Symantec

DATA SHEET

Symantec Content Analysis – Dynamic Sandboxing

Respond to Malicious Threats That Elude Traditional Defenses

At a glance

Description

Advanced sandboxing within Symantec Content Analysis detects and analyzes unknown, advanced, and targeted malware using a unique, dual-detection approach that safely detonates suspicious files and URLs, reveals malicious behavior, and exposes zero-day threats.

Capabilities

- Comprehensive, enterprise-class malware detonation in highly realistic sandbox environments that match corporate “gold images”
- Combines dynamic, static, and reputational analysis techniques for more thorough exposure of malware
- Fully-scalable and customizable solution available via on-premises hardware or cloud
- Detailed forensics and shared threat intelligence
- Seamless integration with Symantec Endpoint Protection (SEP), Symantec Messaging Gateway (SMG), Symantec Security Analytics and many 3rd-party security solutions

Key Benefits

- Helps protect organizations against advanced, targeted attacks
- Prioritizes and accelerates incident response
- Delivers superior detection, more accurate and relevant analysis
- Exceptional performance, even on high-volume networks
- Transforms malware exposure into continuous security improvement
- Easily deployed as on-premises, cloud or hybrid solution

Symantec Content Analysis sandboxing is a key component of Symantec’s Advanced Threat Protection solution. It provides highly-scalable detection and analysis of unknown, advanced, and targeted malware. This adaptive and customizable sandbox solution delivers enterprise-class, comprehensive malware detonation and analysis using a unique, dual-detection approach to quickly analyze suspicious files and URLs, interact with running malware to reveal its complete behavior, and expose zero-day threats and unknown malware.

Expose More Malicious Behavior

Symantec’s sandboxing in Content Analysis utilizes a powerful dual-detection approach that combines virtualization and emulation to capture more malicious behavior across a wider range of custom environments that typical sandbox solutions miss.

Emulation Sandbox: An instrumented, fully-controlled, replicated PC computing environment emulates Windows systems to detect malware that otherwise will not detonate within a virtualized environment.

Virtualization Sandbox: Custom analysis profiles replicate actual Windows production environments, down to the applications and versions in use, to quickly spot anomalies and behavioral differences that unveil anti-analysis, sleep, and other advanced evasion techniques. A virtualized Android sandbox detects and analyzes mobile threats traversing enterprise networks.

Multiple Detection Techniques

Content Analysis sandboxing uses a combination of static and dynamic analysis techniques that employ standard, custom, and open source YARA patterns to unmask cleverly disguised malware. It detects packed malware and VM-aware samples that alter their behavior in an artificial environment, plus malware that attempts to wait out any sandbox analysis using short or long sleeps.

Defeat Anti-Analysis at Many Levels

Anti-analysis defeating tools – such as hook-based introspection, high-level and low-level event capture, and detection in both kernel and user modes – intercept and convert behavior into detailed forensic intelligence.

Interact with Running Malware

A flexible plug-in architecture extends detection and processing by interacting with running malware, clicking through dialog boxes and installers, and generating unique post-processing analysis artifacts.

Generate More Relevant Results

Virtual machine profiles replicate multiple custom production environments, allowing security analysts to analyze threats across a range of operating systems and applications and only those that apply to their environment, reducing false positives and optimizing analyst's workloads. They can closely match their organizations' desktop environments, or "gold images", gathering intelligence on malware targeting their organizations directly or seeking to exploit specific application vulnerabilities.

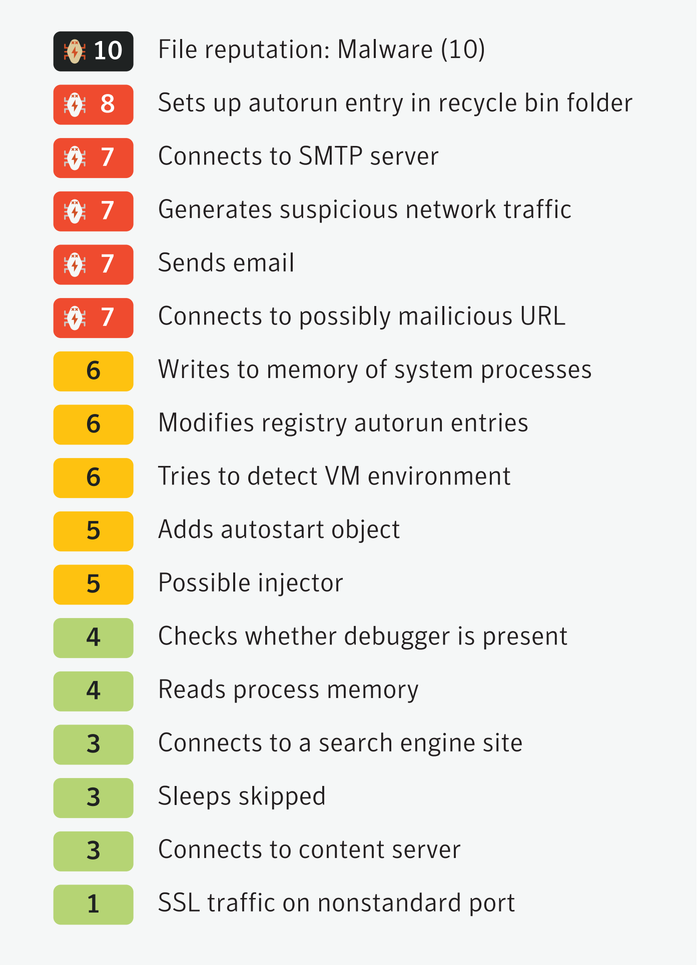
Customized Detection and Risk Scoring

Detection criteria, analysis parameters, firewall settings, and risk scoring can all be customized to add flexibility, unique detection, and fast response capabilities when analyzing non-traditional and targeted malware in unique production environments.

