Datasheet

# 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.

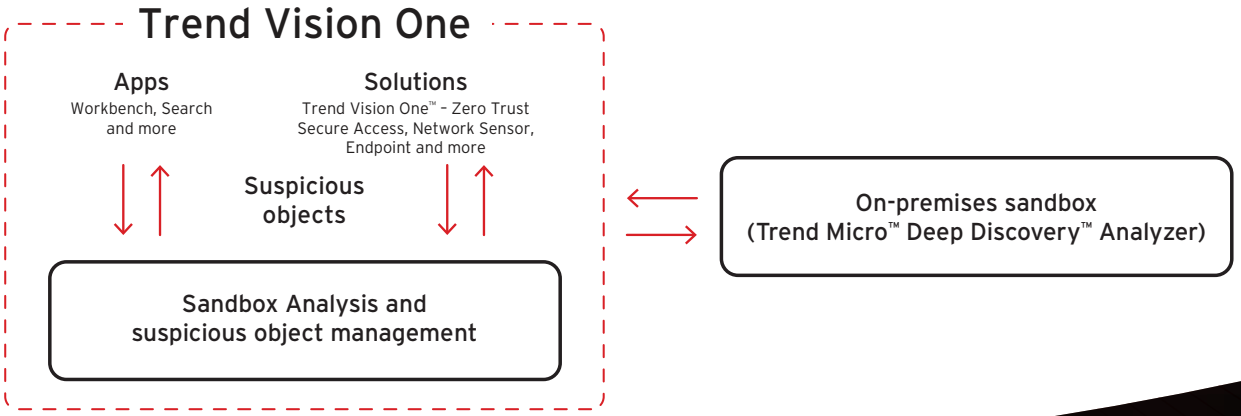
Sandbox Analysis samples can be submitted either manually or automatically without user intervention. High-risk samples are blocked automatically across all solutions right away. Collectively, this provides detailed threat context, helping inform how best to respond to—and manage—cyber risk.

