Malware Analysis Service Success Plan

MAXIMIZING THE VALUE OF YOUR APPGATE MALWARE ANALYSIS SERVICE SUBSCRIPTION

Introduction

Appgate's Malware Analysis Service is a confidential, powerful tool that can mitigate the risk of malware-based threats, providing significant value for any organization. However, to achieve maximum benefits, it is important to understand how to effectively use its feature set and findings.

To that end, this success plan is a comprehensive blueprint to help you optimize your cybersecurity investment. Our confidential, personalized approach offers customized services, specialized expertise and actionable insights to harden your security posture, mitigate cyberthreats and help you achieve your goals.

To strengthen your defenses, findings from the Malware Analysis Service Rapid Analysis or Deep Analysis reports should be fully integrated into your cybersecurity protection methods. This means incorporating the findings into your security analysts' daily workflows. All generated reports are strictly confidential and only accessible to Appgate and authorized personnel from your organization. To ensure this, Appgate requires users to have approved email addresses associated with your organization.

Additionally, to gain ongoing attack insights, your team should submit every malware sample they find, unless they can trace it back to previously analyzed malware.

Subscriptions

Appgate's Malware Analysis Service provides flexible subscription packages designed to meet your specific organizational needs. The subscriptions include Rapid Analysis, Deep Analysis and a combination of both.

- Rapid Analysis options are available in packages of 50 and 100 submissions.
- Deep Analysis options are available in packages of 20 and 40 days.
- The combined Rapid and Deep Analysis options are available in packages of combination of 10 and 3, and 50 and 10, respectively.

The analyses are time-bound for 12 months, except for the combined Rapid and Deep Analysis package (10 and 3) which is for 60 days. For most organizations, we strongly recommend a combination of Rapid and Deep Analysis to get the most of out the service in terms of quick time-to-value, and deeper levels of examination through an engagement with Appgate's Malware Analysis team.

Getting Started

Appgate will work with your designated primary point of contact to establish access to the Malware Analysis Service. Appgate will also request a secondary point of contact, who can act as a backup. Both contacts will be registered as Appgate customers. Given the sensitivity of the service, please inform Appgate of any changes in user access needs, including provisioning or revoking access.

Once accounts are activated, authorized users can submit malware samples for analysis, and subsequently view your organization's historical reports, stored in the system's dashboard. Any desired restrictions on these requests should be managed by your organization.

Logging in

To log in, users will receive an email from mas.no-reply@appgate.com with a website link and instructions. Users should click the link provided in the email and will be prompted to enter their email address, create a password and set up a second authentication factor. This additional layer of security will ensure that only authorized users can access your organization's sensitive information.

YOUR ROADMAP TO CYBERSECURITY RESILIENCE

- **Accelerate Outcomes:** Experienced success managers assist you in executing outcome-focused plans and identify ways to strengthen your cybersecurity posture with Appgate's Malware Analysis Service.
- **Enable Your SOC:** Integrate the service into existing security operations workflows to enhance threat detection and response capabilities.
- **Malware Research:** Enhance your malware defense strategy by equipping your Security Operations Center (SOC) team with advanced malware analysis expertise and helpful techniques.
- **Maximize Your ROI:** Gain unparalleled guidance on malware threat management and program execution to fully leverage the benefits of Appgate's Malware Analysis Service.

Using the Service

To achieve optimal benefits, Malware Analysis Service report findings should be integrated into your team's existing analytical process.

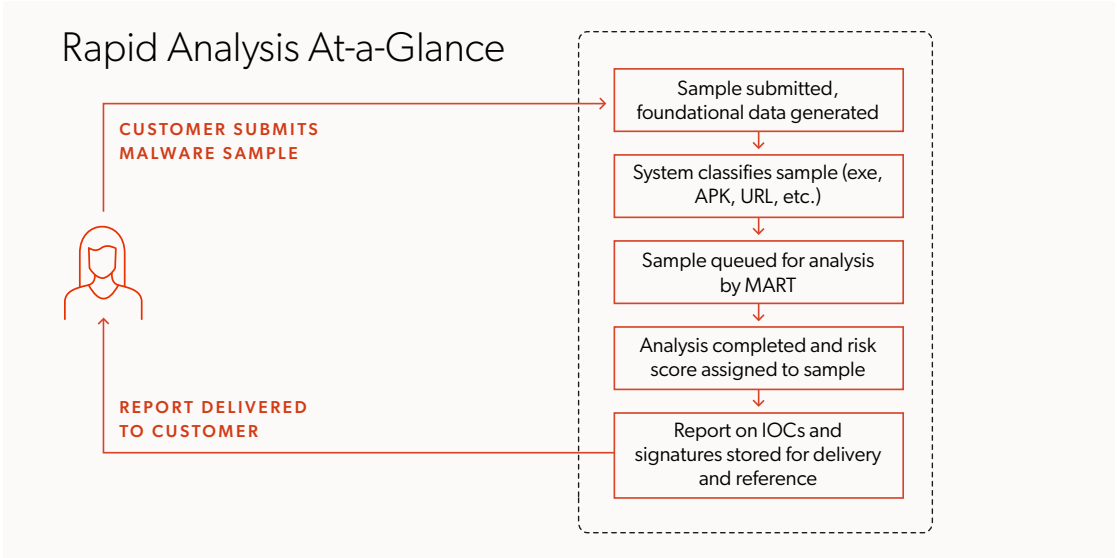
When a team member finds a suspected malware sample, they should follow established procedures to identify and isolate it. Depending on your organization's protocols, this may involve escalating the issue to a higher analytical tier for validation before submitting the sample for analysis.

