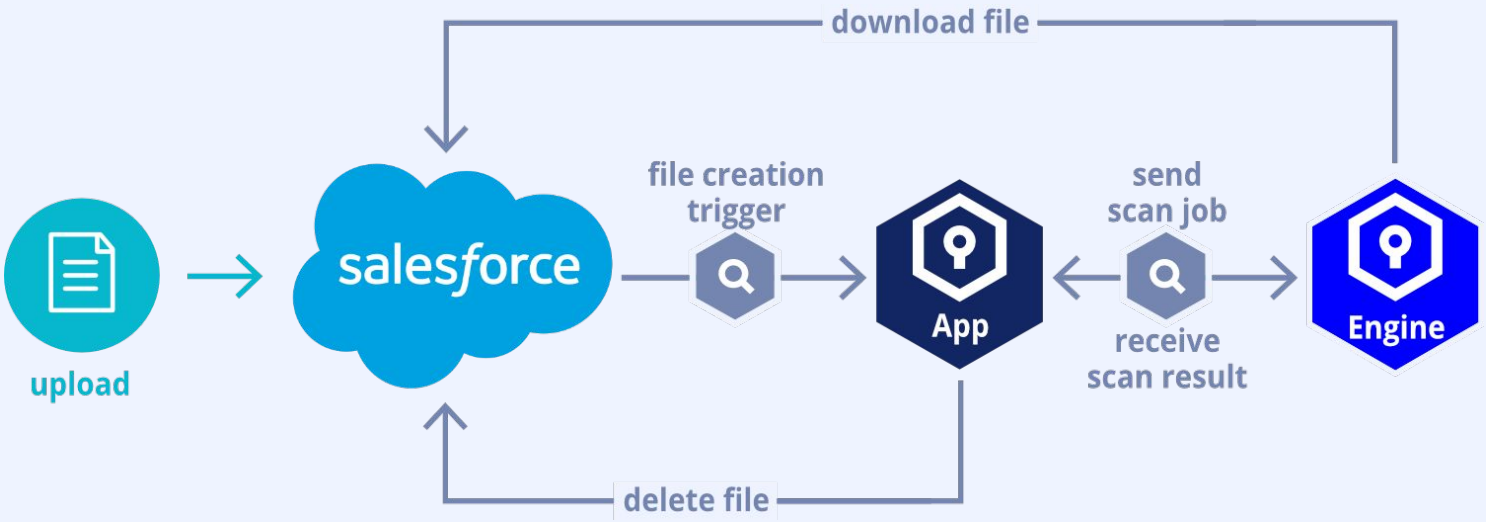
attachmentAV

Malware protection for Salesforce

Factsheet

How it works



This is how attachmentAV works when uploading a file:

1. A file is uploaded to Salesforce.
2. Salesforce triggers the attachmentAV app.
3. The attachmentAV app sends a scan job to the attachmentAV engine in a jurisdiction of your choice.
4. The engine downloads the file over encrypted HTTPS.
5. The engine temporarily stores the file on an encrypted disk.
6. The engine scans the file.
7. The engine deletes the temporary file from the encrypted disk.
8. The engine sends the scan result back to the app.
9. The app stores the scan result, publishes a platform event with the scan result, runs mitigation actions, and notifies the uploader about the scan result.

attachmentAV can also scan existing files.

Key Benefits

Simple

Enable malware protection with a few clicks. Scans newly uploaded files and existing files.

Fast

The Sophos® engine signatures database is updated hourly to protect you against the latest threats.

