ESET Tech Center

ESET LiveGuard Advanced FAQ

Mitch | ESET Nederland - 2022-10-24 - Reacties (0) - ESET LiveGuard Advanced (ESET Dynamic Threat Defense)

Solution

ESET LiveGuard Advanced operation | Security and Privacy

ESET LiveGuard Advanced Operation

1. How does ESET LiveGuard Advanced determine which samples to send for analysis?

a. When an ESET LiveGuard Advanced compatible ESET product detects a new sample, it is automatically scanned using the multilayer ESET scanning engine.

b. If the result is not 100% malicious or 100% clean, your product decides if the sample should be analyzed in ESET LiveGuard Advanced.

c. If the sample can be analyzed, a hash is sent to ESET to check if the file has already been analyzed in ESET LiveGuard Advanced.

d. If ESET has not yet received this sample, it will be sent to ESET for analysis.

e. Metadata from your ESET product are sent to ESET PROTECT (or ESET Security Management Center) for administrator visibility.

2. How are sample results received by ESET products after they have been analyzed in ESET LiveGuard Advanced?

a. Sample test results are sent to the ESET Cloud running in MS Azure.

b. All ESET LiveGuard Advanced compatible products check ESET Cloud periodically for recent results.

c. If a new result is available, the hash and result are saved, and if applicable, an action is taken.

3. Does Mail Security send internal email samples to ESET LiveGuard Advanced or only external email samples?

ESET Mail Security scans all emails. However, ESET LiveGuard Advanced only scans emails received from outside of the organization.

4. What if ESET LiveGuard Advanced detects a threat in a sample you know to be clean?

If a threat is detected in a known clean sample, the product will most likely have remediated the threat and put the sample in Quarantine. If this happens, the admin can exclude the sample by clicking on the sample in **Submitted Files** and selecting **Add exclusion to Policy**. After that, create a task to move the sample out of quarantine. The sample will never be scanned again.

5. Can I select the files that I will submit to ESET LiveGuard Advanced?

The Admin can select from five categories of file types that will be sent from each ESET product using a policy. The file types include Executables, Archives, Scripts, Documents, and others. The admin can also create an exclusion list based on file extension or directory.

6. Which file types does ESET LiveGuard Advanced support?

ESET LiveGuard Advanced can analyze any file. However, only files that can harm a computer, contain or download malicious content are automatically sent for analysis. ESET specifies that executables, scripts and documents are supported in the event files are stored in an archive.

7. Which operating system environments can use ESET LiveGuard Advanced for analysis in a controlled environment?

ESET LiveGuard Advanced works with supported ESET security products on Windows and Linux. The analysis starts on the operating system, where the sample has the highest chance to do harmful actions. Parameters cannot be manually defined.

8. How will I receive notifications about the availability status of ESET LiveGuard Advanced after it is enabled?

When ESET LiveGuard Advanced is not available, notifications about its protection status will be displayed in the Status Overview section in ESET Security Management Center.

9. Does ESET LiveGuard Advanced require that I allow additional IP addresses through my firewall?

Visit our Knowledgebase article for the list of all required addresses and ports for ESET products.

10. Where can I see the samples that I sent to ESET LiveGuard Advanced?

To view the samples that were sent to ESET LiveGuard Advanced as well as other data that was sent to ESET, including LiveGrid and diagnostics data, log in to ESET PROTECT (or ESET Security Management Center) and click **More → Submitted Files**.

11. Where can I see the emails that have been postponed for delivery while ESET LiveGuard Advanced completes an analysis?

ESET Mail Security for Exchange postpones delivery of email for a pre-defined time or until the results are received. The list of postponed mail is available in the Mail Security for Exchange user interface under **Tools → ESET LiveGuard Advanced**.

12. How long does it take ESET LiveGuard Advanced to analyze a sample?

It typically takes up to 5 minutes to analyze a sample that has never been analyzed by ESET LiveGuard Advanced before. If a sample has already been analyzed, the result will be received in the next product request cycle, which can take up to 2 minutes.

13. How often is ESET PROTECT updated with ESET LiveGuard Advanced status changes?

ESET PROTECT refreshes in 1-minute intervals, which updates the newly sent sample data and associated results.

