will walk through critical issues found with detection operationality such as, but not limited to disconnected appliances, low traffic, unidirectional traffic, or sub-optimal device tracking. To ensure the efficacy of the Workshop, Customer should ensure that there at least one active member of its Network team is in attendance. The

Network team member(s) should have the necessary network access to make the changes needed to resolve critical alerts.

Where the customer has purchased an Autonomous Response subscription, the Darktrace Engineer will walk through critical issues with Autonomous Response, such as but not limited to: low tagging, running human confirmation mode, poor reachability tests, poor model edits, licensing issues, or autonomous actions. To ensure efficacy of the Workshop, Customer should ensure that there at least one active member of its Security team and/or user of Darktrace is in attendance. The Security team/User(s) should have permission from the Customer organization to update the configuration as recommended in the Workshop.

If the Customer has purchased coverage in multiple environments such as /EMAIL, /IDENTITY, /CLOUD, /OT, /ENDPOINT and other cross platform products and services, the Darktrace Engineer will walk through critical issues in those areas. Some of the issues commonly discovered here include disconnect between servers, inaccurate data flow, active directory issues, API concerns, etc. To ensure efficacy of the Workshop, Customer should ensure that there at least one active member of its Security team and/or user of Darktrace is in attendance. The Security team/User(s) should have permission from the Customer organization to update the product configuration as recommended in the Workshop.

There is no limit to the number of Customer participants that may join the Workshop and Customer is advised that Workshops cannot be recorded.

It is the Customer's responsibility to apply and maintain any recommendations offered by the Darktrace Engineer. Customer acknowledges that the results of the Technical Health Assessment indicate the functionality of their Darktrace deployment, and accepts that, if the recommendations resulting from the Health Workshop are not followed, it may result in an associated reduced level of functionality from their Darktrace Offering.

Notes of the contents of the call will be taken throughout and a summary of what was covered will be shared with the Customer after the Workshop in a report along with any relevant materials that were presented during the Workshop.

#### 1.2.3. Post-Workshop Support

If the issues are not resolved within the anticipated hour, the workshop can be extended to a longer period or a follow up workshop can be scheduled. If a follow up workshop is needed, the engineer will schedule it with the Customer upon their availability. Ad hoc sessions can be booked via the portal as described below.

If Customer needs to reach their engineer outside of planned workshops, the requests are to be made via Customer Portal. If a remote session is required, the request for one is to be made at least two business days in advance of planned activity, to ensure the best available resource is allocated for the session.

If unable to schedule the consultation on the requested date, Darktrace will offer a mutually agreeable alternative date as close to the requested date as possible. If a detailed explanation of the focus of the proposed workshop is not provided, Darktrace reserves the right to delay any booking request until proper clarification is provided.

### 1.3 Quarterly Technical Health Reports & Reviews

Darktrace will provide Quarterly Technical Health Reports derived from the service, made available to the Customer via the Customer Portal. The Technical Health Assessment Report will consist of a Microsoft Word report that includes information specific to the Customer, outlining the critical alerts that have been identified and areas for optimization. An average report will consist of circa 15 pages as well as additional appendices, the number and length of which are determined by the number of critical alerts found that quarter. The report will be accompanied with a remediation playbook outlining some key areas to check for troubleshooting. Technical Reviews are made available to the Customer once every 3 months in the form of a remote meeting to go over findings from the health assessments and discuss remediation plan. All sessions and reporting are provided to ensure full capabilities within the Customer's Darktrace deployment are reached and to provide best-practice guidance and tailored recommendations.

### 1.4 Remediation Playbooks

Together with the findings report, Customer will receive a remediation plan from our engineering team outlining how certain issues can be addressed in their environment. If the quarterly report reveals issues, it links the corresponding

remediation steps from the playbook and adds them as an appendix at the end of the Technical Health Assessment. Customers are encouraged to follow the remediation steps to rectify the problem identified. Active Customer remediation is an essential component of the Proactive Health Optimization - Standard Service.

### 1.5 Infrastructure Engineer

An Infrastructure Engineer will be assigned to a given deployment. The Infrastructure Engineer serves as technical guide for resolving problems, planning upgrades, solving visibility issues, and more. They work collaboratively with Customers' organizations to strategically optimize successful deployments and help realize optimal performance and growth. The assigned Infrastructure Engineer may change over the course of the Subscription Period.

### 1.6 Executive Review

Yearly executive reviews are made available to Customers in the form of remote meeting to highlight high level findings and achievements. A review of the Customer’s deployment health, engineer workshops, alerts overview, asset overview and an appropriate area of enrichment will be discussed in the meeting. The engineer will identify a set of objectives where it is recommended that Customer focuses their improvements next.