Up-to-date Malware Database

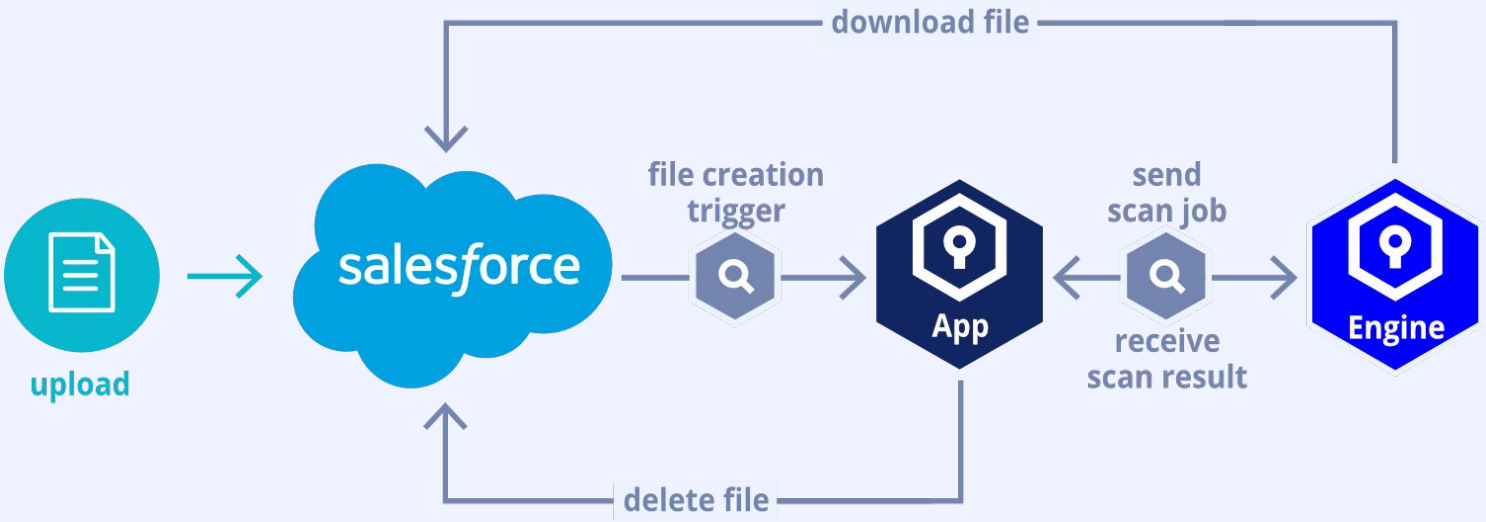
The signatures are updated continuously to protect you against the latest threats.

Automated Mitigation

attachmentAV deletes and notifies about infected files. Configure as needed.

Features

Real-time scan

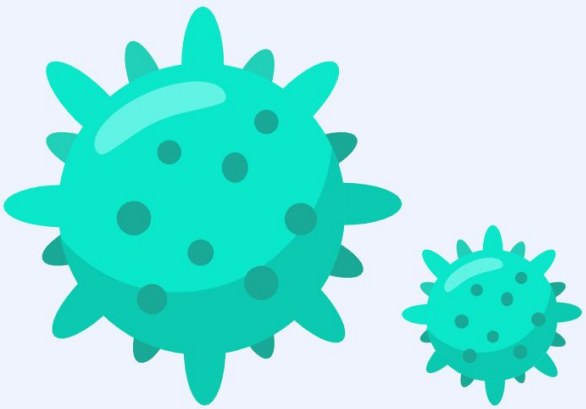


Newly uploaded files are scanned within seconds using Sophos' leading antivirus engine. Immediate zero-day protection with an up-to-date malware signature database ensures your files remain secure from the latest threats.

Full scan

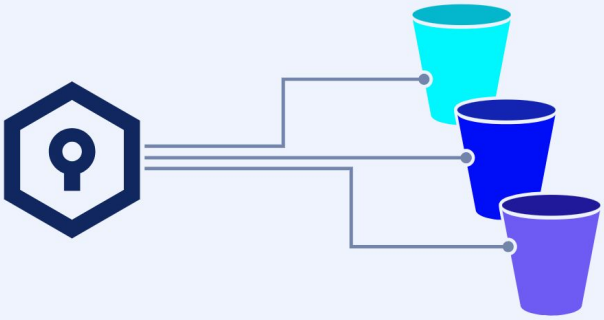
You can scan all existing files after installation. You can also define a schedule to scan all files periodically against the latest malware signature database.

