

Mainstream Digital Ltd
Mainstream Managed Security
Service Agreement
Appguard
Version 1.0
1st July 2024

This Agreement applies to the provision to you, (the "Customer"), by us, Mainstream Digital Limited, a company incorporated in England and Wales with Company Number 02742235 whose registered office is at 701 Stonehouse Park, Sperry Way, Stonehouse, Gloucestershire, GL10 3UT

Definitions of the terms used in this Agreement are detailed in the Definition's document that can be found in Terms & Conditions at www.msdigital.com

1. Scope of this agreement

This document provides details agreements related to Mainstream Managed Security Service – Appguard Platform

2. Definition of Service

The service is a managed service using the Application Guarding product Appguard. The service is managed by the Mainstream Security Operations Centre (MSOC).

3. Service Installation & Setup

3.1 The Appguard Licences will be applied remotely to the clients nominated MS Windows Clients and Servers in accordance with the clients estate coverage requirement.

3.2 The installation will be enacted in two stages.

3.2.1 – Discovery Phase, where the service is left to operate in non-intrusive mode. This period will be at the agreement of both parties, but typically operates for a period of 2 to 4 week.

3.2.2 – Operational Phase, where the service actively prevents events that are notified as security threats for each and every licenced MS Windows system assigned to the Appguard Management Console.

3.3 Mainstream may need to engage directly with the clients security teams and or any other managed service provider involved to create the Appguard Policies of protection.

3.4 Once the client environment is in Operational Mode Mainstream will monitor the event logs within its UK based operational centre.

3.5 Once in Operational Mode the client should inform the MSOC of any additional Windows systems added to the environment that require appropriate licensing.

3.6 Any information used by Mainstream is kept at a UK (England) secure data site, conforming to **ISO 27001** security standards.

4. Service Requirements & Data Collection

4.1 The service is designed to operate in any MS Windows environment where the MS versions are conformant to Versions **XP SP3** and above

4.2 Appguard is agnostic of all and any 3rd party applications, whether they are in-house or commercially available software platforms. During Discovery Mode all application events will guide the setup of Operational Policies.

4.3 Once policies are set, any changes to MS software or 3rd Party applications that break policy will be stopped. At this point the MSOC will review required policy adjustments as per section 6.

5. Alerts & Support

5.1 In agreement with the client the Appguard service will be configured to display events according to the client requirements. This is aimed to reduce event signalling noise but not limit Zero Trust Protection. Mainstream will review all Level 4 events, which indicate a newly triggered event that requires investigation.

5.2 In the event of a Level 4 event alert the client may find that the software generating that event is either partially or fully malfunctioning. This only occurs in production mode and will require adjustments to the Policy applied by Appguard. **Normal hours of support are 09:00 – 17:30 unless other contractual arrangements are in place.**

6. Policy Management

6.1 Policies are designed to inhibit actions/events which are not implicitly trusted and therefore appear to be suspicious and treated accordingly.

6.2 Changes to Policy may be required when the client is either installing or upgrading 3rd party services.

6.3 Where the client is knowingly upgrading or newly installing 3rd party software, it is recommended that a Discovery Bubble is created

6.3.1 A Discovery Bubble allows both the client and Mainstream to assess Policy change without interruption to the clients operational environment

6.3.2 Where setting up a Discovery Bubble is not possible, Mainstream will advise in writing potential impacts to the client operations with the intent to ensure both parties acknowledge any risk this may create.

6.4 Policy changes will be distributed by Mainstream from the Service console once both parties are in agreement of the new Policy.

7. SOC Integration

7.1 Where required Mainstream will facilitate any requested feed to the clients existing SIM/SIEM services.

7.2 All clients running existing malware detection systems may find that Appguard has causes to block such tools. Discovery mode will pick up on this, but changes to the 3rd malware services as a result of upgrades may result in alerts which require immediate investigation.

7.3 Under this agreement Appguard is not responsible for the removal of viral code and viral load inside the client environment. Removal must be affected by the clients chosen anti-virus service.

8. Connectivity

Once policies are distributed and active on all ends points the clients and servers are protected and application guarding is active. If there is interruption to the network connectivity such that event/alerts cannot be forwarded, the service will continue to Guard via the policies. New policy updates will not be operational until connectivity is restored.

9. Risk acknowledgement

9.1 The MSOC cannot offer guaranteed 100% protection from attack. It aims to apply Trust and

Guarding within the boundaries of MS and 3rd Party software.

9.2 Zero Trust policy softening will be discussed with the client and the MSOC will, as necessary, separately assess and document risks associated.

9.3 The MSOC cannot be held responsible for digital intrusion not managed by the Trust Policies.

10. Commercial Terms

10.1 The Appguard service is a monthly service rental with a fixed duration commitment.

10.2 Cancellation of the service ahead of the term will be subject to 100% of the fees due.

10.3 On cancellation the clients setup will be disconnected from the Mainstream Appguard Service and the client will be advised on how to remove the policy event collectors from their systems.

10.4 The client will be billed annually or monthly as agreed ahead of commencement of the service.