ReversingLabs Cloud Deep Scan

Fast, Quality File Classification for Cloud File Shares

Key Solution Highlights

LARGE FILE PROCESSING

By leveraging Reversing Labs unique technology, ReversingLabs Cloud Deep Scan can unpack and analyze a broad range of file types up to 10GB. Get fast results as you continuously monitor your Amazon S3 buckets for malware or submit files for classification scanning via the ReversingLabs Cloud Deep Scan portal, API or CLI tool.

EASY MALWARE IDENTIFICATION

Prioritize files to investigate through fast, easy-to-understand malware identification (goodware/malware) or use Expert Classification for more detail. Actionable intelligence includes file type, malware family. ReversingLabs File Decomposition technology analyzes your files and provides dashboard highlights on any malicious or suspicious files.

INDUSTRY-BEST DETECTION

Classification is based on Reversinglabs unique static analysis technology combined with ReversingLabs world-class goodware and malware repository, which provides better detection for malicious documents, archives, and media than any other method.

PRIVACY

Original files are scanned and remain in the customer's AWS S3 environment. ReversingLabs does not retain the customer's files.

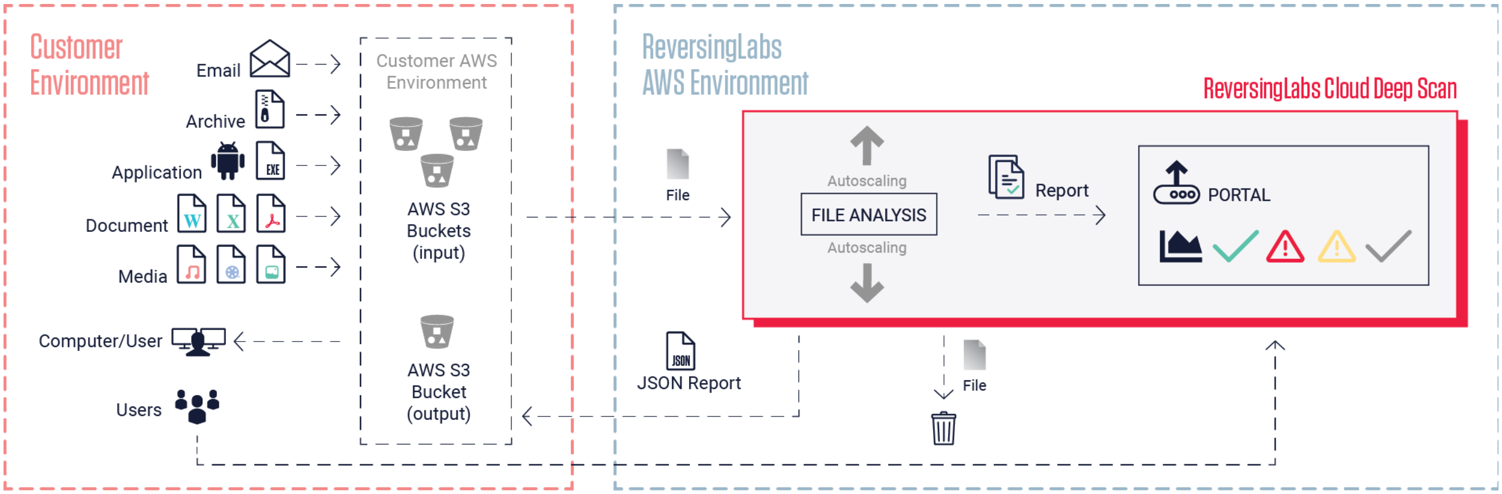
Overview

ReversingLabs Cloud Deep Scan file analysis is a security solution hosted in the cloud that scans large files and cloud storage to detect malicious and suspicious threats, limiting the risk and impact of incidents and breaches.

Files can be submitted for analysis and classification in three ways: continuously monitoring designated Amazon Web Services (AWS) S3 (Simple Storage Service) buckets, manual upload via the ReversingLabs Cloud Deep Scan Portal, or by using a CLI tool. Users view results by logging into an intuitive graphical dashboard via a web browser, or through a standards-based report written to the designated S3 location. ReversingLabs Cloud Deep Scan has a friendly interface and is created for a broad range of personas in IT and security.