Industry-leading antivirus engine



attachmentAV is powered by the Sophos® engine. Sophos is a trusted cybersecurity provider. The engine comes with immediate zero-day protection.

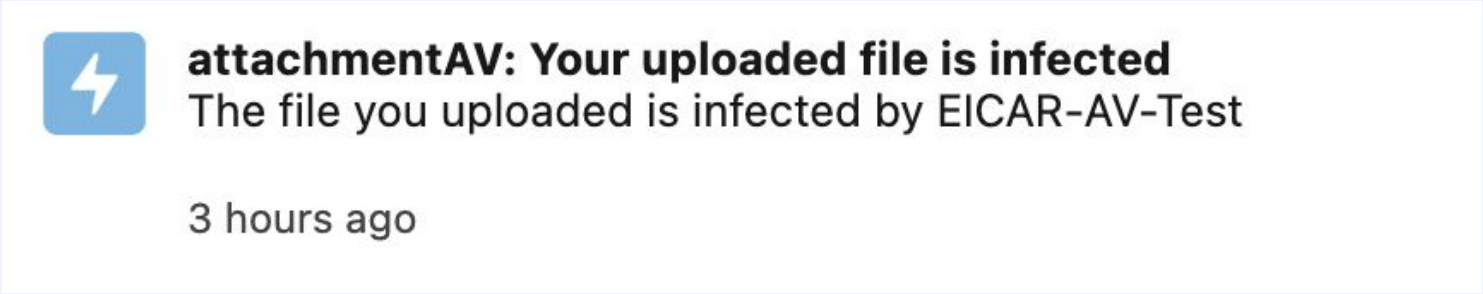
Automated mitigation



attachmentAV deletes infected files by default.

You can also block downloads of not scanned, infected, or unscannable files.

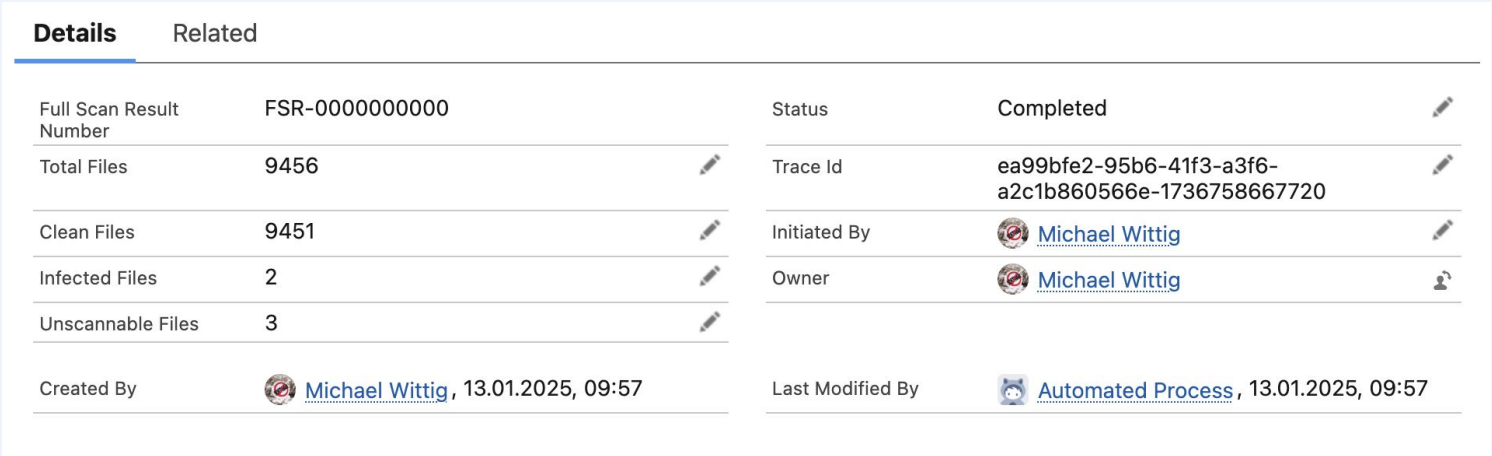
Notifications



You can notify the uploader about scan results. By default, uploaders are notified about infected and unscannable files. For external users, an email is sent.

