MailGate

DATA SHEET

MailGate SC Sandbox

Strengthen antivirus defense with dynamic malware analysis

Our next-generation sandbox provides a complete ATP solution with an advanced emulation based purpose-built environment for real-time malware analysis of email attachments. The cloud-based solution provides the ability to run in-depth and sophisticated analysis of an unknown or suspicious file in an isolated environment, thereby monitoring its execution and likely malicious impact that could threaten the integrity of your environment.

Overview

Sandboxing technology is becoming increasingly critical for advanced malware detection. MailGateSC Sandbox solution leverage's extensive threat research experience to understand how malware authors attempt to evade conventional signature-based protection with cleverly crafted malicious code.

With a view to addressing this malware-detection gap, MailGate provides next-generation sandbox, utilizing full-system emulation to provide proactive defense against evasive and targeted threats.

Uncovers the modern cyber threat from its guise

The sandbox is designed to provide IT security, forensics teams and threat analysts with high-resolution visibility into the behavior of the modern malware. Replacing first- generation sandbox techniques with more evolved capabilities like full-system emulation, the solution provides targeted attack protection, visibility and analysis by detecting, blocking and responding to evasive, unknown threats.

This approach delivers more reliable defense and helps identify persistent threats, zero-day exploits and obfuscated attacks like malicious JavaScript code that fly under the radar.

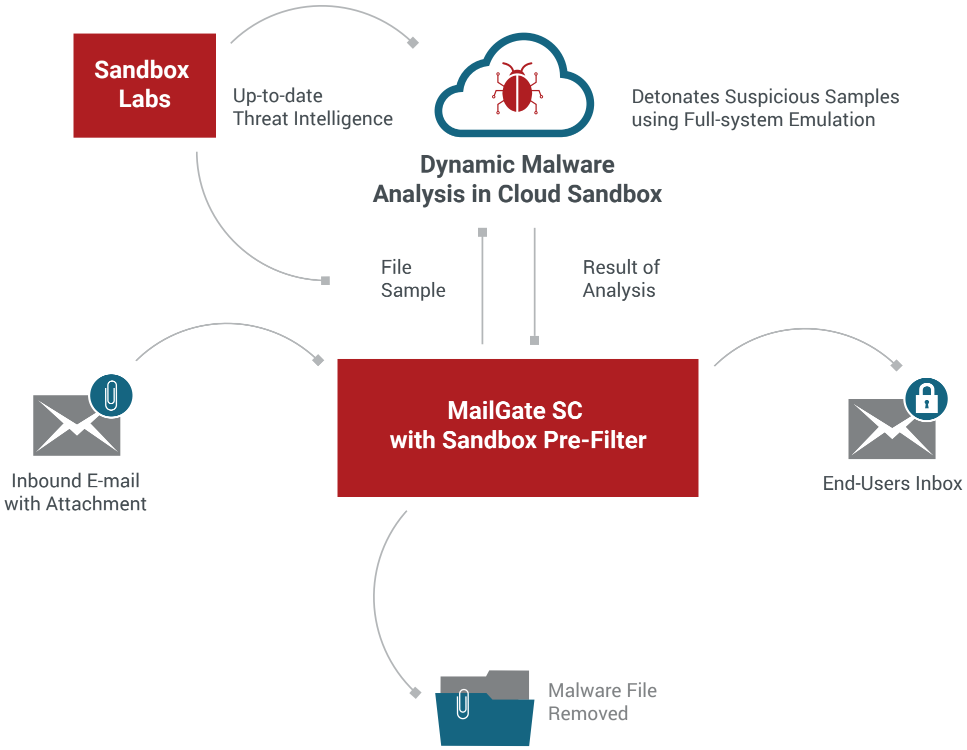
Aligns with your existing MailGate SC security features

- Complements other MailGate defenses to quickly and accurately detect and remove evasive threats using powerful, cloud-based threat analysis technology
- Complemented by a local in- solution pre-filter, which provides the first line of defense. This results in low resource usage and faster analysis of suspicious files in the sandbox
- Easy and rapid deployment helps reduce cost and complexity associated with implementing advanced threat detection systems
- Provides conclusive evidence for suspicious websites, files, applications and events by analyzing threats in a secure environment

Key Benefits:

- Secluded environment providing automated real-time malware analysis to uncover unknown or suspicious malicious file
- Easy and rapid deployment without any additional hardware or appliance upgrade
- Cloud-based threat analysis for faster and consistent performance
- Complete visibility into malware behaviors
- Safe execution and inspection of threat samples
- Provides granular analysis of malicious web sites, the identification of web-based zero-day exploits, and the deobfuscation of malicious script or code

MailGate's cloud-based next-gen sandbox provides simple yet effective detection for evasive threats without impacting performance and fits with ease in existing security infrastructure.


Sandbox Labs
Up-to-date Threat Intelligence
Detonates Suspicious Samples using Full-system Emulation
Dynamic Malware Analysis in Cloud Sandbox
File Sample
Result of Analysis
MailGate SC with Sandbox Pre-Filter
Inbound E-mail with Attachment
End-Users Inbox
Malware File Removed

Advanced Threat Protection

Protect against incidents such as Ransom Lockouts, C&C Callbacks and other sophisticated threats carried by Ransomware, Malware and botnets.

Sandboxing removes suspicious attachments from the mail flow, opening them in an isolated environment.

Dedicated support with rich threat research data

Keep pace with malware advancements using state-of-the-art threat research.

Evaluation

To evaluate MailGate Sandbox, please contact your MailGate SC account manager.

Protect your environment in real time →

mailgatesc.com