DATA SHEET

Zscaler™ Cloud Sandbox

Intelligent patient-zero protection

Zscaler Cloud Sandbox is built on a breakthrough proxy-based architecture for inline detection, prevention, and quarantine for unknown attacks, including threats hiding in TLS/SSL traffic. Driven by advanced AI/ML, Cloud Sandbox stops patient-zero attacks with instant verdicts for common file types and automatic quarantine for high-risk unknown threats.

When was the last time you launched email client software to check your email? Things have changed. Enterprises are rapidly embracing digital transformation to fulfill the high demand for SaaS applications, public cloud workloads, and remote access, which have dramatically expanded and opened up new attack surfaces for businesses whose network infrastructures are based on the outdated castle-and-moat model. Modern adversaries know this and are taking advantage by crafting and launching automated and highly targeted attacks that easily bypass traditional legacy network-centric malware defenses, often resulting in patient-zero infections.

Suddenly, security and IT leaders are faced with a dilemma: castle-and-moat networks are irrelevant, users and data are everywhere, and the attack surface continues to expand. They have realized that appliance-based/out-of-band sandbox passthrough approaches are no longer adequate. Their security outcomes are having a reverse effect. Instead of staying ahead of the attackers by maintaining a solid security posture, they are dealing with:

Reactive damage control

Appliance-based and out-of-band sandboxes are built for legacy castle-and-moat networks. Their passthrough architecture allows the first unknown and potentially malicious file to go through without deep inspection or quarantine, often resulting in patient-zero infections. As a result, security and IT leaders end up scrambling to stop the lateral movement of unknown malware, which should have been prevented in the first place. They continue to deploy additional protection inside their networks and create complex network segmentation rules on their legacy appliance-based and virtual firewalls, adding to their operational costs. To put things in perspective, in 2017, a historic attack on Maersk completely shut down an 80,000-employee company in just three hours and caused billions in damages[1].

SECURITY LEADER BENEFITS

- **True inline protection:** Detect, prevent, and quarantine unknown threats inline with advanced AI/ML to stop patient-zero attacks.
- **Complete SSL visibility:** Find unknown threats in all TLS/SSL traffic with a unique proxy-based architecture that enables unlimited, latency-free inspection.
- **Consistent protection everywhere:** Cloud-delivered protection for every user, regardless of location. Everyone gets the same protection on or off the network without cumbersome VPNs or costly MPLS links.
- **Globally shared prevention:** Get automated protection for previously unknown threats with integrated threat intelligence shared across all users in real-time.
- **Reduced TCO and complexity:** Eliminate complexity and deploy in seconds with no hardware to buy or software to manage. Cloud Sandbox is a fully integrated capability of Zscaler Internet Access™, part of the Zscaler Zero Trust Exchange™.

[1] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Never-ending administration issues

On average, an enterprise deploys 45 different security tools[2] in its network to protect against cyberattacks. Adding more appliance-based sandboxes or out-of-band solutions that rely on yet another appliance for enforcement doesn't make sense. Furthermore, it is counterproductive for security and IT leaders to deal with ongoing digital transformation projects and tackle hardware upgrades, patches, inflated policies, network segmentation, routing protocols, and never-ending support calls. In a legacy network environment, most of IT's time is spent putting out fires instead of solidifying the organization's security posture.

Lack of visibility

Eighty-four percent of global internet traffic is encrypted via SSL/TLS, quickly approaching 92 percent in the United States[3]. Adversaries see this as an opportunity and are launching stealthy attacks hidden in encrypted traffic. A recent ThreatLabZ Report showed a 500 percent increase in ransomware attacks hidden in SSL traffic and, interestingly, 30 percent of trusted cloud apps like Google Drive, AWS, and OneDrive were observed delivering malware. Network-centric sandboxes are not built to inspect SSL traffic, rendering them useless when it comes to detecting stealthy and targeted unknown attacks.

