

Trend Vision One™ Sandbox Analysis

Ensure unknown and advanced malware has nowhere to hide

Advanced threats and targeted attacks are designed to bypass conventional cybersecurity defenses, often remaining undetected while stealing sensitive data or encrypting it for ransom. When a cyberattack occurs, it's crucial to quickly understand the malware's intent and operation to contain damage and prevent future incidents. However, current malware analysis is often slow and incomplete, allowing increasingly sophisticated adversaries to exploit blind spots and evade detection. To help address these threats, implement advanced detection technology as part of your broader security strategy.

Determine your cyber risk with Sandbox Analysis

Sandbox Analysis detonates objects—such as files and URLs—in a secure virtual environment to detect unknown threats. It manages and analyzes objects submitted by integrated solutions and users. It also enables automatic sharing of indicators of compromise (IoCs) across the Trend Vision One™ platform and helps automatically safeguard your environment from suspicious or unknown objects.

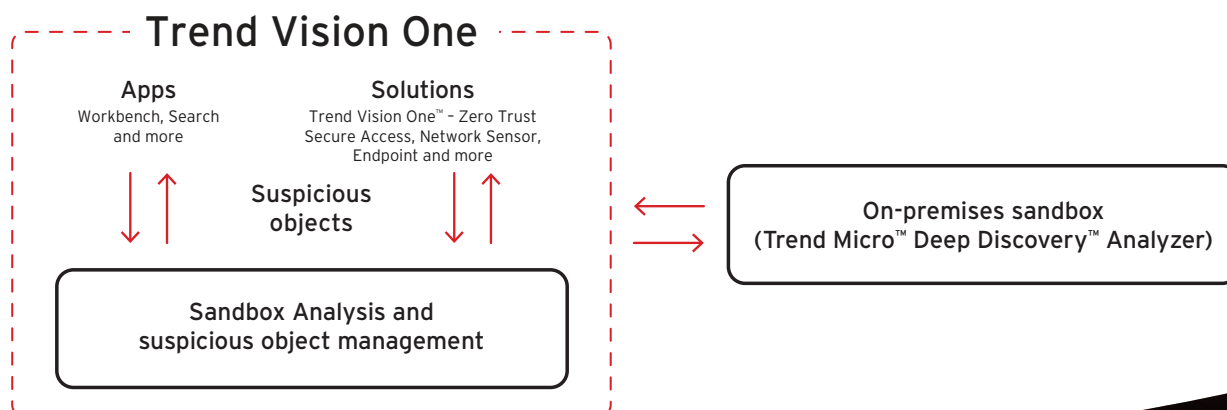
Sandbox Analysis samples can be submitted either manually or automatically without user intervention. High-risk samples are blocked automatically across all solutions right away. Collectively, this provides detailed threat context, helping inform how best to respond to—and manage—cyber risk.

Sandbox Analysis can also enhance XDR detection, enabling a more efficient response. Advanced, automatic malware analysis enhances threat detection for all layers of XDR as part of the seamless XDR workflow in Trend Vision One—empowering your security operations center (SOC), incident response, and forensics teams to analyze and mitigate threats more effectively. The result is a stronger set of incident response, investigation, and threat-hunting capabilities.

Key benefits

- Automatically protect your environment from suspicious and unknown/zero-day objects
- Strengthen XDR detection by analyzing and blocking advanced malware early in the process
- Accelerate XDR incident response and threat hunting
- Identify and analyze new threats, strengthening your cyber risk exposure management (CREM)
- Submit, share, and block high-risk samples across unified
- AI-powered Trend Micro solutions and third-party software

Figure 1: Sandbox Analysis integration with Trend Vision One



Key capabilities

- Executes unknown samples in an isolated, safe environment and supports multiple operating systems and software applications to simulate malicious attacks
- Harnesses advanced detection methods such as static analysis, heuristic analysis, behavior analysis, web reputation, and file reputation
- Detects multi-stage malicious files, outbound connections, and repeated command and control (C&C) attempts from suspicious files
 - Broad file analysis examines a wide range of Microsoft Windows executables, Microsoft 365, PDFs, web content, and compressed file types using multiple detection engines and sandboxing
 - Document exploit detection discovers malware and exploits delivered in common document formats via specialized detection and sandboxing
 - URL analysis performs sandbox analysis of URLs, including those contained in emails or manually submitted samples
- Shares new IoC detection intelligence automatically with XDR, Trend Vision One™
- Cyber Risk Exposure Management (CREM), and on-premises and third-party solutions
- Supports Windows, Mac, and Linux operating systems
- Detects ransomware including script emulation, zero-day exploits, and targeted and password-protected malware commonly associated with ransomware
- Integrates with Trend Companion™, our generative artificial intelligence (GenAI) cybersecurity technology—supporting analysts as they make quick and informed decisions based on sandbox reports

Boost your XDR and CREM capabilities

Strengthen your XDR detection:

Sandbox Analysis enhances threat detection for all layers of XDR by analyzing and blocking advanced malware early in the process. It removes the burden of manual analysis and enables a deeper understanding of the malware in question. Sandbox Analysis can be set up in your Trend Vision One playbook as a rule to automatically collect and analyze suspicious objects in large volumes.