Adaptive Intelligence for Changing Threats

Since Content Analysis sandboxing does not rely on static signatures, its flexible detection patterns are designed to detect polymorphic files, single-use targeted malware, and fast-changing website domains.

Pattern Matching Results



10	File reputation: Malware (10)
8	Sets up autorun entry in recycle bin folder
7	Connects to SMTP server
7	Generates suspicious network traffic
7	Sends email
7	Connects to possibly mailicious URL
6	Writes to memory of system processes
6	Modifies registry autorun entries
6	Tries to detect VM environment
5	Adds autostart object
5	Possible injector
4	Checks whether debugger is present
4	Reads process memory
3	Connects to a search engine site
3	Sleeps skipped
3	Connects to content server
1	SSL traffic on nonstandard port

Clear scoring reveals malicious activity and prioritizes threats

Detailed Forensics for Remediation

Content Analysis sandboxing technology provides security defenders a comprehensive map of the damage – including both host-based and network indicators of compromise – that any malicious file or URL would cause to equivalently-configured production machines – without putting actual computers or sensitive data at risk.

Share Threat Intelligence

As unknown, advanced, or targeted malware and zero-day threats are exposed, the previously unseen or uncategorized threats are shared across the security infrastructure and to all Symantec customers through the Symantec Global Intelligent Network, a network effect of our 15,000 customers and over 175 million endpoints worldwide.

Inoculation for Forward Defenses

Content Analysis sandboxing turns unknown threats into known threats and shares threat data with others across the global network, improving the effectiveness of front-line defenses. By moving protection forward to termination points at the perimeter, such as Symantec ProxySG, Symantec Endpoint Protection, Secure Messaging Gateway, CloudSOC and others security solutions, blocking will immediately take place for subsequent attacks.

Flexible Deployment Options

Content Analysis sandboxing can be deployed to meet any customer environment. Options include:

- License for deployment on the same appliance with Content Analysis
- Configure as a stand-alone sandbox to support large enterprise networks
- Enable forwarding of unknown files to Symantec's cloud sandbox – Malware Analysis Service

Content Analysis Sandboxing Features

- Dual-detection emulated and virtual sandbox analysis environments
- Customizable Windows 7/10 profiles closely match corporate "gold image" production systems
- Virtualized Android sandbox detects mobile threats
- Pattern-based detection exposes malicious files and URLs including polymorphic, unique, and targeted threats
- Supports any PC file format
- Clicks through dialogs and installers to expose interactive malware requiring user interaction
- Thwarts VM-aware malware, bypasses sleep calls, and detects generic exploits such as "heap sprays"
- Customizable pattern matching, analysis settings, and risk scores
- Automatic pattern updates for continuous protection against fast-evolving threats
- Generates relevant, granular verdicts plus a complete range of analysis artifacts
- Seamlessly integrates with Symantec ProxySG, Symantec Endpoint Protection, Messaging Gateway and Security Analytics, as well as other 3rd-party solutions to provide detailed inspection of unknowns
- Uses the Symantec Global Intelligence Network for continuous threat sharing among our 15,000 customers and 175 million endpoints
- Supports centralized appliance management for enterprise provisioning and deployment
- Provides real-time sandboxing to delay file delivery until a complete verdict is rendered, protecting "first victims" from receiving malicious content

Content Analysis Sandboxing Benefits

- **Superior threat detection**: Unique dual-detection approach combines emulation and virtual sandboxing, plus static and dynamic analysis techniques to deliver unrivaled intelligence for unknown threats
- **Accurate and relevant analysis**: Customized virtual machine profiles running Windows 7 and Windows 10 closely replicate actual corporate gold images to detect targeted threats against actual production configurations, reducing security analyst workloads
- **Customizable analysis and risk scoring**: Automatic sample classification and risk scoring – augmented by custom detection patterns, interactive analysis plugins, and risk scores – flag suspicious system events based on degree of potential malicious activity within your unique environment
- **High throughput performance**: Parallel sample processing on up to 36 virtual machines per single Content Analysis appliance generates continuous enterprise-class performance on high-volume, high-threat networks
- **Improved incident response**: Helps prioritize and focus efforts of incident response teams, streamlining damage assessments and speeding remediation efforts
- **Inoculates forward defenses**: Shares threat intelligence with the Global Intelligence Network, providing rapid updates to inline forward termination points that quickly block newly exposed malware