ZSCALER WHITE PAPER

Combating Advanced Persistent Threats (APTs) with Cloud Sandboxing

GET THE BENEFITS OF COMPLETE SANDBOXING IN A CLOUD-FIRST WORLD

THE NEED FOR SANDBOXING

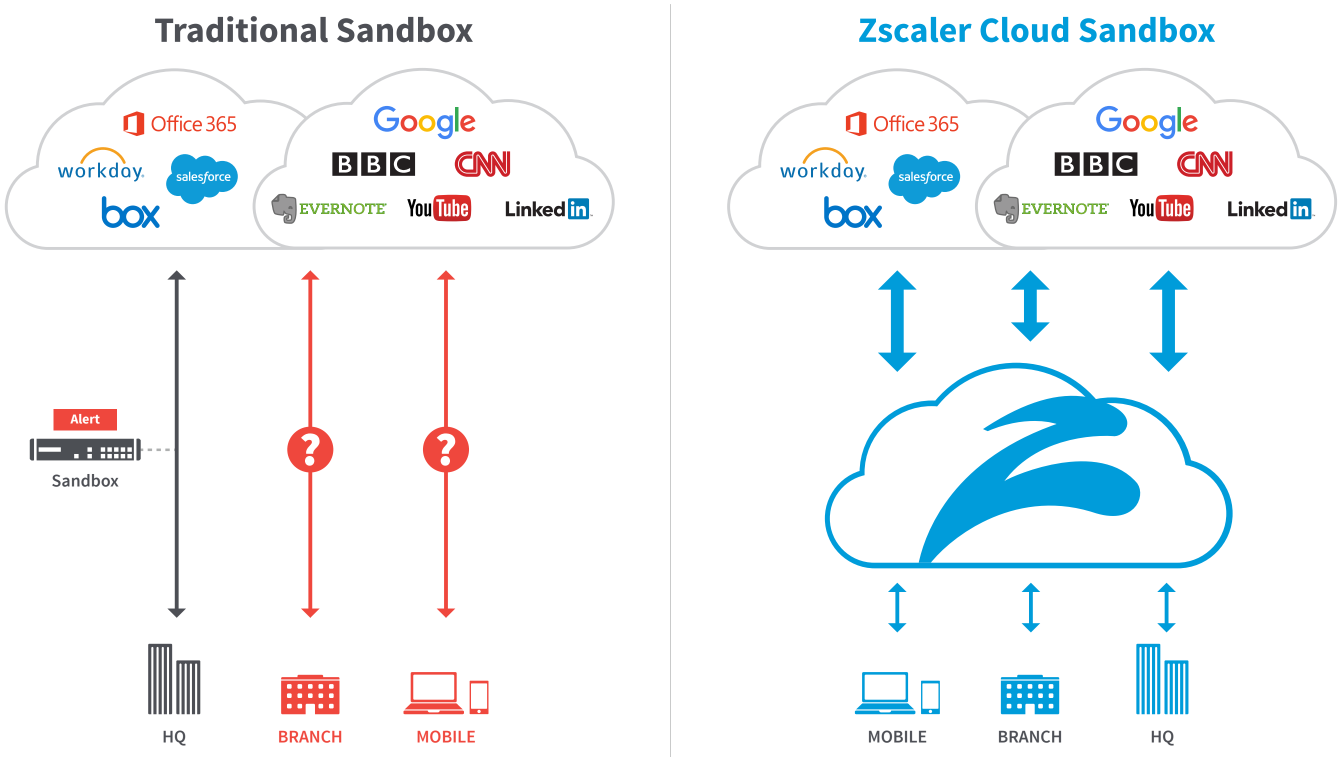
How can the enterprise efficiently protect itself against previously unforeseen threats, especially when dealing with highly mobile and unpredictable end-users? Signature-based approaches depend on an understanding of patterns that suggest an attack, and therefore are incapable of detecting threats that are not already being searched for by these systems. A zero-day threat is an attack that exploits a previously unknown vulnerability, meaning that the attack occurs on day zero of awareness of the exploit. Signature-based security methods are futile in preventing zero-day threats because zero-day threats obviously lack threat histories and known patterns that can be detected.

Blacklisting, whitelisting, anti-virus systems, intrusion detection systems (IDS) and intrusion prevention systems (IPS) are measures for catching “known threats” that have previously been observed and have unique characteristics that can be monitored to protect end users. These protections are all signature based, in that they involve searching for known patterns within executable code. Preventing attacks with these approaches therefore requires a clear knowledge of the threat history.

Enterprises also increasingly face advanced persistent threats (APTs) that may leverage previously unknown attack techniques and vulnerabilities. Attacks are increasingly multi-part and sophisticated, sometimes combining APTs and zero-day threats. Sandboxing, which uses behavior analysis, is an important technique for identifying previously unknown threats because this approach does not rely on signatures. Well-executed behavioral analysis can also result in low false-positives compared to traditional pattern matching or signature-based approaches because suspicious activity is observed over a period of time and confirmed. With sandboxing solutions, a binary file is permitted to run in a controlled environment, and its behavior is monitored and analyzed. Identification of suspicious behavior—such as the downloading of malware, accessing the file system, logging keystrokes, etc. — allows for the identification of malicious content, even if the sample or techniques leveraged have never been previously observed.

