Trustwave®

Trustwave MailMarshal Sandbox Service

Benefits

Unrivalled in Security

- 5+% additional threat detection of zero-day malware and stealthy attacks.
- Advanced machine-learning and dynamic runtime analysis detects all forms of targeted and advanced malware.
- Effective prefiltering limits the files sent to the sandbox, ensuring minimal latency and disruption.
- Monitoring that's difficult for the malware to detect and alter its behavior to evade detection.
- Safely execute suspicious code without risking harm to the host device or network.

Ease of Implementation

- Implemented as a cloud service, ensuring continual security with minimal performance impact.
- Scalable, with the ability to automate analysis of many samples.

Trustwave MailMarshal is the industry's most reliable and flexible email security solution with decades of leadership and recognition. Augment MailMarshal with the Sandbox Service to maximize catching what others miss.

The Trustwave MailMarshal Sandbox Service is an anti-malware layer available in MailMarshal On-Prem & Hybrid Cloud Edition and MailMarshal Cloud that detects both known and unknown malware.

Today's advanced malware is often engineered to evade detection by traditional security tools. Within an email gateway, traditional tools can look for file structures and code, but they cannot observe the behavior of the running software.

Malware sandboxing is a way of dynamically running an untrusted file or application within a safe, isolated environment to check what it does.

Sandboxing can detect many behaviors, including Operating System calls, file activity, Registry edits, in-memory activity, and network traffic. The Sandbox destroys fast-moving threats like EMOTET early in the attack chain and minimizes the risk of exposure to costly malware attacks.

Ultimately, the Trustwave MailMarshal Sandbox detects malware that other sandboxes often miss.

Why Add a Sandbox to Your Multi-Layered Email Security?

These are the key reasons to choose a sandbox.

Advanced Detection

The increasing attack surface and targeted nature of today's threats have made it hard for traditional defenses to keep up. By observing behavior and using advanced AI the sandbox is not reliant on set rules or signatures for detection.

Deferred Payloads

Many malware campaigns start with an inconspicuous attachment that downloads the payload when it runs. Detonating the attachment in a sandbox and observing the full infection chain reveals the true nature of the threat.

Risk & Compliance

Cyber security failures are subject to more fines and reputational damage than ever before.

Deploying an advanced sandbox minimizes the chance of malware getting through established defenses.

Efficiency & Scale

A Sandbox is best deployed as a scalable cloud service which can apply many advanced forms of analysis and detection. Deploying such techniques locally is usually suboptimal due to the computational load and infrastructure cost.

How it works

The Trustwave MailMarshal Sandbox is implemented as a cloud service and capable of emulating a complete host. This makes it difficult for malware to determine whether it is running in a sandbox, and the Sandbox also watches for tricks that malware uses to try to evade detection.

In all, the Sandbox:

- Follows the full infection chain and monitors attempts to evade the sandbox, effectively dealing with geo-aware, VM-aware and time-delayed malware.
- Detects all types of malware regardless of the target operation system.
- Includes technologies to detect credential theft and unauthorised encryption attempts from ransomware.
- Employs regional data centers that ensure low-latency and data privacy policies can be managed for retention and data sharing.
- Delivers comprehensive analysis reports with configurable detail and granular verdicts.

Ultimately, the Sandbox returns an overall score for malicious behavior. Then the customer's policies can dictate how email is managed based upon the scores.

Content	• Version-less inspection and analysis • Identification of malicious document macros
Operating System	• Dormant code analysis • Exploit symptom diagnosis • True kernel visibility
CPU	• Dynamic code analysis elicits malicious behaviors • Evasion detection and TLS fingerprinting
Memory	• Inspection of malware memory, including encrypted strings

Trustwave MailMarshal Sandbox is comprehensive, analyzing potential threats from the hardware and the operating system to the email content

Trustwave MailMarshal Sandbox Goes Further than Other Sandboxes

The Trustwave MailMarshal Sandbox Service goes much further than other sandbox approaches with the following additional capabilities.

Credential Theft

- Custom Yara rules applied to memory dumps
- API tracing shows when other process' memory is manipulated or code is injected
- CookieGuard detects access to stored cookies
- Behavioral detections for credential theft

Ransomware Detection

- CryptoGuard detects encryption in-progress
- Monitoring for excessive file manipulation
- Canary files used to flag malicious access
- Monitoring of C2 and high- risk site access

Anti-Evasion

- Multiple locales for geo- aware malware
- Simulates real system for VM-aware malware
- System clock adjustment for time-dependent payloads
- Full web access with malware run to completion
- AMSI detections for obfuscated scripts

Upgrade Your Email Protection Today

The Trustwave MailMarshal Sandbox adds a premier level of protection against unknown malware delivered through emailed attachments. This maximizes protection for your users from the most sophisticated threats attempting to disrupt your business.

Trustwave®

www.trustwave.com

MMSB-0122