Accelerate your XDR response:

Sandbox Analysis is part of the seamless XDR workflow within Trend Vision One, allowing SOC, threat hunting, incident response, and forensics teams to perform proactive threat hunting, investigation, and threat mitigation more effectively. It helps you analyze any suspicious objects found in your environment, providing further context to inform your response actions.

Bolster your CREM efficacy:

Sandbox Analysis helps reduce your attack surface by identifying and analyzing new threats. Contextual threat information helps determine if assets are vulnerable to specific threat types and identifies malicious behaviors. Detailed threat context from sandbox reports allows analysts to understand potential scopes of impact to support risk prioritization and management for efficient resource allocation.



Built-in sandbox convictions of unknown or untrusted files and ingested telemetry from other product lines provide a rich correlation data set, allowing for rapid, high-fidelity convictions at the analyst's fingertips.

The Forrester Wave™:
Network Analysis and Visibility,
Q2 2023

Our sandboxing solution expertise

- Leader in the Forrester Wave: Network Analysis and Visibility (Q2 2023)
- More than 10 years of malware analysis sandbox technology—one of the first in the industry
- Complete visibility of Sandbox Analysis results across all connected solutions as part of the Trend Vision One platform, and across cloud-based and on-premises sandboxes as a hybrid solution

Your local threat intelligence center

Sandbox Analysis samples can be submitted across Trend Vision One solutions with sharing and blocking of high-risk objects. All samples submitted across the platform are consolidated in one view for IT and SOC efficiency, including submissions from all Trend Vision One features (such as Response Management and Workbench), all integrated solutions, and on-premises products including Deep Discovery Analyzer.

Sandbox Analysis Report

Consult the Sandbox Analysis Report to determine if a sample poses a risk to your operations. This report contains threat details such as risk level, object file type, size, and correspondence with any MITRE ATT&CK™ Framework Tactics and Techniques, and notable characteristics such as data theft or malware. This information helps you understand sample behavior while also bolstering incident response and threat hunting measures.

Submission types

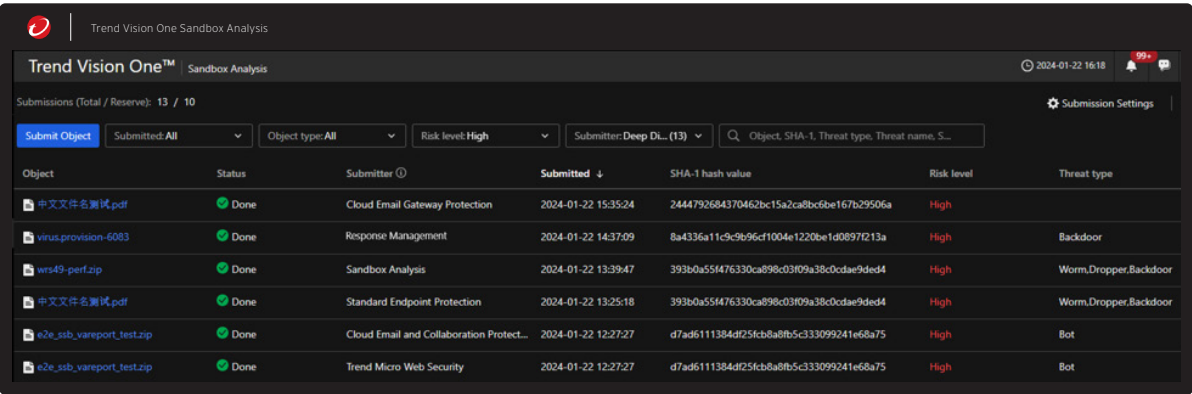
Manual submission

- Manual object submissions are made within Sandbox Analysis

Automatic submission

- These are managed in solutions such as Trend Vision One™ Zero Trust Secure Access (ZTSA)
- Trend Vision One™ XDR for Networks, and Trend Vision One™ Endpoint Security