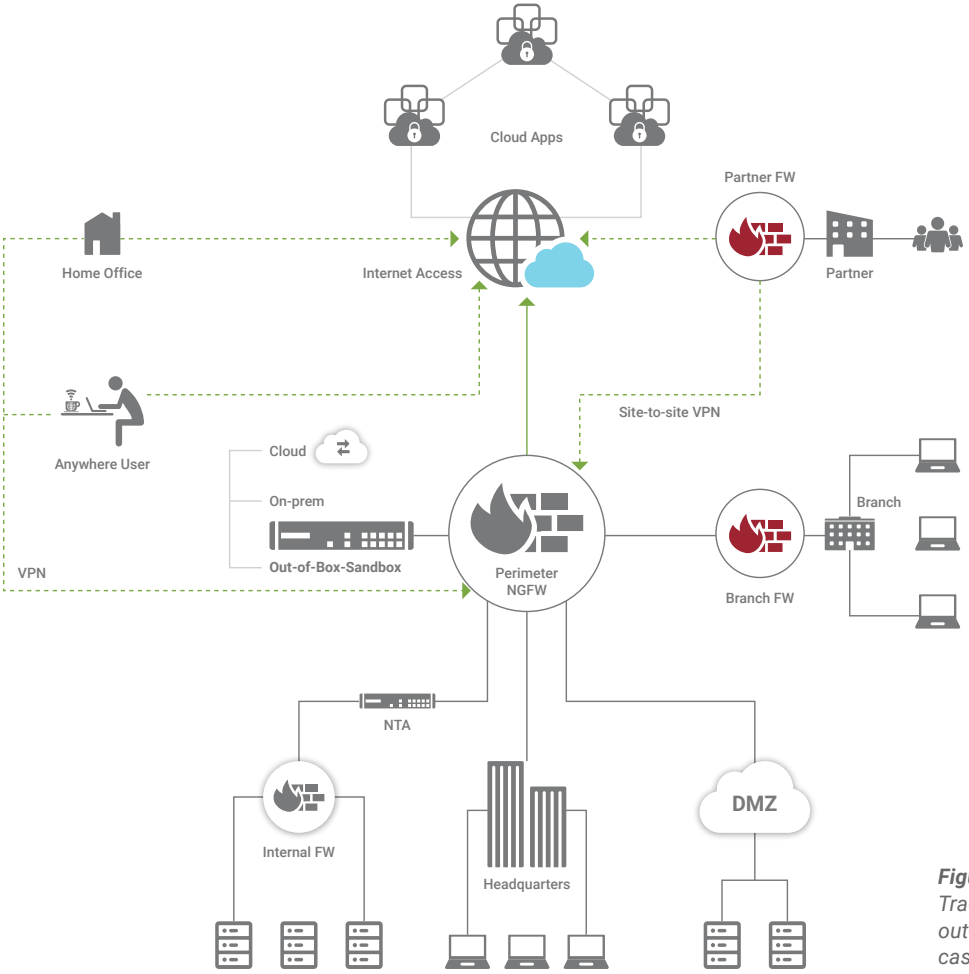

Figure 1: Legacy architecture: *Traditional appliance-based and out-of-band sandbox built for the castle-and-moat network*

[2] https://www.zdnet.com/article/the-more-cybersecurity-tools-an-enterprise-deploys-the-less-effective-their-defense-is/
[3] https://www.abetterinternet.org/documents/2020-ISRG-Annual-Report.pdf

