ESET Tech Center

ESET Dynamic Threat Defense (EDTD) FAQ - operation, security, and privacy

Anish | ESET Nederland - 2018-08-20 - Reacties (0) - FAQ's

Solution

ESET Dynamic Threat Defense operation

1. How does ESET Dynamic Threat Defense determine which samples to send for analysis?
2. How are sample results received by ESET products after they have been analyzed in ESET Dynamic Threat Defense?
3. Does Mail Security send internal email samples to Dynamic Threat Defense or only external email samples?
4. What if ESET Dynamic Threat Defense detects a threat in a sample you know to be clean?
5. Can I select the files that will be submitted to ESET Dynamic Threat Defense?
6. Which file types are supported by ESET Dynamic Threat Defense?
7. Which operating system environments can use ESET Dynamic Threat Defense for analysis in a controlled environment?
8. How will I receive notifications about the availability status of ESET Dynamic Threat Defense after it is enabled?
9. Does ESET Dynamic Threat Defense require that I allow additional IP address through my firewall?
10. Where can I see the samples that were sent to ESET Dynamic Threat Defense?
11. Where can I see the emails that have been postponed for delivery while ESET Dynamic Threat Defense completes an analysis?
12. How long does it take ESET Dynamic Threat Defense to analyze a sample?
13. How often is ESET Security Management Center updated with Dynamic Threat Defense status changes?

Security and Privacy

1. How are documents kept secure when they are sent from an ESET product to Dynamic Threat Defense?
2. Is the information anonymized in any way?
3. In which regions are Dynamic Threat Defense processing servers and storage hosted?
4. How are samples from Dynamic Threat Defense handled?
5. Why should I opt to allow ESET to keep samples for 30 days after analysis?

6. Are the samples or metadata that is sent to ESET Dynamic Threat Defense shared with 3rd party entities?
7. How long does ESET Dynamic Threat Defense keep submitted samples and documents?
8. What happens if one data center becomes temporarily unavailable?
9. Which data stores ESET in the Azure Cloud?

ESET Dynamic Threat Defense Operation

1. **How does ESET Dynamic Threat Defense determine which samples to send for analysis?**
    1. Once an ESET Dynamic Threat Defense compatible ESET product detects a new sample, it is automatically scanned using the multi-layer ESET scanning engine.
    2. If the result is not 100% malicious or 100% clean, your product decides if the sample should be analyzed in Dynamic Threat Defense.
    3. If the sample can be analyzed, a hash is sent to ESET to check if the file has already been analyzed in ESET Dynamic Threat Defense.
    4. If ESET has not yet received this sample, it will be sent to ESET for analysis.
    5. Metadata from your ESET product are sent to ESET Security Management Center for administrator visibility.
2. **How are sample results received by ESET products after they have been analyzed in ESET Dynamic Threat Defense?**
    1. Sample test results are sent to the ESET Cloud running in MS Azure.
    2. All ESET Dynamic Threat Defense compatible products check ESET Cloud periodically for recent results.
    3. 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 Dynamic Threat Defense or only external email samples?**

ESET Mail Security scans all emails, however Dynamic Threat Defense only scans emails received from outside of the organization.

1. **What if ESET Dynamic Threat Defense 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.

1. **Can I select the files that will be submitted to ESET Dynamic Threat Defense?**

The Admin can select from 5 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.

1. **Which file types are supported by ESET Dynamic Threat Defense?**

Any file can be analyzed by ESET Dynamic Threat Defense. However, only samples that can harm a computer or contain or can download malicious content are automatically sent for analysis. So we specify that executables, scripts, and documents are supported (also in case they are stored in an archive).

1. **Which operating system environments can use ESET Dynamic Threat Defense for analysis in a controlled environment?**

The available OS are Windows 10, Windows 7, and Windows XP. The analysis starts on one, where the sample has highest chance to do harmful actions. It's not possible to define this parameter manually.

1. **How will I receive notifications about the availability status of ESET Dynamic Threat Defense after it is enabled?**

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

1. **Does ESET Dynamic Threat Defense require that I allow additional IP address through my firewall?**

Visit our Knowledgebase article for the list of all required addresses and ports for ESET products: https://support.eset.com/kb332/

1. **Where can I see the samples that were sent to ESET Dynamic Threat Defense?**

To view the samples that were sent to ESET Dynamic Threat Defense as well as other data that was sent to ESET, including LiveGrid and diagnostics data, log in to ESET Security Management Center and click **More** → **Submitted Files**.

1. **Where can I see the emails that have been postponed for delivery while ESET Dynamic Threat Defense 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 Dynamic Threat Defense**.

1. **How long does it take ESET Dynamic Threat Defense to analyze a sample?**

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

1. **How often is ESET Security Management Center updated with Dynamic Threat Defense status changes?**

ESET Security Management center 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 Dynamic Threat Defense?**

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

1. **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. However, the customer ID is not associated with the data sent from a particular computer that has sent a sample for analysis. By default, the customer ID and the customer name are not available to any employee.

1. **In which regions are Dynamic Threat Defense processing servers and storage hosted?**

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

Once 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 in Europe. All computers request the results from MS Azure, not ESET HQ.

1. **How are samples from Dynamic Threat Defense handled?**

Once the samples sent to Dynamic Threat Defense 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 select employees have access to the Dynamic Threat Defense samples. Since this is your data, you determine when the clean samples should be deleted from our servers once they have been 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 ESET Dynamic Threat Defense service. Document samples are always deleted from ESET servers. Please note that if the sample is found to be malicious, it will be kept for further analysis and to enhance our detection systems.

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

It is possible that as our 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 update result, which detects a new type of advanced persistent threat in your infrastructure.

1. **Are the samples or metadata that is sent to ESET Dynamic Threat Defense shared with 3rd party entities?**

No. We cooperate with other vendors to exchange malicious samples sent via LiveGrid to improve our knowledge. However, samples sent to Dynamic Threat Defense are never shared with other parties. ESET does not share any of the samples or metadata sent to Dynamic Threat Defense with any 3rd 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.

1. **How long does ESET Dynamic Threat Defense keep submitted samples and documents?**

Once Dynamic Threat Defense is purchased, the administrator can set 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, 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.

1. **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 once processed the results are delivered as soon as possible.

1. **Which data stores ESET in the Azure Cloud?**
   ESET stores in the Azure Cloud following data:

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