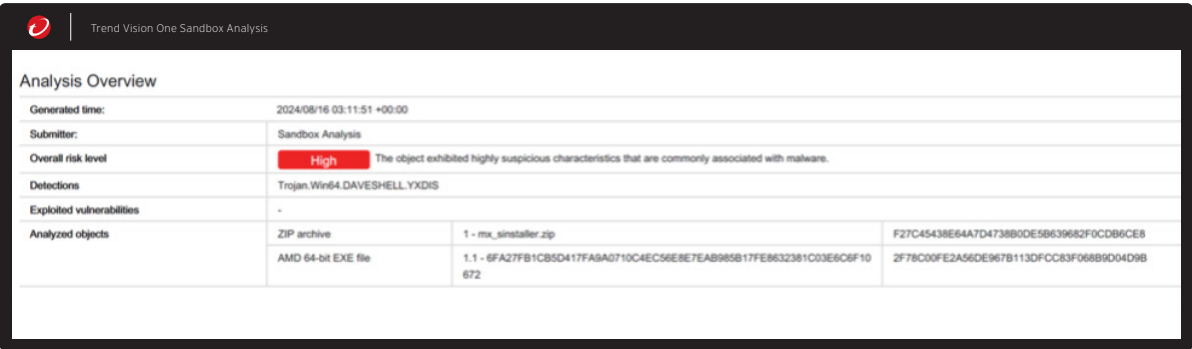
Figure 2: Sandbox Analysis view within Trend Vision One



The screenshot shows the 'Trend Vision One™ Sandbox Analysis' interface. At the top, there's a header with the Trend Vision One logo and the text 'Trend Vision One™ Sandbox Analysis'. Below the header, there's a navigation bar with 'Submissions (Total / Reserve): 13 / 10' and a 'Submission Settings' button. The main area contains a table with columns: Object, Status, Submitter, Submitted, SHA-1 hash value, Risk level, and Threat type. The table lists several submissions, including PDF files, ZIP files, and executables, with their respective status (Done), submitters (Cloud Email Gateway Protection, Response Management, Sandbox Analysis, Standard Endpoint Protection, Cloud Email and Collaboration Protect..., Trend Micro Web Security), submission times, SHA-1 hash values, risk levels (all High), and threat types (Backdoor, Worm, Dropper, Bot).

Object	Status	Submitter	Submitted	SHA-1 hash value	Risk level	Threat type
中文文件名测试.pdf	Done	Cloud Email Gateway Protection	2024-01-22 15:35:24	2444792684370462bc15a2ca8bc0be167b29506a	High	
virus.provision-6083	Done	Response Management	2024-01-22 14:37:09	8a4336a11c9c9696cf1004e1220be1d0897f213a	High	Backdoor
wcs49-perf.zip	Done	Sandbox Analysis	2024-01-22 13:39:47	393b0a55f476330ca898c03f09a38c0dae9ded4	High	Worm,Dropper,Backdoor
中文文件名测试.pdf	Done	Standard Endpoint Protection	2024-01-22 13:25:18	393b0a55f476330ca898c03f09a38c0dae9ded4	High	Worm,Dropper,Backdoor
e2e_ssb_vareport_test.zip	Done	Cloud Email and Collaboration Protect...	2024-01-22 12:27:27	d7ad611384d25fcb8a8fb5c333099241e68a75	High	Bot
e2e_ssb_vareport_test.zip	Done	Trend Micro Web Security	2024-01-22 12:27:27	d7ad611384d25fcb8a8fb5c333099241e68a75	High	Bot

Figure 3: Sandbox Analysis Report overview



The screenshot shows the 'Analysis Overview' section of the Trend Vision One Sandbox Analysis interface. It displays a table with analysis details. The 'Generated time' is 2024/08/16 03:11:51 +00:00. The 'Submitter' is Sandbox Analysis. The 'Overall risk level' is High, with a note: 'The object exhibited highly suspicious characteristics that are commonly associated with malware.' The 'Detections' are Trojan.Win64.DAVESHELL.YXDIS. The 'Exploited vulnerabilities' are none. The 'Analyzed objects' are listed in a table with columns for file type, name, and SHA-1 hash value.

Generated time:	2024/08/16 03:11:51 +00:00		
Submitter:	Sandbox Analysis		
Overall risk level	High The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	Trojan.Win64.DAVESHELL.YXDIS		
Exploited vulnerabilities	-		
Analyzed objects	ZIP archive	1 - mx_installer.zip	F27C45438E64A7D4738B0DE5B639682F0CDB6CE8
	AMD 64-bit EXE file	1.1 - 6FA27FB1CB5D417FAB9A710C4EC56E8E7EAB985B17FE8632381C03E6C6F10672	2F78C00FE2A56DE967B113DFCC83F068B9D04D9B