LEVERAGING A CLOUD ARCHITECTURE FOR BEHAVIORAL ANALYSIS

Zscaler, the cloud security leader, combines the benefits of behavioral analysis with the reach of a SaaS-based service to collect and analyze binary files from global clouds, analyze them centrally and ensure that all customers benefit when even a single malicious file is identified.



Limited Capacity with no SSL inspection

- *Users off network go unprotected*
- *Sandbox allows files to pass and infect*
- *Threat data is often localized and not shared*

Unlimited Capacity with full SSL inspection

- *Easily scale across all users/locations*
- *Inline architecture holds file until clean*
- *Cloud effect shares blocks to all customers*

Appliance-based APT approaches are limited to protecting employees in the office and are insufficient for protecting the enterprise; road warriors and home-based workers remain exposed to APTs and zero-day attacks. When sandboxing is part of a comprehensive and multi-faceted cloud security solution—as opposed to just being offered as a point product—it is not limited to simply being a detective control highlighting malicious files that were downloaded, but may not have succeeded in compromising end user machines.

Zscaler's advanced security solution provides full SSL inspection and inline blocking; firewalls and tap-mode sandbox appliances can not accomplish this. It provides continuous coverage for any user, anywhere, and Zscaler's advanced security solution scans every packet, every byte, every time—for both inbound and outbound traffic. It scans all communications to block botnets calling home, cookie stealing and anonymizers, and it provides vulnerability shielding. Zscaler also generates dynamic risk scores based on content and behavior to block zero-day threats. Zscaler has numerous industry partnerships to ensure access to real-time feeds of known compromises, and every transaction is logged in detail for forensic analysis.

ADVANTAGES OF ZSCALER'S CLOUD SANDBOX

Zscaler identifies and catches threats via a sandboxed analysis of binaries. Zscaler's Cloud Sandbox includes behavioral analysis, which delivers three key differentiators in the market:

Protection of ALL users, including mobile

Unlike appliance-based alternatives, Zscaler's Cloud Sandbox protects all users, including the difficult to follow mobile user, from APTs. By delivering sandboxing from the cloud, protection is alway on and placed closest to the user regardless of location or connection. On or off network, the users connects to the Zscaler Cloud Platform and Sandboxing solution first before accessing the Internet, so all traffic is always being inspected. This architecture far surpasses traditional data center sandbox approaches, as these appliances
go blind once the users drops off the corporate network.

Immediate Protection with the Cloud Effect

Global, unified collection of samples across the Zscaler Cloud Platform ensures that even a single targeted attack against a single victim can automatically improve security protection for all customers globally. Once a threat is confirmed, all Zscaler customers receive worldwide protection from it. We call this the Cloud-effect, and it easily out-paces appliance approaches to keep users safe from new and emerging threats as they are discovered across the globe.

Greater Context for Threat Protection

The integration of big data, static analysis and behavioral analysis provides a fuller context for threat protection. By combining behavioral analysis and big data analysis, Zscaler enhances traditional behavioral analysis techniques. In traditional behavioral analysis, a sample is analyzed in isolation. In that scenario, while behavioral analysis would uncover the fact that a given sample requested a specific URL when executed, the behavioral analysis engine would have no way of knowing if the request was benign or malicious. Zscaler is able to further interrogate this information by comparing it to all historical transactions to ensure that the behavioral analysis engine benefits from the latest intelligence derived from mining the overall Zscaler cloud.

IMPLEMENTING ZSCALER ADVANCED SECURITY

With Zscaler, behavioral analysis is not a separate offering, but rather an enhancement of an already powerful advanced security suite. Zscaler Enforcement Nodes (ZENs) are continually collecting suspicious binary files and delivering them to the central behavioral analysis engine. Samples are executed and monitored in controlled environment and malicious behaviors are recorded and analyzed. Collected metadata is compared to intelligence sources, and malicious files are blocked at ZENs.

This is accomplished through an automated, six-step process:

1. Fast Pre-Processing – Pre-processing ensures that files are quickly classified to identify those that will benefit from behavioral analysis. Files are divided into those that are portable executable files and those that aren't, and the portable executable files are then parsed to ensure that they are appropriately formed.

