ArmorPoint Sandbox Detonation

Service Agreement

Contents

ArmorPoint Sandbox Detonation Service Scope

SERVICE OVERVIEW

Service Description

The ArmorPoint Sandbox Detonation service is an enhancement to existing ArmorPoint Managed SOC solution subscriptions, designed to provide advanced URL and file analysis capabilities for organizations seeking to strengthen their cybersecurity posture. This service enables Clients to submit suspicious or potentially malicious files or URLs to a secure, isolated sandbox environment, where automated behavioral analysis is performed. Each detonation generates a comprehensive report detailing observed behaviors, indicators of compromise, and risk assessments, empowering your security team with actionable intelligence.

By leveraging ArmorPoint Sandbox Detonation, your organization benefits from enhanced threat detection, reduced false positives, and enriched SOC intelligence, supporting faster, more accurate incident response and improved overall security outcomes.

Service Prerequisite

The ArmorPoint Sandbox Detonation service supplements an existing ArmorPoint Managed SOC solution subscription. No detonations are included or available without an active ArmorPoint service subscription.

DETONATION ALLOCATIONS

Included Detonations by Service Tier

As part of your ArmorPoint service subscription, you receive a specific quantity of URL and file detonations per month based on your service tier.

ArmorPoint Service Subscription	Monthly Detonation Allocation
360	50 detonations
Open360	50 detonations
MDR/XDR	25 detonations
Core	10 detonations

Detonation Reset and Rollover Policy

Detonation limits are reset on the 1st or 15th of each month. Unused detonations within the month are not carried over to subsequent months unless otherwise agreed in writing.

ADDITIONAL DETONATION PACKAGES

For organizations with higher analysis needs, additional detonation packages are available for purchase. Additional detonations will be sold as an add-on service and require an amendment to your existing service agreement.

Minimum Purchase Requirements

Detonation packages must be purchased with a minimum of 25 detonations. After the 25-detonation minimum is met, additional sandbox detonations may be increased by unit of 1 with no limitation on the maximum cap. Additional detonation packages are purchased for the remainder of the existing contract term.

DETONATION SUBMISSION AND REPORTING

Submission Process

The service enables the secure submission and automated analysis of URLs or files in an isolated sandbox environment. Each detonation consists of the submission, analysis, and reporting of a single URL or file.

Detonation Reports

Every detonated URL or file receives a comprehensive analysis report. Each report details observed behaviors, indicators of compromise, and risk assessments. Detonation reports are delivered through the ArmorPoint Platform and are accessible to authorized Users.

COMPATIBLE FILE TYPES AND SIZE LIMITATIONS

Maximum File Size

The maximum size for files submitted for review using the ArmorPoint Sandbox Tool is 100 MB.

Supported File Types

The ArmorPoint Sandbox Detonation service supports the following file types:

File Types	Archive File Types
MZ/PE files [executable]	7z
MS Excel	ACE
MS PowerPoint	ALZip
MS Word	ARJ
PDF	AR
RTF	BZip2
Batch	GZip
URL [binary]	MS Cabinet
HTML	LHA
XHTML	Linux TAR
MHTML (doc)	MSI
MHTML (xls)	RAR
MHTML (ppt)	UnixZ
JS	ZIP
VBS	ZIP (multivolume)
PIF [executable]	ZOO
JAR [archive]	XZ
PS1	PKZIP
	cpio

	LZMA Compressed Archive LIB Lzip LRZip LZOP Zstandard Brotli

Extractable Email Attachments

The service can parse and extract attachments from email formats and documents:

Format	Description
EML	Generic Format (RFC822)
TNEF	Microsoft Proprietary Format

Document Attachment Extraction

The service parses and extracts attachments from the following documents:

- MS Excel
- MS PowerPoint
- MS Word
- MS OneNote

SCOPE AND LIMITATIONS

The ArmorPoint Sandbox Detonation service is subject to the following scope and limitations:

- The service is intended for the analysis of URLs or files reasonably suspected to be malicious or suspicious.
- The sandbox environment is isolated and does not interact with production systems.
- The service does not guarantee detection of all threats or prevention of all security incidents.
- Detonation analysis is automated and may not identify all malicious behaviors, particularly for advanced or evasive threats.
- The service is designed to enhance threat detection and enrich SOC intelligence but does not replace comprehensive security controls or incident response procedures.

ArmorPoint reserves the right to refuse detonation of files that violate applicable laws or regulations, or that pose undue risk to the sandbox environment.

CONFIDENTIALITY AND DATA HANDLING

All URLs and files submitted for detonation, as well as resulting analysis reports, will be managed in accordance with the confidentiality and data protection provisions of the Client's existing ArmorPoint Managed SOC service agreement.

ArmorPoint will maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of submitted files and analysis reports. Submitted files and reports will be retained in accordance with ArmorPoint's standard data retention policies and the terms of the Client's service agreement

Contractual Changes

This Service Agreement may change and ArmorPoint may update this Service Agreement from time to time. It is your responsibility to check this Service Agreement periodically for changes.

The following Governance structure defines the Contract Change Process:

Change To	Vehicle	Process
Service scope	Change of scope presented with justification and supporting data. Changes that cause a change to the monthly cost to Client of more than $1,000 will require further Executive Approval through a Contract Change process.	Order Form
New project or effort	Each proposed effort or initiative will be presented to executive leadership and/or board with supporting charter, solution outline and estimates.	Order Form
Change to the overall service requirements and performances	Each change will be presented to the Executive and be processed with further Executive Approval	Contract CCR or Addendum
Change to the scope, terms, and conditions of the current	Each change will be presented to the Executive and be processed with further Executive Approval	Contract Addendum

This Service Agreement is supplemental to and governed by the terms of the Master Services Agreement between Client and ArmorPoint. In the event of conflict, the Master Services Agreement shall prevail except where this Service Agreement explicitly modifies those terms.

Exclusions

The following exclusions apply to the scope of the work stated above:

- Custom investigations or threat hunting services beyond automated detonation analysis
- Custom data analysis or reporting services related to detonation results
- Integration with third-party security tools or platforms not expressly provided for herein
- Training or consulting services related to threat analysis or sandbox usage
- Implementation of technology, including software agents, is not included within the Service Agreement
- Any work or services not expressly provided for herein
- Any application development or integration efforts not expressly provided for herein
- Any actual hardware purchases for on-premises needs
- Any migration or upgrade of Client infrastructure (servers, network, etc.)
- Any actual implementation of the recommendations made by ArmorPoint unless specified in this document
- Any data recovery and forensics work due to purposeful or malicious Client or application errors
- Any software license or physical hardware expenses
- Any software license that is not explicitly mentioned, and not covered by ArmorPoint
- All Travel and lodging costs
- Any fees related to shipping, handling, customs, duties and/or taxes
- Any additional work requested beyond the scope of this Agreement will be expressly set forth by subsequent agreement, including, but not limited to, a Contract Change Request (“CCR”)

Revision History

Document Version	Published Date	Description or Notes
1.0	12.17.2025	Initial Publication Date