Figure 4: Object overview example

Object 1.1 - 6FA27FB1CB5D417FA9A0710C4EC56E8E7EAB985B17FE8632381C03E6C6F10672 (AMD 64-bit EXE file)			
File name	6FA27FB1CB5D417FA9A0710C4EC56E8E7EAB985B17FE8632381C03E6C6F10672	Risk Level	High
File type	AMD 64-bit EXE file	Detection	Trojan.Win64.DAVESHELL.YXDIS
SHA-1	2F78C00FE2A56DE967B113DFCC83F068B9D04D9B	Exploited vulnerabilities	-
SHA-256	6FA27FB1CB5D417FA9A0710C4EC56E8E7EAB985B17FE8632381C03E6C6F10672	Threat Characteristics	Anti-security, self-preservation (28)
MD5	55243ADAF8E211F336580EBF83268E03		File drop, download, sharing, or replication (3)
TLSH	T141557B0ABAA808F9E47791398853590AE7F2BC560760DBDF13A0136E5F777E05A3E710		Hijack, redirection, or data theft (5)
Size	1366016 byte(s)	Malformed, defective, or with known malware traits (3)	
Command Line	-	Process, service, or memory object change (8)	
		Tactics, Techniques, and Procedures (10)	

Figure 5: Notable threat characteristics and significance level overview

Hijack, redirection, or data theft (5)		
Characteristic	Significance	Details
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2568 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 1728 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2568 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 1728 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2344 Info: Obtains system version from API result
Malformed, defective, or with known malware traits (3)		
Characteristic	Significance	Details
Causes process to crash	■ ■ ■	Process ID: 2344 Image Path: msedge.exe
Detected as known malware	■ ■ ■	Source: ATSE Detection Name: Trojan.Win64.DAVESHELL.YXDIS Engine Version: 24.320.2001 Malware Pattern Version: 19.529.92
Rare executable file	■ ■ ■	Global Detections: 0
Process, service, or memory object change (8)		
Characteristic	Significance	Details
Resides in memory to evade detection	■ ■ ■	Injecting Process ID: 908 Target Process ID: 2568 Target Image Path: explorer.exe Injected Content: Injected API: CreateRemoteThread
Resides in memory to evade detection	■ ■ ■	Injecting Process ID: 1728 Target Process ID: 2344 Target Image Path: msedge.exe Injected Content: Injected API: CreateRemoteThread

Figure 6: MITRE ATT&CK Framework Tactics and Techniques overview


Trend Vision One Sandbox Analysis

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Privilege Escalation (TA0004)	Process Injection (T1055) : Dynamic-link Library Injection (T1055.0 01)	<div> <div></div> <div></div> <div></div> </div> Characteristics: 1, 2
	Process Injection (T1055) : Portable Executable Injection (T1055.0 02)	<div> <div></div> <div></div> <div></div> </div> Characteristics: 1, 2
	Process Injection (T1055) : Process Hollowing (T1055.012)	<div> <div></div> <div></div> <div></div> </div> Characteristics: 1
	Obfuscated Files or Information (T1027)	<div> <div></div> <div></div> <div></div> </div> Characteristics: 1, 2, 3, 4, 5
Defense Evasion (TA0005)	Process Injection (T1055) : Dynamic-link Library Injection (T1055.0 01)	<div> <div></div> <div></div> <div></div> </div> Characteristics: 1, 2
	Process Injection (T1055) : Portable Executable Injection (T1055.0 02)	<div> <div></div> <div></div> <div></div> </div> Characteristics: 1, 2
	Process Injection (T1055) : Process Hollowing (T1055.012)	<div> <div></div> <div></div> <div></div> </div> Characteristics: 1
	Application Window Discovery (T1010)	<div> <div></div> <div></div> <div></div> </div> Characteristics: 1, 2
Discovery (TA0007)	Process Discovery (T1057)	<div> <div></div> <div></div> <div></div> </div> Characteristics: 1, 2, 3, 4, 5, 6, 7, 8
	System Information Discovery (T1082)	<div> <div></div> <div></div> <div></div> </div> Characteristics: 1, 2, 3
	File and Directory Discovery (T1083)	<div> <div></div> <div></div> <div></div> </div> Characteristics: 1
	System Time Discovery (T1124)	<div> <div></div> <div></div> <div></div> </div> Characteristics: 1
Command and Control (TA0011)	Data Encoding (T1132) : Standard Encoding (T1132.001)	<div> <div></div> <div></div> <div></div> </div> Characteristics: 1

© ATT&CK™ is a trademark of The MITRE Corporation.

Learn more
at TrendMicro.com

Copyright ©2025 Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro logo, Trend Vision One, Trend Companion, Deep Discovery, and the t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. Trend Micro, the Trend Micro logo, and the t-ball logo Reg. U.S. Pat. & Tm. Off. [DS00_Sandbox_Analysis_Datasheet_240730US]

TrendMicro.com

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy