Cloud Sandbox

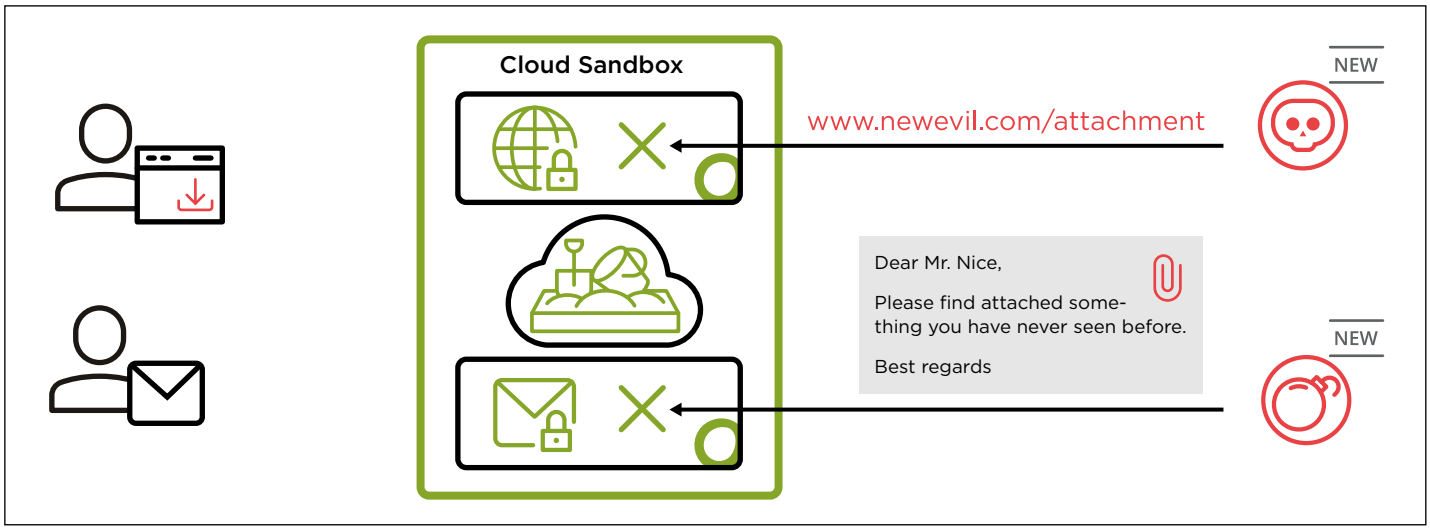
PRODUCT BRIEF

Protect your users from previously unknown malware

Detect and defend against brand new malware

Unknown malware is a challenge for standard protection products
Every day, more than 350,000 new malware attacks are registered. As malicious hackers use diverse strategies to evade detection by traditional threat protection and file scanning appliances and programs, there are thousands of files every day that can't be classified through a standard malware scanning approach. Their file hash can't be found in common malware hash databases, and general antivirus methods are not conclusive.

Identify zero-day attacks effectively through the Cloud Sandbox
The Cloud Sandbox consists of general and heuristic methods as well as an intelligent neural network that takes over 8,600 file attributes into account to determine whether a new, unknown file contains malware. The Cloud Sandbox is trained through machine learning and is continuously improved with every new file that is uploaded for analysis.



The Cloud Sandbox protects users against new malware in files on the web or in email attachments

Why choose Cloud Sandbox by Open Systems?

Defend against the unknown

The Cloud Sandbox is an additional, advanced layer of web and email security which protects your business against breaches and data loss from today's sophisticated threats – even if they are brand new and previously unknown.

Leading technology

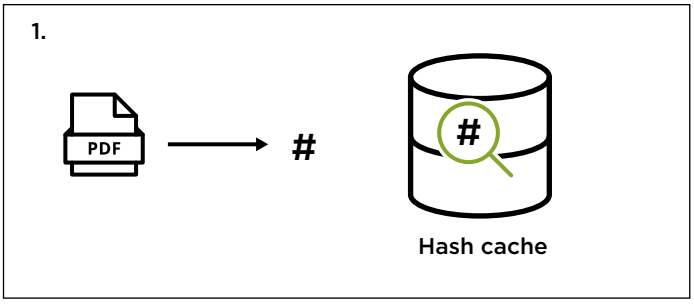
Over 99.99% of malware is successfully detected by industry-leading intelligence of the neural network. It analyzes over 8,600 file attributes and is continuously trained for an effective and up-to-date malware radar.