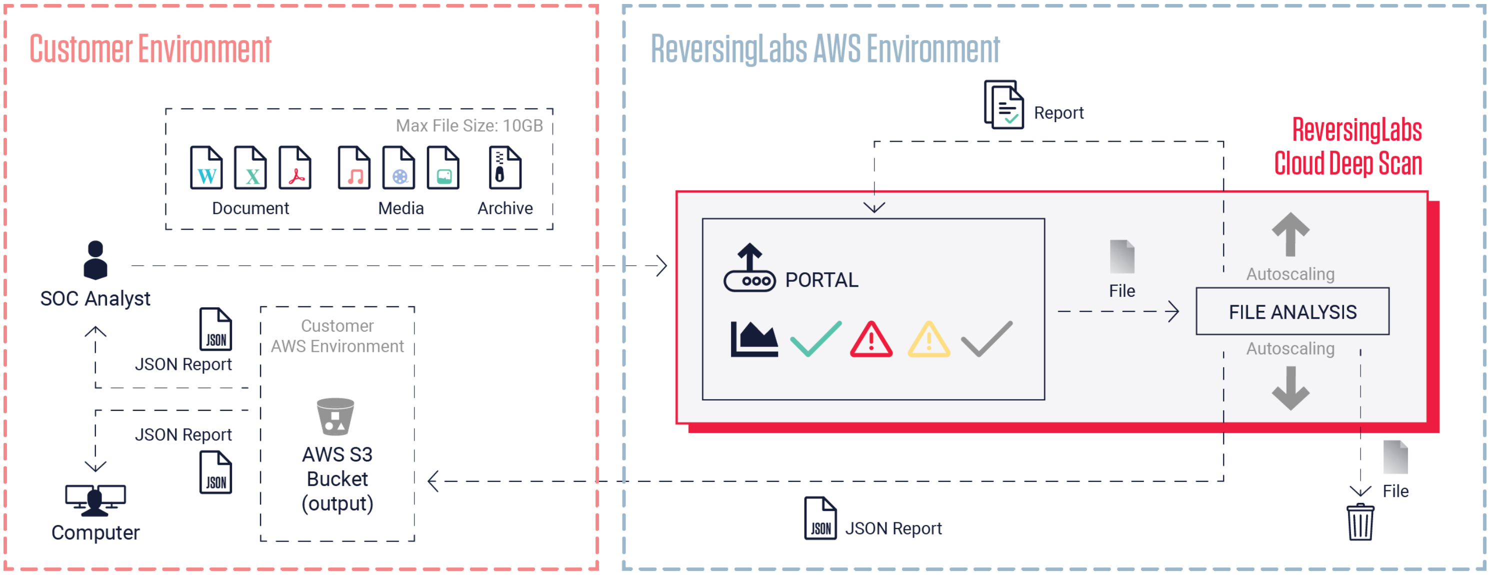
ReversingLabs Cloud Deep Scan is based on the Titanium Platform which uses unique ReversingLabs File Decomposition technology to extract detailed metadata, add global reputation context and classify threats. Users can take additional actions using the specific S3 path and filename, or the associated file hash. ReversingLabs Cloud Deep Scan is a quick and easy way to detect malware and suspicious files up to 10GB in size.

Use Case 1 | Continuously monitor the designated Customer Amazon S3 and analyze files automatically.



Picture 1. Automatic analysis of files within AWS S3 bucket

Use Case 2 | Upload large files to analyze, up to 10GB, via the ReversingLabs Cloud Deep Scan Portal.



Picture 2. Upload a file via the ReversingLabs Cloud Deep Scan Portal for analysis