Security and Privacy

1. How are documents kept secure when they are sent from an ESET product to ESET LiveGuard Advanced?

All samples are encrypted and sent through HTTPS. They are then stored on a dedicated storage server with limited access by ESET employees for the pre-defined time set by the sender's computer policy, after which they are deleted or stored securely.

2. Is the information anonymized in any way?

The data arrives in an anonymous format: our systems only have access to the customer ID from their ESET Business Account or ESET MSP Administrator. However, the customer ID is not associated with the data sent from a specific computer that has sent a sample for analysis. By default, the customer ID and the customer name are not available to any employee.

3. In which regions are ESET LiveGuard Advanced processing servers and storage hosted?

All samples are sent to ESET HQ, located in Bratislava, Slovakia, Europe.

When the analysis is finished, the hash and result are stored in the ESET Cloud, which runs on an MS Azure data center hosted in the US and Europe. All computers request the results from MS Azure, not ESET HQ.

4. How are samples from ESET LiveGuard Advanced handled?

When the samples sent to ESET LiveGuard Advanced are received, they are stored on a dedicated storage server with exceptional security. They are not stored on the same server as the LiveGrid samples. As an additional layer of security, only selected employees have access to the ESET LiveGuard Advanced samples. Since this is your data, you determine when the clean samples should be deleted from our servers when analyzed. This setting is located in your product and includes the following delete options:

- Never
- After 30 days
- Immediately after analysis

This option is available only when you've purchased the ESET LiveGuard Advanced service. Document samples are always deleted from ESET servers. Note that if the sample is found to be malicious, it will be kept for further analysis and to enhance our detection systems.

5. Why should I opt to allow ESET to keep samples for 30 days after analysis?

As ESET Machine Learning models or Scanning Engine are updated, a sample that was classified as clean might be reclassified as Suspicious or Malicious. If this occurs, we will re-analyze stored samples and notify you with the updated result, which detects a new type of advanced persistent threat in your infrastructure.

6. Are the samples or metadata that is sent to ESET LiveGuard Advanced shared with third-party entities?

No. We cooperate with other vendors to exchange malicious samples sent via LiveGrid to improve our knowledge. However, samples sent to ESET LiveGuard Advanced are never shared with other parties. ESET does not share any samples or metadata sent to ESET LiveGuard Advanced with any third-party entity. We believe in consumer privacy and have put in place countless measures to be considered a trustworthy partner with whom you can trust your data. All samples always stay in ESET HQ, and all hardware is owned by and located in ESET facilities, which stores or processes samples.

7. How long does ESET LiveGuard Advanced keep submitted samples and documents?

When ESET LiveGuard Advanced is purchased, the administrator can set the per-computer policy to delete samples like executables, scripts, archives, or others immediately after analysis, after 30 days, or never if the result is clean. For documents, the admin can set only immediately after analysis or after 30 days after the result of the analysis is clean. If the sample is detected as suspicious or worse, we'll keep the sample for further analysis. We're also keeping metadata for improving the service.

8. What happens if one data center becomes temporarily unavailable?

At ESET HQ, where we're analyzing your data, all systems are in high-availability mode and under 24/7/365 monitoring.

For the ESET Cloud in Microsoft Azure, all systems are in a high-availability mode within a data center. The systems in our data centers are under 24/7/365 monitoring. If the US or Europe data center is not available, they are still in high-availability mode between each other, and all information is synchronized among data centers. Therefore no degradation of service should ever occur. As a precaution, however, all samples are stored in a queue, and after they are processed, the results are delivered as soon as possible.

9. Which data does ESET store in the Azure Cloud?

ESET stores in the Azure Cloud the following data:

- Customer ID
- Data visible in ESET PROTECT (or ESMC):
    - Hash of sample
    - The result (status)
    - Category (file type)
    - State of analysis
    - Size of the analyzed file
- Other internal statistical data

10. Where are the Terms of Use and Privacy Policy documents for ESET LiveGuard Advanced?

- Terms of Use
- ESET Management Agent EULA
- Data Processing Agreement
- Standard Contractual Clauses
- Privacy Policy