## Requirements

Proactive Health Optimization - Standard is only available to customers with an active Customer Portal account and Call Home connection. Below are the requirements for access in each coverage area:

1. /Network:
    - Customer must have access to managed switches that can support port mirroring. Alternatively, customers can use network TAP/Packet Brokers to send traffic to Darktrace for analysis.
    - Customer must have access to Firewalls to make necessary access rules.
2. /Email:
    - Customer must have access to a global or super admin account for their email tenant.
    - Customer must have access to Firewall to make necessary rules to allow communication with the Darktrace/Email instance
    - Darktrace/Email is only available to organizations with specific licenses due to Google Workspace restrictions on Third-Party Email Archiving: Google Workspace Enterprise or Enterprise for Education License (or above). Consult the relevant Product Guide on the Darktrace Customer Portal for other licensing restrictions
3. /Identity:
    - Customer must have Administrator permissions to authorize each Darktrace/Apps module. Please consult the relevant Product Guide on the Darktrace Customer Portal for App-specific requirements
4. /Endpoint:
    - Customer must have access to all endpoints where cSensors should be installed.
    - Customer must have access to firewalls to make necessary rules to allow communication between the sensors and the rest of the Darktrace deployment.
5. /OT:
    - Customer must have access to managed switches that can support port mirroring. Alternatively, customers can use the network TAP/Packet Broker to send traffic to Darktrace for analysis.
    - Customers must have access to Firewalls to make necessary rules.
    - For air gapped networks, customer must have access to those networks to be able to install Darktrace products.

6. /Cloud:

    - Customer much have access to an account on the Cloud Service Provider, with permissions required to make necessary changes.

## 2 Responsibilities

### 2.1 Shared Responsibility Model

Customers are advised that Darktrace may only offer advice on Darktrace products, and to check their coverage areas before requesting assistance.. It is Customer's responsibility to apply and maintain any recommendations offered by the Darktrace engineer as part of the Service, and Customer accepts that, if the recommendations are not followed, it may result in an associated reduced level of the Darktrace Offering.

Darktrace encourages Customers to be familiar with their existing security & network stack and be able to perform the actions outlined in the following RACI Matrix. The RACI table is to clarify the accountability and responsibility between Darktrace and Customer. The table below describes each role and activity/responsibility.

| **Role** | **Activity/Responsibility** | |
|---|---|---|
| **R – Responsible** | The party is responsible for implementation, owns the problem/project | |
| **A - Accountable** | Right to make decisions, signs, and improves work | |
| **C – Consulted** | Has information, resources, and/or capacities necessary to assist the job | |
| **I – Informed** | Must be informed of the results, but does not need to be consulted | |
| **Professional Services Roles & Responsibilities** | Darktrace | Customer |
| Service Setup & Configuration | RA | CI |
| Provision of guides to support troubleshooting | RA | CI |
| Prepare Darktrace system for component troubleshooting | RA | CI |
| Product Licensing | RA | CI |
| **Physical Components** | | |
| **Rack and Stack** | CI | RA |
| Configure network settings for appliance | CI | RA |
| Update SPAN or TAP that sends traffic to Darktrace appliance | CI | RA |
| Modify Firewall rules to allow communication with Darktrace infrastructure (Call Home) | CI | RA |
| Modify firewall rules to allow communication between Darktrace appliances | CI | RA |
| **Email Components** | | |
| Grant API permissions using a global admin user | CI | RA |
| Modify connector & journal rule | CI | RA |
| Keeping Darktrace/Email instance operational (Cloud-only) | RA | CI |
| **Sensor components** | | |
| Download sensor files from Customer Portal | CI | RA |
| Ability to access and deploy new virtual machines | CI | RA |
| Modify firewall rules to allow communication between Darktrace sensors and master instance | CI | RA |

| | | |
|---|---|---|
| Modify rules on endpoint to allow communication with Darktrace FQDN | CI | RA |
| Modify network load balance and mirroring session | CI | RA |
| **Identity Modules** | | |
| Ensure your domain has the required license for monitoring | CI | RA |
| Grant permissions to enable monitoring using an admin user account | CI | RA |
| Where applicable, create roles and apps | CI | RA |
| **Autonomous response** | | |
| Tagging | CI | RA |
| Autonomous mode | CI | RA |
| Reachability Testing | CI | RA |
| Enabling Darktrace/Email Actions | CI | RA |
| **Attack Surface Management** | | |
| Keeping Attack Surface Management environment operational | RA | CI |
| Maintaining up-to-date data in Darktrace/Attack Surface Management | CI | RA |
| **Proactive Exposure Management** | | |
| Setup & configuration | CI | RA |
| **Incident Readiness & Recovery** | | |
| Monitoring integrations status in the UI | CI | RA |
| Resolving integrations errors | CI | RA |
| **Data Quality and Health Check** | | |
| Generation of Technical Health Assessment | RA | CI |
| Schedule quarterly sessions | RA | CI |
| Resolve issue within Customer environment | CI | RA |
| Resolve issues within Darktrace environment | RA | CI |