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

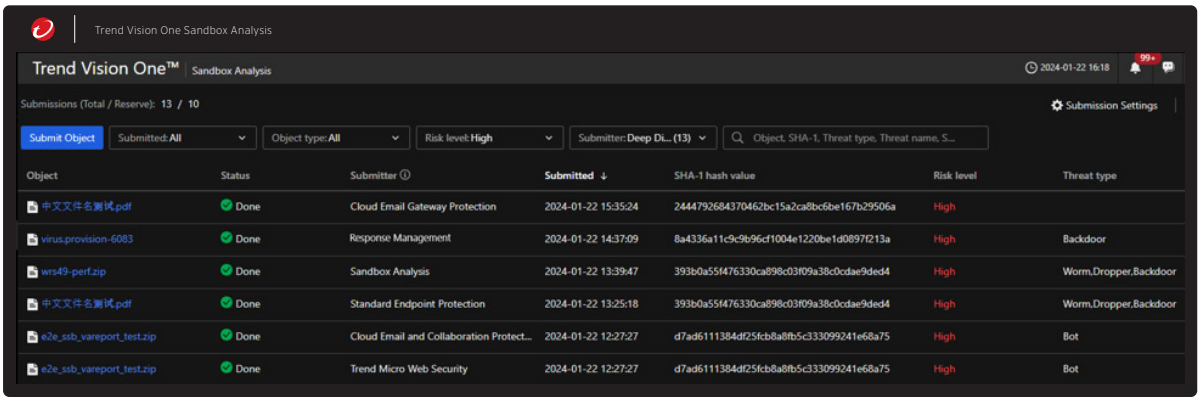



Figure 3: Sandbox Analysis Report overview

Figure 4: Object overview example

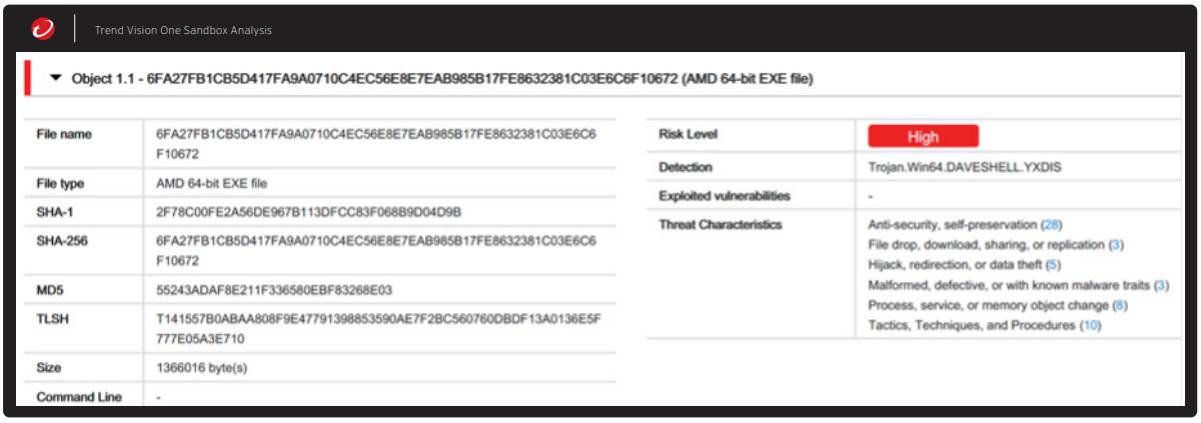