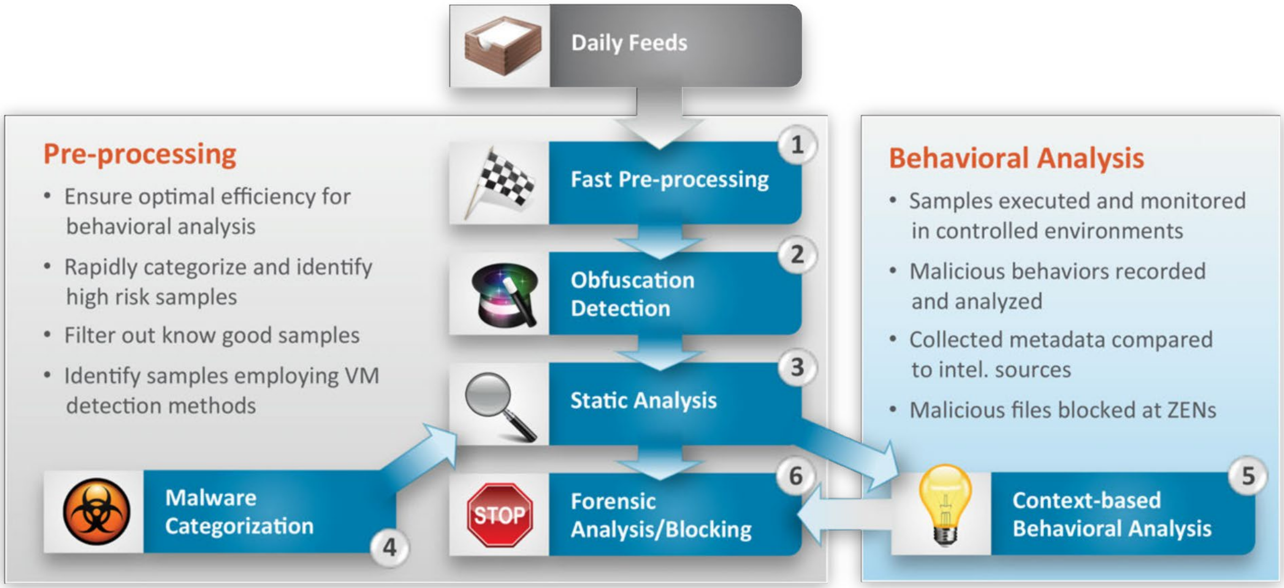
2. Obfuscation Detection – Malware often leverages file formats called "packers" to obfuscate file content and further complicate reverse engineering of the sample. Static analysis techniques are applied to identify those portable executable files that have been packed and identify the packer that has been leveraged. Packed files must first be unpacked before additional static analysis can be applied, and identifying the packer used can assist in identifying particular malware families.

3. Static Analysis – Applying static analysis to unpacked samples can identify malicious samples and bypass the need to conduct behavioral analysis, which is less efficient due to the fact that samples must be permitted to execute.

4. Malware Categorization – When static analysis techniques uncover malware, the samples are named and categorized. Malicious samples are gathered to ensure that new static analysis checks are added to the overall process to continually improve detection rates.

5. Context-Based Behavioral Analysis – Unpacked portable executable files not already flagged as malicious are delivered to the behavioral analysis engine. Files are executed in a controlled environment and monitored for malicious behavior. Meta data retrieved during the process—such as requested URLs—are also compared to other Zscaler data sources. This hybrid approach ensures that files are not analyzed in isolation, but instead benefit from previous analysis and data collected from data mining efforts and partner data feeds. An overall risk score is calculated based on this analysis to help policy and configuration rules decide what to do with the files.

6. Forensic Analysis/Blocking – Transaction reports are generated for forensic analysis, and threats are blocked for all users on the Zscaler Security Cloud.


Daily Feeds
Pre-processing
Ensure optimal efficiency for behavioral analysis
Rapidly categorize and identify high risk samples
Filter out know good samples
Identify samples employing VM detection methods
1
Fast Pre-processing
2
Obfuscation Detection
3
Static Analysis
4
Malware Categorization
STOP
6
Forensic Analysis/Blocking
Behavioral Analysis
Samples executed and monitored in controlled environments
Malicious behaviors recorded and analyzed
Collected metadata compared to intel. sources
Malicious files blocked at ZENs
5
Context-based Behavioral Analysis

Zscaler's Cloud Sandbox includes behavioral analysis, which is delivered through an automated, six-step process.

CONCLUSION

The enterprise will continue to encounter APTs that leverage previously unknown attack techniques and vulnerabilities. Sandboxing is essential for protection against APTs. Appliance-based solutions are insufficient for protecting enterprise resources that are highly mobile and platform independent. Zscaler Cloud Sandbox offers an innovative, cloud-based solution that allows the enterprise to successfully combat APTs with context-based behavioral analysis. Organizations can integrate big data and behavioral analysis to protect enterprise resources and ensure the protection of all users, including mobile. The result is the enterprise can gain immediate global protection once a global threat is confirmed and build greater context to enable advanced threat protection.

ABOUT ZSCALER

Zscaler™ enables organizations to securely transform from the old world of IT, which focused on securing the internal network, to the world of cloud and mobility, where the Internet is the new corporate network. Zscaler delivers the inbound and outbound gateway stacks as a service, providing secure access to the Internet and applications in the data center or cloud. Each day, the Zscaler cloud processes more than 160B requests, blocking 100M+ threats for 5,000 organizations in 185 countries, and the ThreatLabZ research team provides continuous protection from new and evolving threats. Visit **www.zscaler.com**.

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/company/zscaler
twitter.com/zscaler
youtube.com/zscaler
blog.zscaler.com