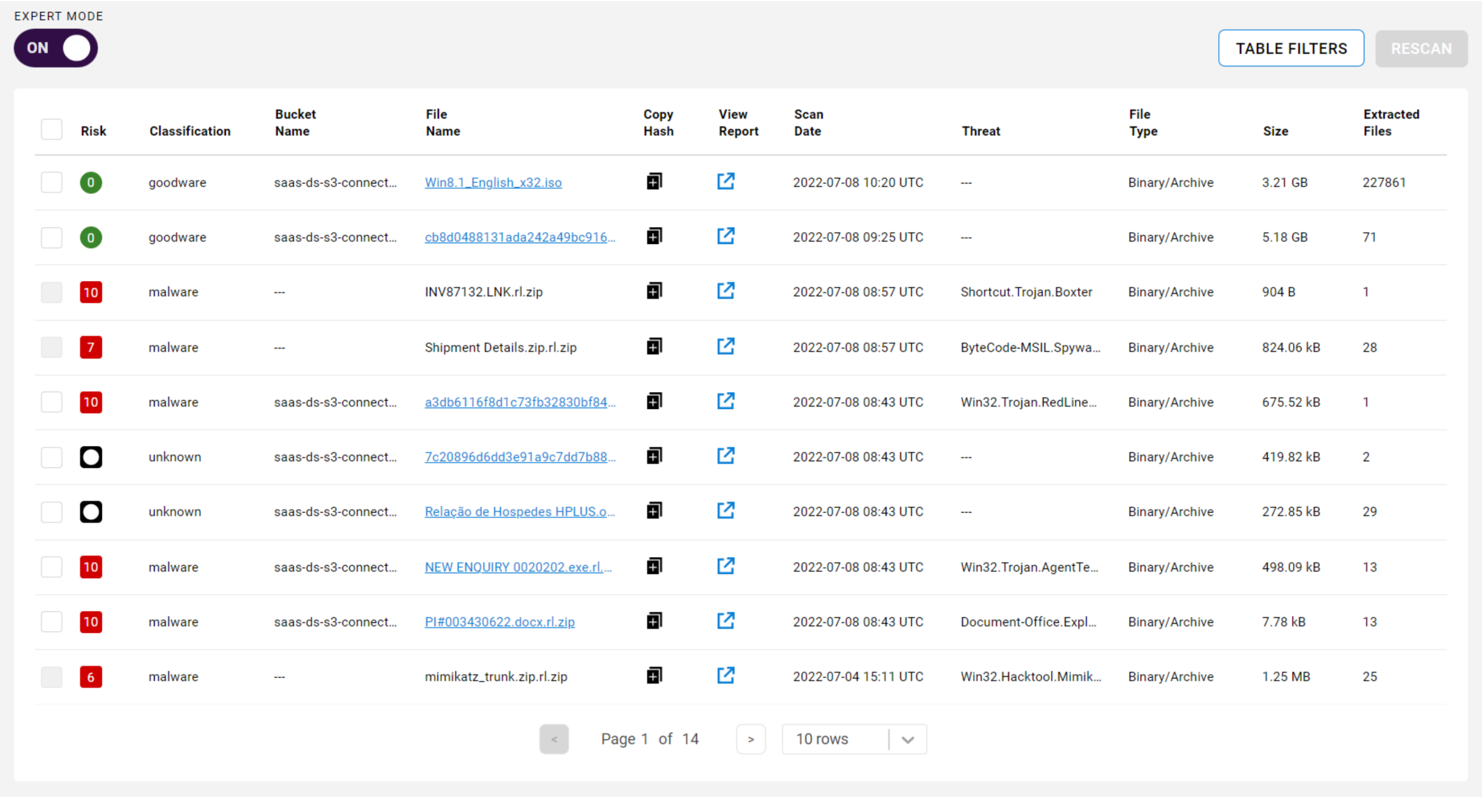
Key Features

FILE SOURCES AND FILE SUBMISSION	• Continuously monitor the designated Amazon S3 buckets and analyze files automatically • Manually upload files through the intuitive ReversingLabs Cloud Deep Scan Portal user interface which pushes it to the scanning service • Submit files using a CLI command that pushes files to the service
LARGE FILE PROCESSING	• Capability to unpack and analyze a wide variety of file types up to 10GB in size • The product extracts all files at all levels from a single top-level object
REPORTING	• A full JSON report is saved to the customer's designated AWS S3 bucket • A reduced summary report of all analyzed files can be found on the ReversingLabs Cloud Deep Scan Portal dashboard in CSV format
CLASSIFICATION	• The product performs high-speed, static analysis to unpack files, extract internal indicators and assign a threat level • Files are classified as goodware, malware, or suspicious, with a risk score that indicates the threat level, or they are unknown

MULTI- USER ENVIRONMENT	• User types in ReversingLabs Cloud Deep Scan Portal: Admin and Regular User • "Admin" manages users and groups that allow a logical separation between buckets and the "Regular Users" who need to have access to the results
PRIVACY	• Each customer has a designated web link to the service • Each user has login credentials with two-factor authentication SOC2 certification • For scanning purposes (file unpacking and classification), files are copied to ReversingLabs Cloud Deep Scan ◦ Original files will stay in the customer's bucket (if files are scanned from AWS S3 buckets) ◦ When the scan is finished, all submitted and extracted files will be deleted from the ReversingLabs Cloud Deep Scan service, i.e. Reversinglabs doesn't retain customer files ◦ Generated JSON report is saved to the customer's bucket