Figure 5: Notable threat characteristics and significance level overview

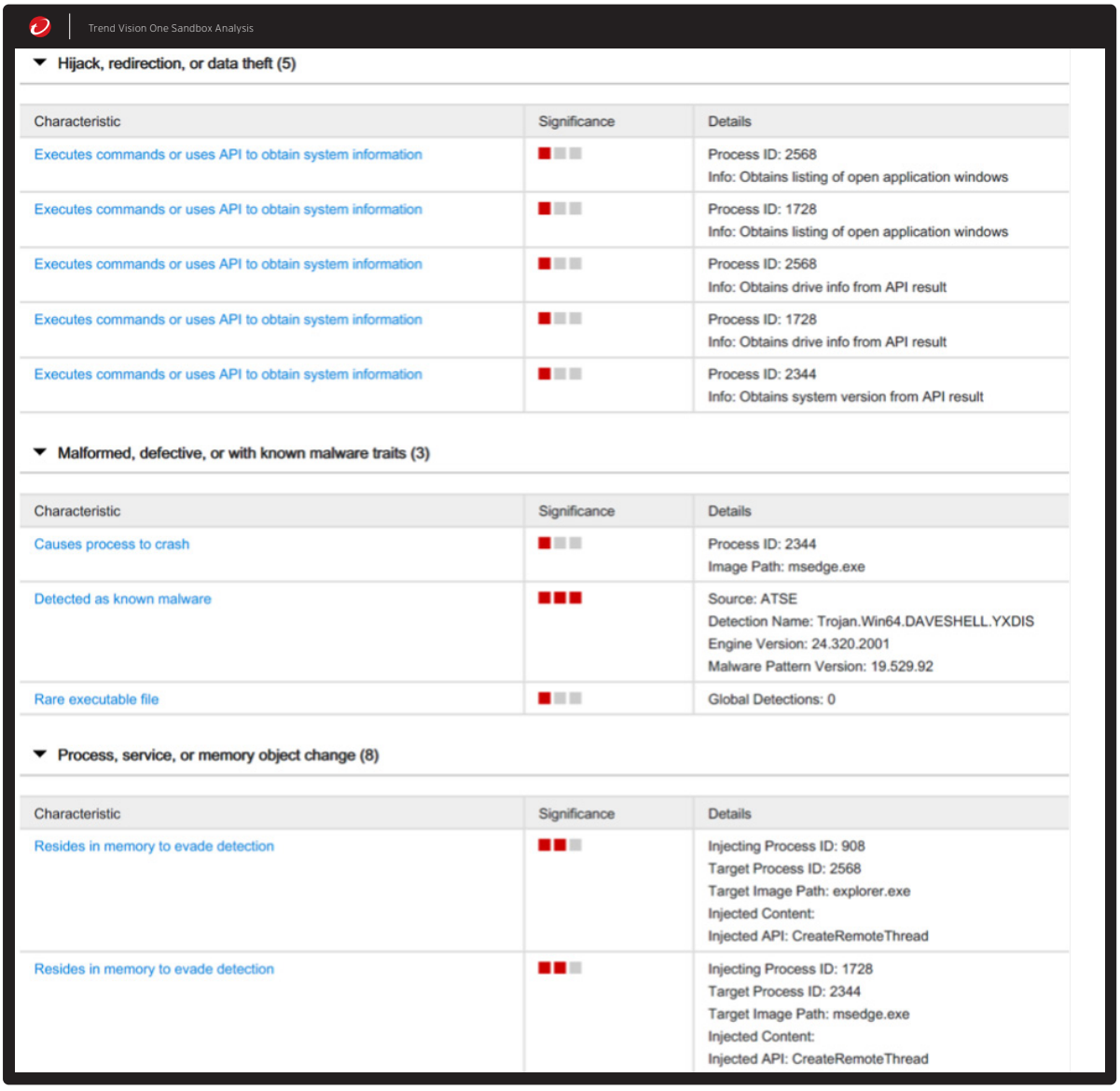
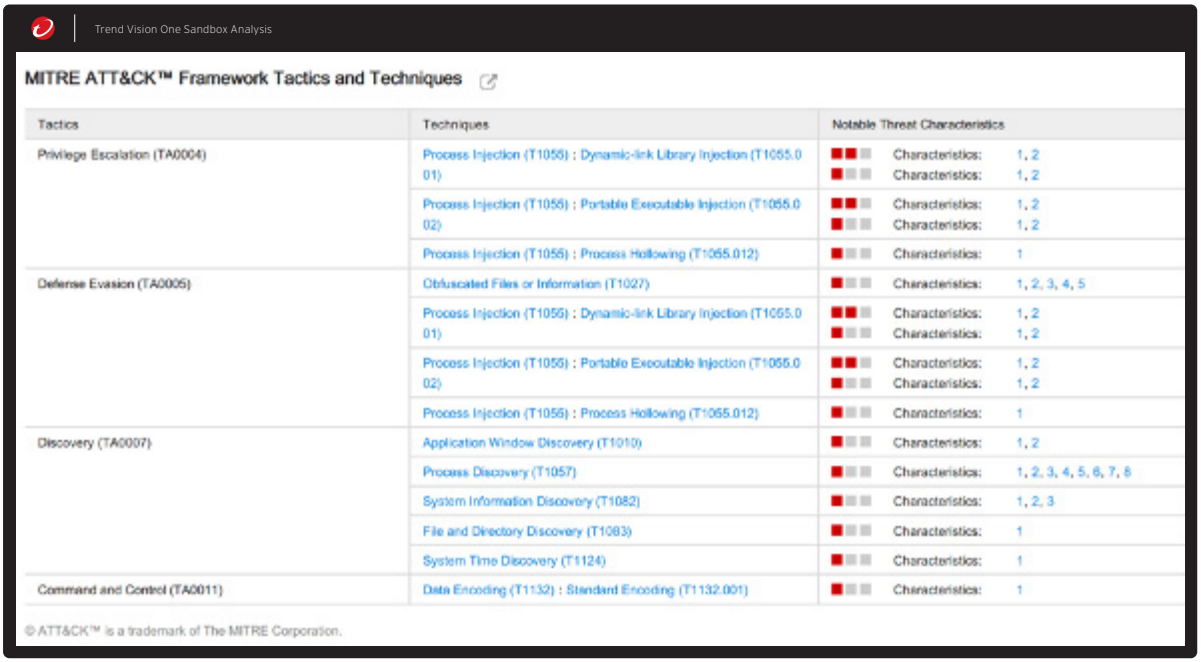


Figure 6: MITRE ATT&CK Framework Tactics and Techniques overview




**Learn more**
at TrendMicro.com