## 2.2 Customer and Darktrace Roles

| Role | Responsibilities |
|---|---|
| **Customer Roles** | |
| Customer Portal Primary User | • Administration of customer contacts in the 'Client Management' section of the Customer Portal |
| Customer Portal Users | • Have access to internal systems to perform required installation steps.<br>• Perform regular checks of Darktrace data ingestion.<br>• Respond accordingly to Sys Status alerts to ensure optimal traffic quality and delivery.<br>• Maintain call-home connectivity with Darktrace for the duration of installation activity. |
| **Darktrace Roles** | |
| Infrastructure Engineer | • Timely response to all Customers' requests.<br>• Following Customer request, collation, and timely delivery of products in response to Customer raised requests.<br>• Respond to feedback and/or requests for further assistance via Customer Portal Tickets. |
| Regional Professional Services Manager | • Owner of Quality Assurance process.<br>• Ensures appropriate resources are available to provide coverage for the Service. |
| Escalation Point | • If Customer is not satisfied with the performance of the Engineer (in accordance with this Service Definition), Customer may seek escalation to the following positions as appropriate.<br>  ○ Customer Success Manager.<br>  ○ Director of Professional Services.<br>• Receives Customer issues and uses all reasonable endeavors to resolve the escalated issues.<br>• Provides regular updates on escalated issues until resolution is reached. |

### 2.3 Contact

For urgent inquiries, customers can call the Darktrace Customer Support helpline to request a call-back from Darktrace delivery team. Customers are advised that the Darktrace helpline follows strict verification protocols to protect our customers from potentially fraudulent communications. Callers must have an active and verified Darktrace Customer Portal account and will be authenticated by providing a 2FA code or answering security questions.

## 3 Assumptions and Exclusions

Darktrace will not be liable to provide services for any request(s) based upon:

i. improper use, site preparation, or site or environmental conditions or other non-compliance with applicable Documentation or these terms;
ii. failure or functional limitations of any non-Darktrace software or product impacting systems receiving Darktrace Hardware Support Services;
iii. malware (e.g. virus, worm, etc.) introduced by Customer;
iv. modifications or improper system maintenance or calibration not performed by Darktrace or authorized in writing by Darktrace;
v. fire damage, water damage, accident, electrical disturbances, transportation by Customer, or other causes beyond Darktrace's control; or
vi. use not in line with a proper manner or in conditions which adequately protect and preserve the Hardware.

NO ADVICE, ALERT, OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY CUSTOMER FROM DARKTRACE OR THROUGH OR FROM THE SUPPORT SERVICES SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED HEREIN OR IN THE MASTER SERVICES AGREEMENT. DARKTRACE SHALL NOT BE LIABLE FOR ANY ERRORS OR DELAYS IN THE CONTENT OR ALERTS AVAILABLE THROUGH SUPPORT SERVICES, OR FOR ANY ACTIONS TAKEN IN RELIANCE THEREON. THE CUSTOMER UNDERSTANDS AND ACKNOWLEDGES THAT NOT ALL ANOMALIES / INTRUSIONS MAY BE REPORTED.

By using this service, Customer acknowledges that Darktrace's ability to perform the Proactive Health Optimization - Standard Service depends upon Customer's timely performance of its obligations and cooperation, as well as the accuracy and completeness of any information and data provided to Darktrace. Where this Service Description requires agreement, approval, acceptance, consent, or similar action by either party, such action will not be unreasonably delayed or withheld. The Customer agrees that to the extent its failure to meet its responsibilities results in a failure or delay by Darktrace in performing its obligations under this Service Description, Darktrace will not be liable for such failure or delay.

Darktrace aims to notify Proactive Health Optimization - Standard customers with at least 72hrs notice of scheduled maintenance that is expected to exceed more than 1 hour in duration and would affect service delivery. Darktrace aims to notify customers as soon as reasonably possible of unexpected outages expected to exceed more than 1 hour in duration and would affect service delivery.

Customers utilizing a cloud/hosted environment for their Darktrace deployment acknowledge that these services are provisioned in accordance with Azure/AWS and as such, any outages or maintenance of this cloud infrastructure may affect service provision.