Intuitive Dashboard

ANALYTICS	• Table with total number of detected malware files per bucket, malware types and malware families • Trends chart: top 5 input buckets/malware types/malware families by detected malware • Stacked chart: top 10 input buckets/malware types/malware families by risk score
FILE DETAILS	File Details contains detection results for each submitted file (also available in a generated JSON report)

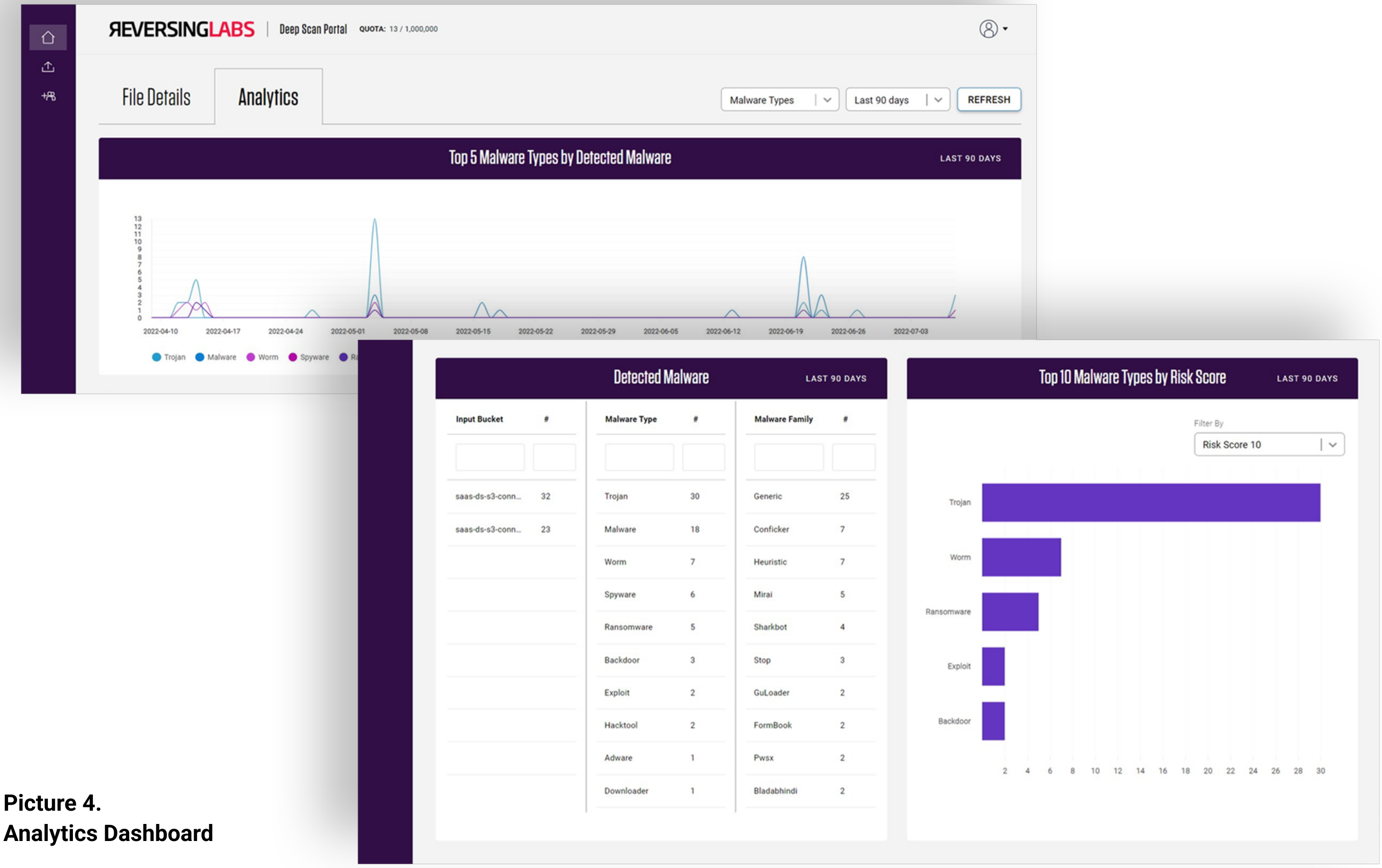


□	Risk	Classification	Bucket Name	File Name	Copy Hash	View Report	Scan Date	Threat	File Type	Size	Extracted Files
□	0	goodware	saas-ds-s3-connect...	Win8.1_English_x32.iso	⧉	↗	2022-07-08 10:20 UTC	---	Binary/Archive	3.21 GB	227861
□	0	goodware	saas-ds-s3-connect...	cb8d0488131ada242a49bc916...	⧉	↗	2022-07-08 09:25 UTC	---	Binary/Archive	5.18 GB	71
□	10	malware	---	INV87132.LNK.rl.zip	⧉	↗	2022-07-08 08:57 UTC	Shortcut.Trojan.Boxter	Binary/Archive	904 B	1
□	7	malware	---	Shipment Details.zip.rl.zip	⧉	↗	2022-07-08 08:57 UTC	ByteCode-MSIL.Spywa...	Binary/Archive	824.06 kB	28
□	10	malware	saas-ds-s3-connect...	a3db6116f8d1c73fb32830bf84...	⧉	↗	2022-07-08 08:43 UTC	Win32.Trojan.RedLine...	Binary/Archive	675.52 kB	1
□	○	unknown	saas-ds-s3-connect...	7c20896d6dd3e91a9c7dd7b88...	⧉	↗	2022-07-08 08:43 UTC	---	Binary/Archive	419.82 kB	2
□	○	unknown	saas-ds-s3-connect...	Relação de Hospedes HPLUS.o...	⧉	↗	2022-07-08 08:43 UTC	---	Binary/Archive	272.85 kB	29
□	10	malware	saas-ds-s3-connect...	NEW ENQUIRY 0020202.exe.rl....	⧉	↗	2022-07-08 08:43 UTC	Win32.Trojan.AgentTe...	Binary/Archive	498.09 kB	13
□	10	malware	saas-ds-s3-connect...	PI#003430622.docx.rl.zip	⧉	↗	2022-07-08 08:43 UTC	Document-Office.Expl...	Binary/Archive	7.78 kB	13
□	6	malware	---	mimikatz_trunk.zip.rl.zip	⧉	↗	2022-07-04 15:11 UTC	Win32.Hacktool.Mimik...	Binary/Archive	1.25 MB	25

Picture 3. File Details

Column	Value
Risk	Risk score is present inside icons. It rates the severity of a threat on a scale of 0 to 10, where 0 means not a threat, and 10 indicates a severe threat. ● Goodware 🟥 Malware ◆ Suspicious ○ Unknown
Classification	• Malicious, suspicious, goodware or unknown
Bucket Name	• Input bucket in which analyzes file is located