Built-in protection

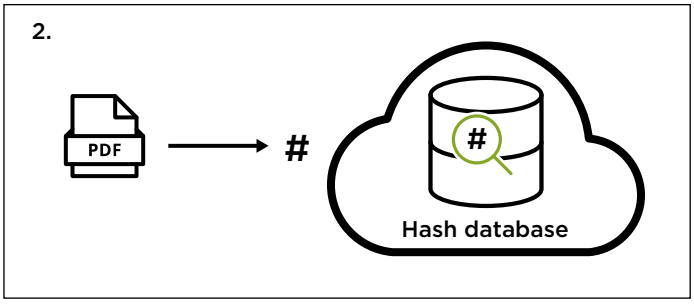
Seamlessly integrated into standard file scanning of Secure Web Gateway and Secure Email Gateway, the Cloud Sandbox helps identify malware whenever the hash lookup or heuristics are not conclusive.

When Cloud Sandbox comes into play

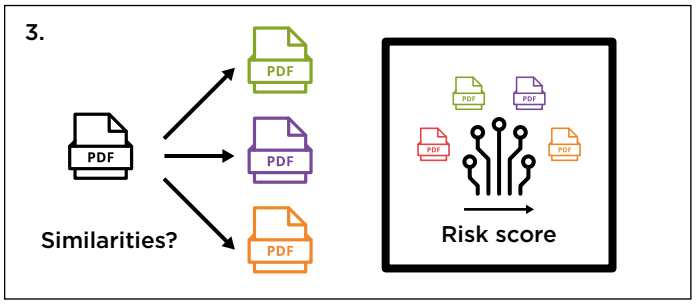
After conventional malware scanning is done, the following happens



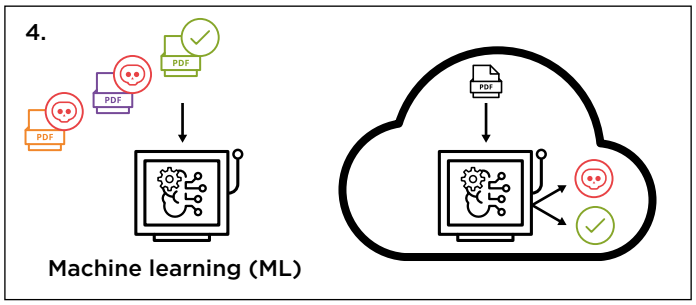
First, a unique file hash is calculated for the email attachment or file downloaded from the web. This file hash is checked against a local hash cache which contains known bad and known good hashes.



Then, if the local cache does not know the file already, the file hash is additionally looked up in the large, global cloud database.



If the hash can't be located in any database, the local engine calculates a risk score based on ML algorithms. Only if the risk level exceeds a certain threshold, the file is uploaded to the cloud.



Finally, if heuristics aren't decisive, the file is evaluated against more than 6,800 attributes in the Cloud Sandbox. They are then taken into account for the final decision induced through machine learning (ML) of whether you're dealing with malware.

How is the Cloud Sandbox trained and continuously updated?

- A neural network is set up to decide whether a file contains malware or not
- More than 6,800 file attributes serve as input to the neural network
- Through a large data set containing malicious and clean, labelled files, the neural network is trained to distinguish one from another
- Whenever a new, unknown file is uploaded to the Cloud Sandbox, the neural network determines whether the file contains malware, based on the previously seen files
- With every uploaded file, the neural network gets smarter as machine learning (ML) is adjusted to fit the most current status quo of how malicious files look
- Re-learning mechanisms ensure that the neural network is not mistrained

opensystems

Open Systems is a secure access service edge (SASE) pioneer that enables organizations to connect to themselves, to the cloud, and to the rest of the world. With cloud-native architecture, secure intelligent edge, hybrid cloud support, 24x7 operations by level-3 engineers, and predictive analytics, the Open Systems SASE delivers a complete solution to network and security.

Learn more at **open-systems.com** |