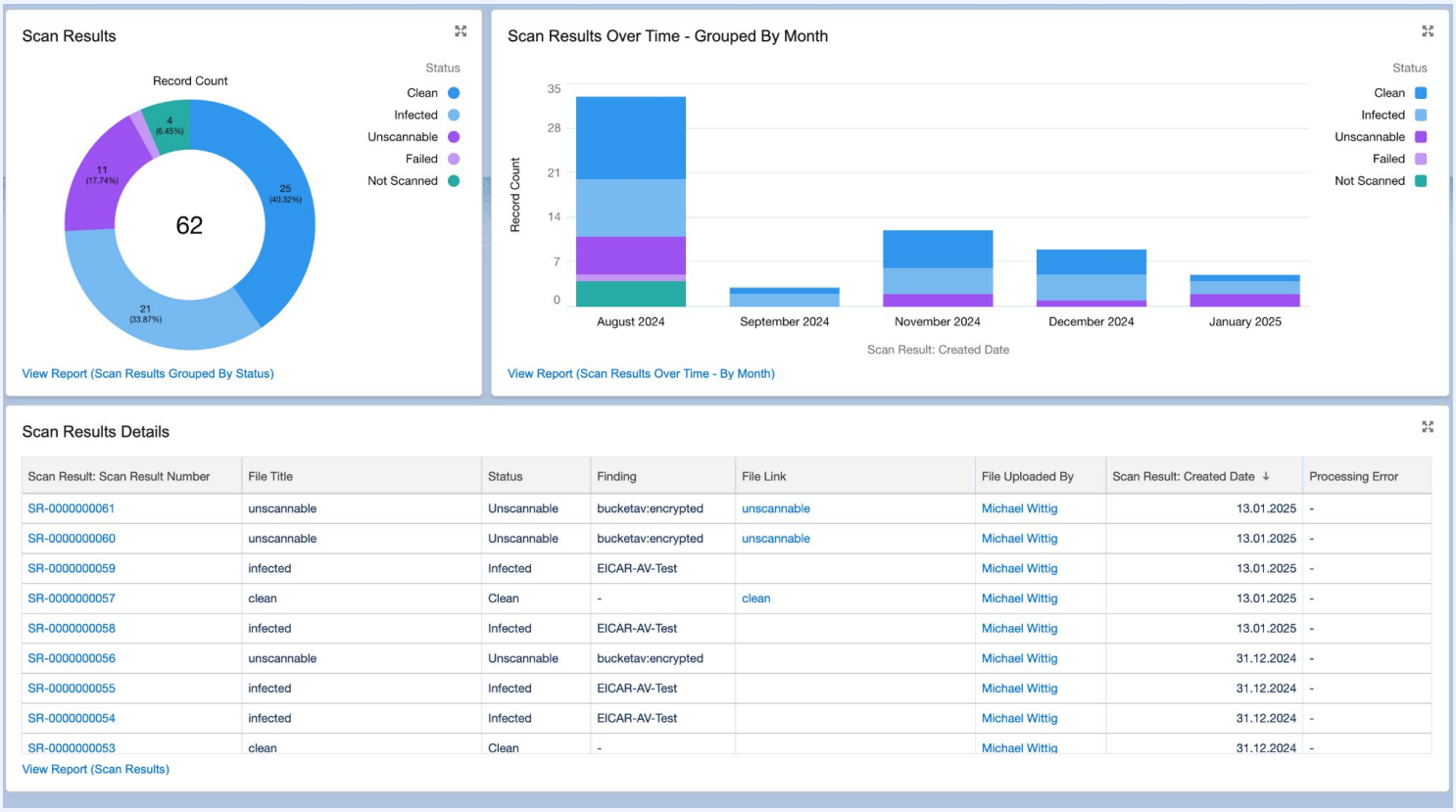
Lastly, all scan results are published as Salesforce platform events.