File Name	• Name of analyzed file
Copy Hash	• On hover over the icon, the user can see a tooltip with the file hash • On click, the hash will be copied to the clipboard.
View Report	• Click on the link icon opens the JSON report location in a designated output S3 bucket
Scan Date	• Date when file was scanned by SaaS Deep Scan File Analysis • It is unpresent for files that exceed size limit
Threat	• Naming convention: affected system.malware type.malware family • Example: win32.Trojan.Kryptik
File Type	• Scanned file type
Size	• Scanned file size
Extracted Files	• Total number of extracted files that were untapped from the submitted file and analyzed

File Details table - columns explanation



Input Bucket	#	Malware Type	#	Malware Family	#
saas-ds-s3-conn...	32	Trojan	30	Generic	25
saas-ds-s3-conn...	23	Malware	18	Conficker	7
		Worm	7	Heuristic	7
		Spyware	6	Mirai	5
		Ransomware	5	Sharkbot	4
		Backdoor	3	Stop	3
		Exploit	2	GuLoader	2
		Hacktool	2	FormBook	2
		Adware	1	Pwsx	2
		Downloader	1	Bladabhindi	2

Picture 4.
Analytics Dashboard

ReversingLabs Cloud Deep Scan Benefits

QUALITY CLASSIFICATION FINDS MALWARE CLOUD AV MISSES	• Unmatched level of detection for advanced threats that signature-based AV and EDR miss • Prioritize events and take quick action with easy-to-understand analysis to keep business processes running • Receive email notifications 24x7 when a breach impacts file-based business processes
IT AND BUSINESS READY EXPERIENCE	• No malware analysis or hunting expertise required to protect business processes from file-based threats • Cloud file share continuous scanning and Web and CLI upload makes it easy to check for hidden malware • Enable file-based business workflows when collecting and sharing files between business partners and internal teams
CLOUD NATIVE INTEGRATION	• Integration with S3 buckets enables quick scanning of file shares, backup, and storage • Native cloud processing of files avoids costly on-premises software and hardware spend • Maintains privacy of files and data which remain in cloud storage

Get Started!

www.reversinglabs.com

REQUEST A DEMO

ЯEVERSINGLABS

Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com