Instantly Scan Attachments for Malware and Store Forensic File Data for Rapid Threat Detection

Analyze All Email Attachments for Malware with ReversingLabs Scale and Speed

Menlo Email Isolation, a component of the Menlo Security Isolation Platform (MSIP), integrates with ReversingLabs TitaniumScale Enterprise Scale Visibility platform to automatically send all attachments for analysis to develop local threat intelligence for combating undetected malware.

Email attachments submitted by Menlo Email Isolation are processed to extract rich metadata and threat indicators from the files and their internal objects. The result is detailed local intelligence data on each extracted object that is automatically stored into a data lake and a file lake to make it available to SIEM, orchestration and analytics platforms for further action.

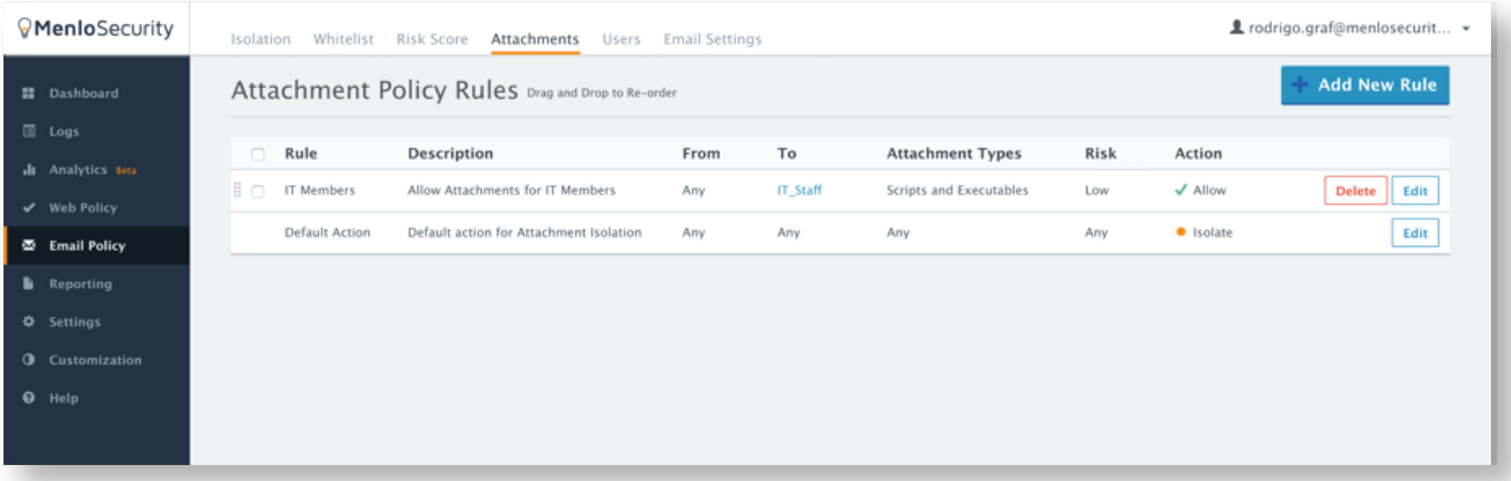
Analysis results can also automatically be sent back to Menlo Email Isolation in real-time to provide real-time file information to determine whether to block, isolate or forward decisions for attachments. The attachment analysis results are returned in less than a second to provide the most accurate and up to date information available for policy enforcement to minimize business disruptions.

The TitaniumScale and Menlo Email Isolation solution analyzes millions of objects per day in near real-time and the detailed file analysis results are stored to create a local threat intelligence data lake that enables advanced analytics, threat correlation, hunting, and response teams to search for and combat undetected malware. It also leverages RL's industry-leading file intelligence database of known goodware and malware for identification and context.

The joint solution gives instant visibility into threats coming from email that security operations teams can't see today and automates steps for quick, accurate decisions to block or isolate - saving crucial time to contain malware.

