DATA SHEET

Zscaler Cloud Sandbox

Protection from ransomware and polymorphic threats

Zscaler Cloud Sandbox uses advanced behavioral analysis techniques to find and block zero-day threats. Delivered as a service from the Zscaler global security cloud, Zscaler Cloud Sandbox provides a higher level of threat protection than any other solution.

Stop threats that bypass traditional security controls

It's pretty well understood that traditional signature-based security approaches are falling behind in the task of protecting today's organizations. The critical weakness is that in order to stop a threat with a signature, you need to have prior knowledge of the threat. With the alarming rise of zero-day ransomware and polymorphic malware, organizations need to move beyond signature-based detection and add sandboxing as an additional layer of defense. Sandboxing uses dynamic analysis to monitor file behavior in an isolated environment to protect users from zero-day threats.

The challenge with appliance-based sandboxes is that they are traditionally deployed in centralized gateways, and hub-and-spoke architectures are needed to centrally route all traffic for inspection. That means traffic from remote offices must use expensive Multiprotocol Label Switching (MPLS) to backhaul traffic, and mobile users must use slow VPN connections. Sandbox appliances themselves are limited by their finite processing power. This limits the amount of inspection you can afford to deliver, especially when it comes to SSL, where a majority of malware can hide. The cost of ownership also requires administration, software updates and proper integration with other security appliances, which drives up costs and IT requirements even more.

WHY ZSCALER CLOUD SANDBOX

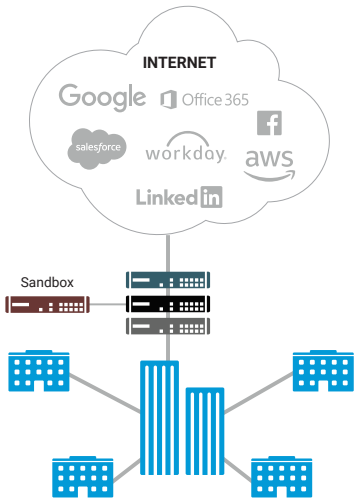
- **Simply scalable:** Break free of costly appliances and architectural compromises. Zscaler Cloud Sandbox easily scales to protect the entire organization, including remote offices and mobile users.
- **Better protection:** Built as an integrated service into the Zscaler Cloud Security Platform, Zscaler Cloud Sandbox provides native inline protection across all traffic, including SSL traffic.
- **Cloud effect:** Every new threat uncovered by Zscaler Cloud Sandbox is instantly shared across the Zscaler cloud and blocked for all users. Get the power of extended visibility far beyond the scope of any other sandbox offering on the market.
- **Cost effective:** Since Zscaler Cloud Sandbox is delivered as a service, you only pay for what you need instead of overpaying for appliance performance. And as your needs grow, you'll never run out of inspection capacity.

> "Analysis of one of our larger datasets showed that 99% of malware hashes are seen for only 58 seconds or less. This reflects how quickly hackers are modifying their code to avoid detection."
>
> — **Verizon,** 2016 Data Breach Investigations Report

Zscaler Cloud Sandbox

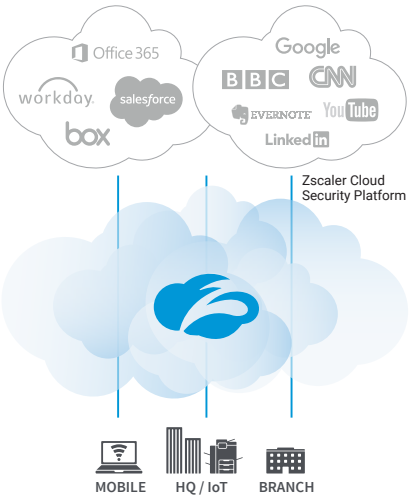
With Zscaler, you can sandbox any suspicious or unknown file without backhauling traffic to the data center. Since Zscaler Cloud Sandbox is implemented from the cloud, it protects all of your users, regardless of their locations. This means that remote office workers and mobile users get the same level of protection as the users at your headquarters, without costly MPLS links or cumbersome VPN connections. Zscaler Cloud Sandbox is architected to provide inline protection to block threats before they enter your network. Malicious files are instantly blocked, quarantined, or flagged based on your defined policies. Can you afford to allow ransomware to land on your endpoint while your appliance-based sandbox is still scanning it?

Hub-and-spoke sandboxing
Expensive and poor protection



- Costly appliances and backhaul links
- Sandbox often sits out-of-line
- Users outside your network go unprotected

Zscaler Cloud Sandbox
Cost-effective and complete protection



- Better user experience and more cost effective to deploy and manage
- All users regardless of location receive the same degree of inline protection

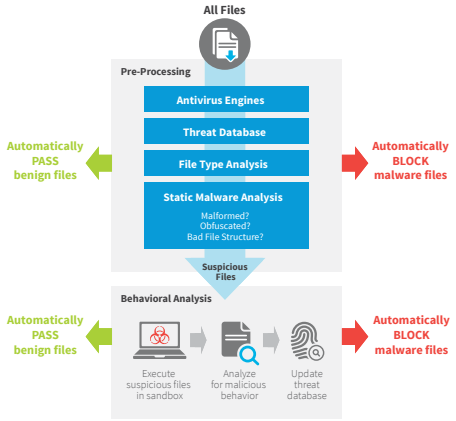
WHY ZSCALER CLOUD SANDBOX IS BETTER THAN HARDWARE-BASED SANDBOXES:

- True zero-day malware protection — it doesn't just alert, it blocks
- Consistently enforces policies across all users and devices, including mobile and remote office users
- Inspects all traffic, including SSL
- Inspects inbound and outbound traffic to prevent botnet communications and data extraction
- Sandboxes all unknown traffic and files from suspicious locations, including blocking all executables
- Uses the latest threat intelligence, with constant updates — more than 120,000 unique updates per day

Unlike appliances, which work in isolation, Zscaler Cloud Sandbox is fully integrated into the Zscaler Cloud Security Platform to deliver maximum threat visibility and multilevel protection. Because Zscaler is delivered as a service, there is no hardware deploy and manage, and no software to update.

Total sandbox protection for all traffic, including SSL

The processing power of Zscaler Cloud Sandbox lets us inspect all suspicious and unknown files with efficiency. Data is correlated across multiple security engines to identify and block sophisticated threats that go undetected by traditional appliances. By performing this in-depth level of sandbox pre-processing, we streamline the detection of suspicious files and improve the user experience. And because SSL inspection is native to the cloud security platform, the tactic of hiding attacks behind encryption fails as well. Malicious files are instantly blocked, quarantined, or flagged based on your defined policy, which can be easily scaled across all users.



Zscaler Cloud Sandbox uses cloud intelligence gained from more than 60 billion transactions processed each day at peak periods and more than 120,000 unique security updates. Once a threat is identified anywhere in the Zscaler cloud, it is immediately blocked for all customers. By default, the Zscaler security cloud sandboxes all executables and libraries to improve the protection to all customers. Zscaler also incorporates over 40 partner threat feeds to make sure the latest threat intelligence is applied across the cloud, which minimizes the number of files that need to be sandboxed.

Zscaler Cloud Sandbox provides:

Integrated platform service

- Pre-filters all known threats using threat feeds from 40+ security partners
- Offers native SSL inspection to close security gaps
- Provides APT protection — for both inbound and outbound traffic
- Delivers rich forensics — including intelligence on users, locations, origins, and evasive tactics

Inline inspection of all suspicious and unknown files

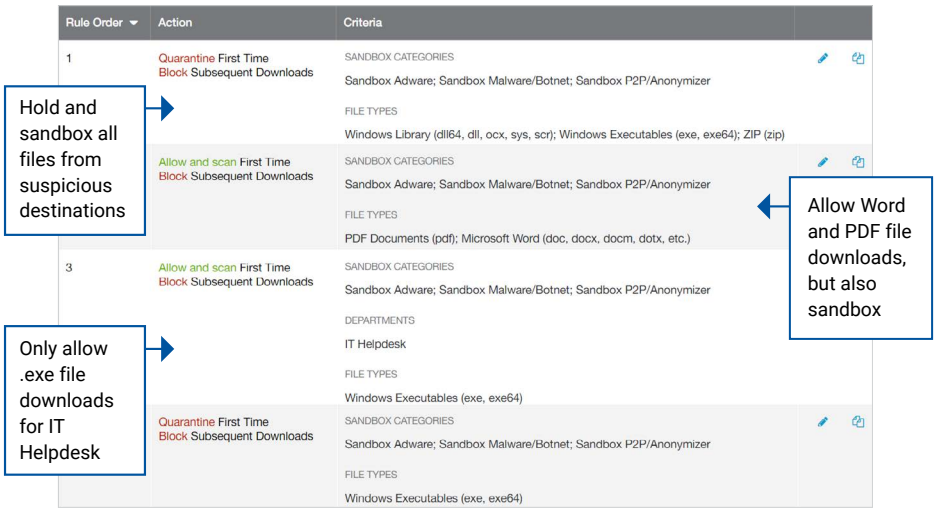
- Fully analyzes executables, libraries, Office documents, archives, and web and mobile content
- Enforces patient-zero quarantines
- Enables manual file submission via a sandbox scanning portal

Uniform policies across all users and locations

- Defines global policies from a single console
- Enforces policy changes immediately across all users, regardless of location

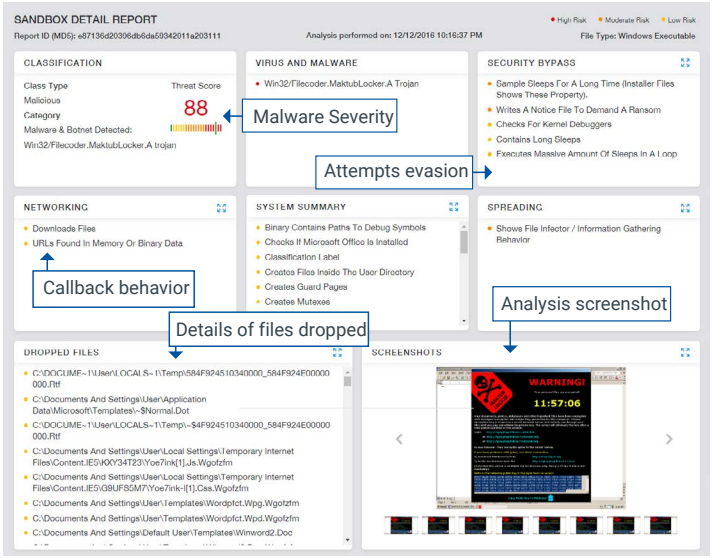
Optimize security policies for protection and user experience