Reports



Real-time scan and full scan results are stored in Salesforce for reporting purposes.

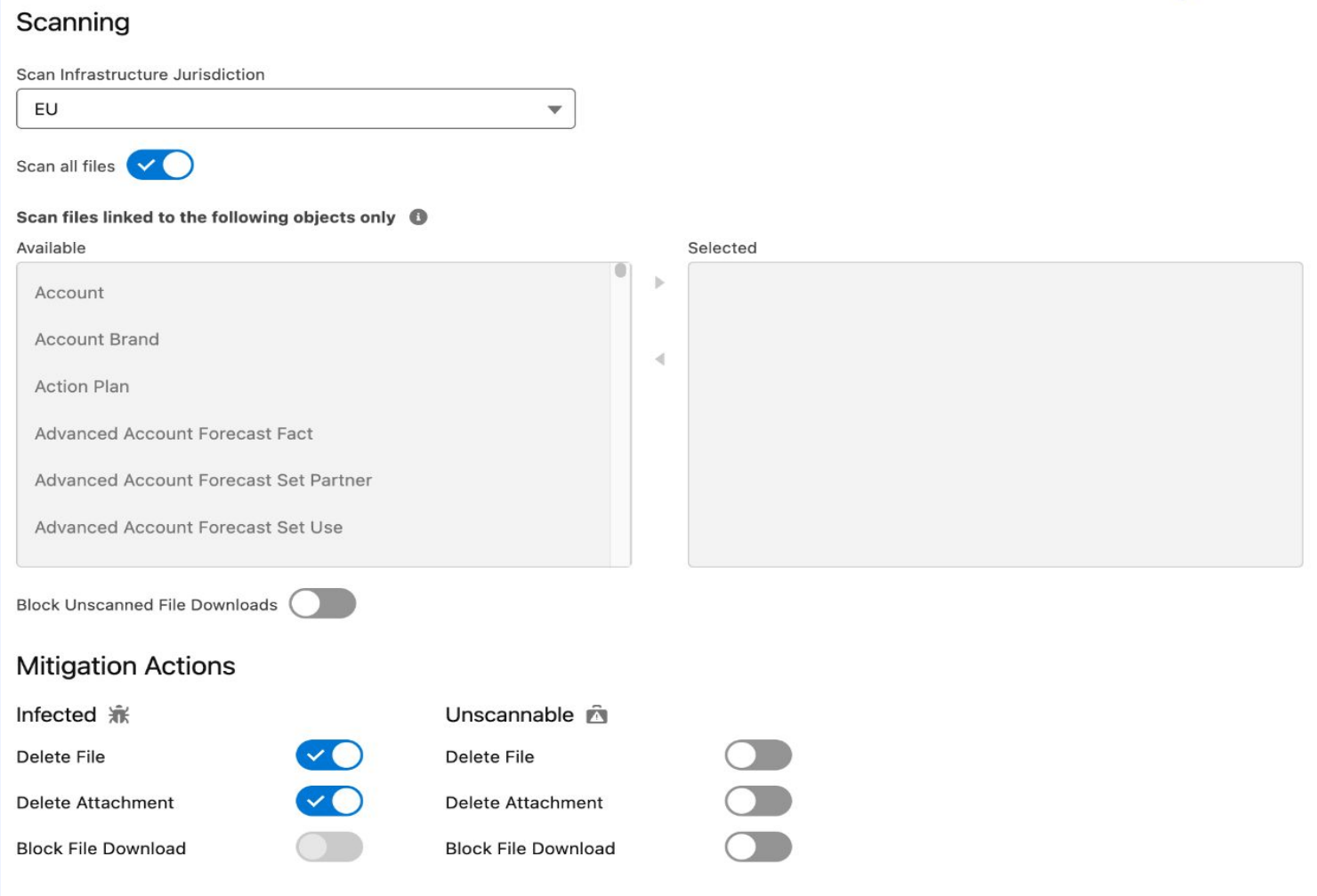
Dashboard



Get an overview of the real-time scan results to identify new threats and unprotected files.