Requesting an Analysis

Depending on your subscription, the team member should log into the service and select Rapid Analysis to begin analyzing the suspected malware. This approach keeps costs down and delivers the report and any associated indicators of compromise (IOCs) quickly.

To submit the sample for Rapid Analysis:

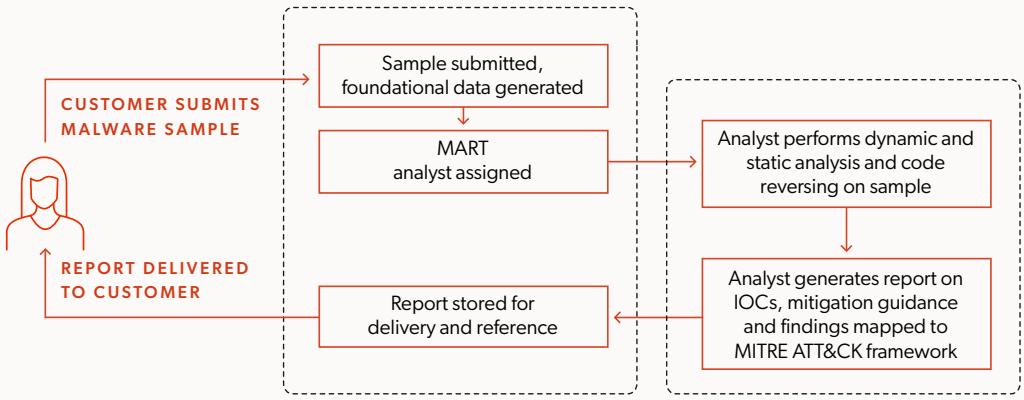
- Use the Malware Analysis Service interface to submit the sample in a file, hash or URL format.
- The Malware Analysis Service automatically analyzes malware sample submissions through a series of automated processes, tools and systems.
- The analysis includes static and dynamic analysis, rule- and signature-based identification, threat intelligence and IOC reports, detection of targeted brands, and more.
- Rapid Analysis reports for most malware samples are available within 30 minutes and will include specific details on filenames, hashes, timestamps, filetypes, Command-and-Control (C2) servers, useful strings, images, and more.
- You can login to the service to retrieve the report, or have the report emailed to you directly; the report will be delivered to the email of the person submitting the request.
- The report will also be maintained in your organization's list of reports, so you and others within your organization will be able to review the reports within the interface.



If you require more information than what is provided in the Rapid Analysis or are limited to a Deep Analysis-only subscription, submit the sample for Deep Analysis. Alternatively, consider upgrading your subscription to include Deep Analysis if you currently only have the Rapid Analysis option. The Deep Analysis report will always be emailed to the submitter and stored in your organization's repository. To submit the sample for Deep Analysis:

- Use the Malware Analysis Service interface to provide specific details about the sample and select Deep Analysis.
- Our Malware Analysis and Research Team (MART) will reverse-engineer malware to uncover customer-specific attack details.
- The team meticulously analyzes communication with C2 servers and pinpoints malware functions such as process injection, web injections and cryptography. A detailed Deep Analysis report provides comprehensive insights including threat behavior and Tactics, Techniques, and Procedures (TTPs).
- Deep Analysis reports are typically delivered in one to three days but may be longer depending on the complexity of the submitted sample.
- The report will be emailed directly to the person submitting the request.
- The report will also be maintained in your organization's list of reports for future reference by you and others within your organization.

Deep Analysis At-a-Glance



Leveraging the Results

Once the analysis is complete and the results are delivered, you can use the IOCs to strengthen your protection grid by adding detection/block rules, as needed. In addition, if a compromise is confirmed or suspected, leverage the indicators and signatures to proactively hunt for malware across your environment.

Tracking Value

We recommend that you evaluate the IOCs themselves, to verify that they are enabling you to detect and mitigate threats; some IOCs are much more valuable than others. Note: The value of the Malware Analysis Service lies in its confidentiality, ensuring that discovered malware is not publicized to external parties. As you integrate the indicators, you can fine-tune their usage and identify the ones with the highest value and those that are of lower value. These insights should be incorporated into your protection and threat hunting capabilities.

Track the specific details of your efforts to ensure the reports are adding value and that you can demonstrate their success to the business. Monitor the impact of your hunting efforts, and how the reports expand your security tools' reach. Sharing these success stories will foster a stronger cybersecurity culture throughout your organization and build a reputation for success.

Usage Reports

Appgate will provide monthly reports (or on-demand reports upon request) detailing your organization's use of the Malware Analysis Service. These reports will help you to track usage and make informed decisions about when to renew the service. Appgate will provide an additional report when you are within five automated reports or within one month of reaching the end of your contract.

Engaging With Your Customer Success Manager

Appgate Customer Success Managers are your partners in maximizing the value of your reports and providing valuable feedback to Appgate. As you roll out the service, weekly check-ins can facilitate seamless integration. Then quarterly check-ins will ensure you are fully taking advantage of the analyses provided.

Providing Malware Analysis Service Feedback

We want to hear from you! Contact your Customer Success Manager or submit direct input about our Malware Analysis Service by sending comments to mas.support@appgate.com. We are constantly working to enhance its value by adding features that will help you bolster your cybersecurity resilience and deepen your understanding of potential vulnerabilities.

About Appgate

Appgate secures and protects an organization's most valuable assets and applications. Appgate is the market leader in Zero Trust Network Access (ZTNA) and online fraud protection. Appgate products include Appgate SDP for Universal ZTNA and 360 Fraud Protection. Appgate services include threat advisory analysis and ZTNA implementation. Appgate safeguards enterprises and government agencies worldwide. Learn more at appgate.com.

appgate