With Zscaler Cloud Sandbox, you have the flexibility to tailor your security policies to your own protection needs. You can write policies that allow you to sandbox files by users, file type, and other criteria. For example, you can sandbox unknown spreadsheets your CFO is trying to download and quarantine them before they have the chance to infect the CFO's laptop.



Complete visibility into zscaler cloud sandbox analysis

For organizations that need in-depth understanding of malware analysis, Zscaler Cloud Sandbox provides extensive reporting on all identified behaviors. To help drive internal investigations, you can review key Indicators of Compromise (IOC), as well as forward your logs to a Security Information and Event Manager (SIEM) to streamline your security efforts further.



A cryptolocker attack: before and after zscaler cloud sandbox

An international bank had just begun evaluating Zscaler Cloud Sandbox and initiated a minimal rollout when it was first attacked by CryptoLocker. In a six-hour period, 352 emails infected with CryptoLocker were sent to employees. During the attack, 114 of the emails evaded the bank's legacy controls. Nine employees clicked the link embedded in the emails and downloaded the malware payload. Though you might think the high cost of ransomware is due to ransom demands, consider the cost in productivity:

Ransomware attack before Zscaler

- Nine employees had their accounts locked while their machines and profiles were rebuilt
- 6,769 network file shares had to be restored from backup
- 11 IBM resources had to be restored, an effort that took 121 hours
- Nine computer emergency response team (CERT) resources had to be restored, which took 108 hours
- There were four executive briefings over five days
- 45 hours of management time was expended on the issue

Ransomware attack after Zscaler

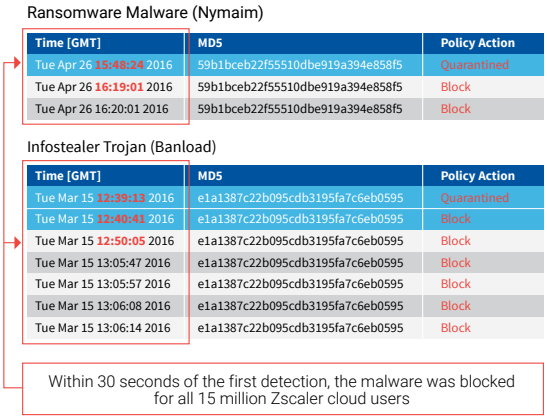
Less than a week after its initial attack, the bank experienced another CryptoLocker attack. But by this time the bank had activated Zscaler Cloud Sandbox for all of its users. In a six-hour period, 5,405 infected emails arrived and 169 of them made it to users' inboxes. Of those, 11 employees clicked the link in the infected email. But this time, there was not a single infection.

> "We turned it on and it just worked."
>
> **— Zscaler Banking Customer**

The cloud effect: zscaler cloud sandbox vs. Others

Zscaler Cloud Sandbox is integrated into the world's largest security cloud, so protection from zero-days can be delivered at a scale not possible with appliance-based products or any other cloud solutions.

In March 2016, new attempts to attack a Zscaler customer in the aviation industry were detected. Zscaler Cloud Sandbox analyzed and blocked the threats, and in a matter of 30 seconds, blocked them for all 15 million users on the Zscaler cloud around the world. How fast can appliance-based sandboxes do that?



> "With Zscaler, we have found a product that is that powerful."
>
> **– Zscaler Aviation Customer**

Why Zscaler Cloud Sandbox

Simply Scalable

Break free from costly gateway-based architectures. Scale protection across all users and all locations with ease from the cloud

Better Protection

Deliver a fully integrated sandbox solution that can inspect all traffic, including SSL, without performance limitations

Cost-Effective

Minimize IT procurement and administration costs with protection that easily grows with your needs

Cloud Intelligence

Empower your sandbox with the power and visibility of the world's largest security cloud

Activate Zscaler Cloud Sandbox Instantly

If you already use the award-winning Zscaler Cloud Security Platform, you may be one click away from activating Zscaler Cloud Sandbox.

The Zscaler Cloud Security Platform

Zscaler ensures that more than 15 million employees at more than 5,000 enterprise and government organizations worldwide are protected against cyberattacks and data breaches, while staying fully compliant with corporate and regulatory policies. Our award-winning cloud security platform delivers a safe and productive Web experience for every user, from any device, and from any location. We effectively move security into the Internet backbone, operating in more than 100 data centers around the world and enabling organizations to fully leverage the promise of cloud and mobile computing with unparalleled and uncompromising protection and performance. Learn more at **www.zscaler.com**

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com