The dashboard is the best place to observe attachmentAV.

Configurable



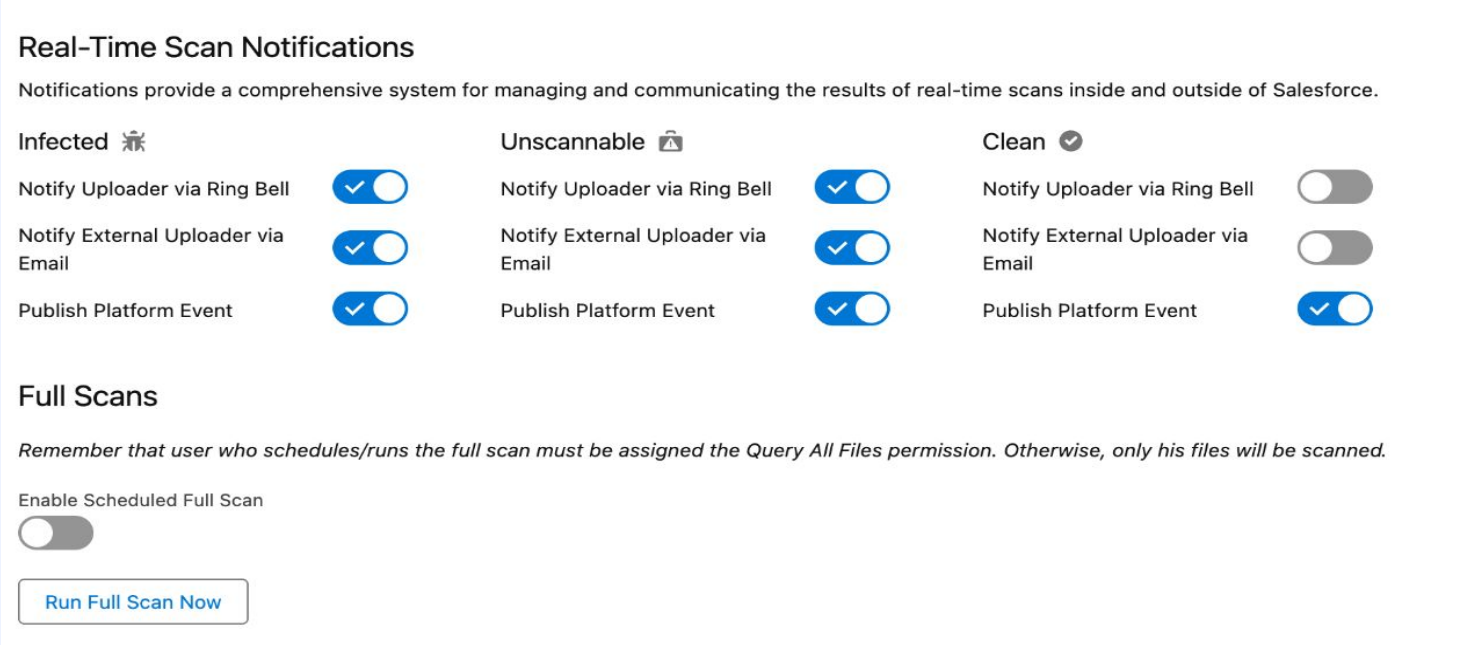
Select the jurisdiction where the scanning takes place to comply with data protection laws.

Filter to scan files related to specific objects only.

Block file downloads for unscanned files.

Define what happens with infected, unscannable, and clean files.

Configurable



Define who is notified with infected, unscannable, and clean files.

Configure the full scan of all files.

Run an on-demand full scan of all files.

attachmentav.com

Malware protection for Salesforce

Need more help? Write us! hello@attachmentav.com