Solution Highlights

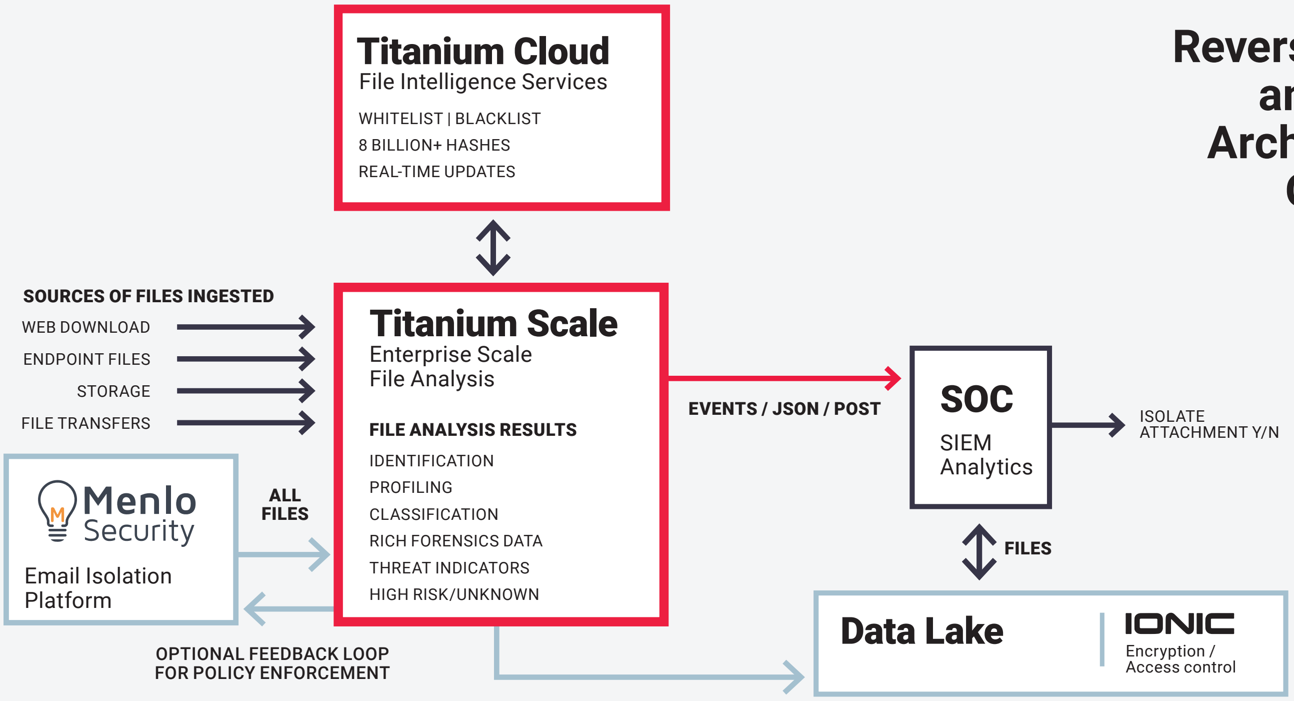
- **Menlo Email Isolation automatically submits all attachments to TitaniumScale for analysis.**
- **TitaniumScale comprehensive analysis results are stored in a data lake to support hunting, identification and response for undetected malware.**
- **TitaniumScale sends events to a SIEM based on a powerful classification engine and customer defined YARA rules.**
- **Analysis results can also be returned in real-time to the Menlo Email Isolation platform to inform block, isolate and forward decisions.**



Attachment Policy Rules Drag and Drop to Re-order

Rule	Description	From	To	Attachment Types	Risk	Action
IT Members	Allow Attachments for IT Members	Any	IT_Staff	Scripts and Executables	Low	✓ Allow
Default Action	Default action for Attachment Isolation	Any	Any	Any	Any	● Isolate

ReversingLabs and Menlo Architectural Overview



Titanium Cloud
File Intelligence Services
WHITELIST | BLACKLIST
8 BILLION+ HASHES
REAL-TIME UPDATES

SOURCES OF FILES INGESTED
WEB DOWNLOAD
ENDPOINT FILES
STORAGE
FILE TRANSFERS

Titanium Scale
Enterprise Scale
File Analysis

FILE ANALYSIS RESULTS
IDENTIFICATION
PROFILING
CLASSIFICATION
RICH FORENSICS DATA
THREAT INDICATORS
HIGH RISK/UNKNOWN

Menlo Security
Email Isolation Platform

ALL FILES

OPTIONAL FEEDBACK LOOP FOR POLICY ENFORCEMENT

EVENTS / JSON / POST

SOC
SIEM
Analytics

ISOLATE ATTACHMENT Y/N

FILES

Data Lake

IONIC
Encryption / Access control

How It Works

- Menlo Email Isolation sends email attachments to ReversingLabs TitaniumScale as one of many sources of files for classification and analysis. The files are unpacked, processed by a powerful static analysis engine, enriched with data from the ReversingLabs File Intelligence Service and then classified. The results are stored in a data lake to support undetected malware identification, hunting and response. TitaniumScale's robust classification engine also includes customer defined YARA rules for identifying new attacks or files of interest. TitaniumScale sends detailed events to a SIEM (e.g. Splunk) when detections occur or YARA rules indicate a match and/or alert.
- The joint solution can also be configured to return TitaniumScale's file analysis results back to Menlo Email Isolation for computing a Document Risk Score. Menlo Security applies Document Risk Scores for enforcing policies to block known bad, isolate suspicious or forward safe attachments and enforce other policy-based access to original files.

SOLUTION PRODUCTS

ReversingLabs TitaniumScale enables an organization to profile and classify large volumes of objects in near real-time to create relevant data for use by advanced analytic platforms for threat correlations, hunting, and response efforts. TitaniumScale helps enterprises perform a comprehensive assessment of millions of files from web traffic, email, file transfers, endpoints, and storage. It acquires objects by integrating with existing security infrastructure, including email gateways, intrusion detections systems, firewalls, and other devices. The results feed into SIEM, orchestration and analytics platforms. The metadata created about each object is stored in a data lake, and many deployments can include a dedicated file lake to store all files classified as high risk or unknown.

Menlo Security's Safe Mail Isolation approach enables safe, responsible use of personal webmail by selectively isolating all personal webmail traffic, including any link that may have been clicked from a personal email account, rendering all malware ineffective. Traditionally a weak link in your security strategy, personal webmail can now be accessed by users at will, and your organization will still be protected.