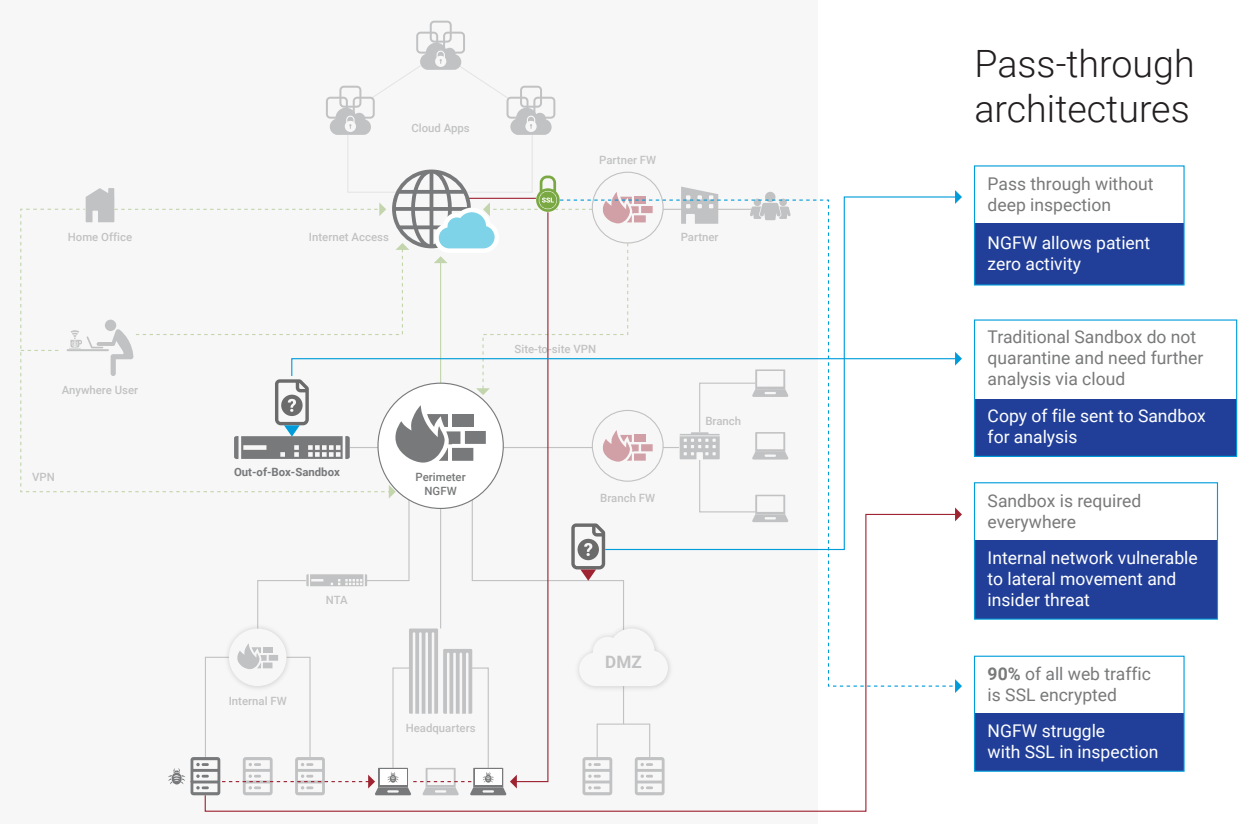

Figure 2: Patient-zero infection: *Legacy sandbox passthrough architecture lets the first potentially malicious file through*

Zscaler zero trust approach with cloud-gen sandbox

Zscaler Cloud Sandbox is built on the Zscaler Zero Trust Exchange™, a platform based on a unique, purpose-built proxy architecture. The Zero Trust Exchange uses an AI/ML-powered data analysis engine that provides true inline detection, prevention, and AI-based quarantining of unknown attacks, including threats hiding in SSL/TLS traffic.

Driven by advanced AI/ML, Cloud Sandbox stops patient-zero attacks with instant verdicts for common file types and automates quarantine of high-risk unknown threats. As an integrated service in the cloud-native Zscaler platform, protections are continuously updated from over 160 billion requests per day.

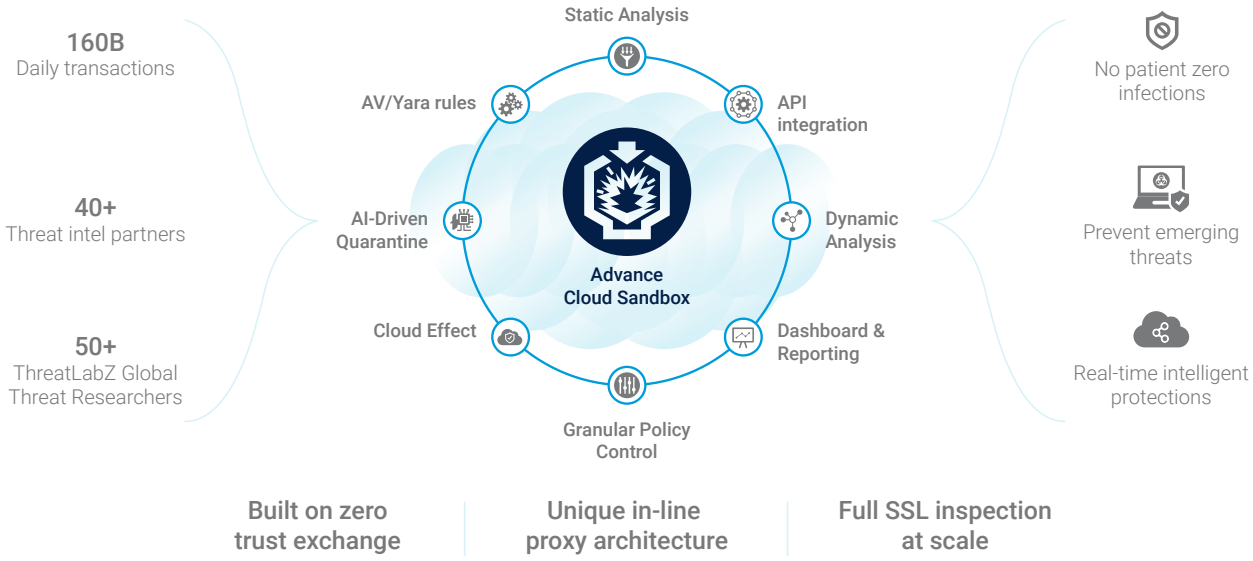

Figure 3: *Zscaler Advanced Cloud Sandbox*

Be proactive

Zscaler's inline proxy architecture enables security teams to be more proactive in stopping patient-zero threats. The cloud-native architecture allows unlimited inspection of all traffic on all ports and protocols, including SSL/TLS. Using the industry's first AI-based quarantine functionality, combined with an in-depth dynamic analysis engine, you can now proactively detect, inspect, alert, and block suspicious and potentially dangerous unknown files before they are allowed into the network. In addition, based on your desired use case, you can create and deploy granular user- and application-based sandbox policies without the need for legacy network configuration parameters.

Break-free from appliances and out-of-band sandboxes

Zscaler Cloud Sandbox is 100 percent cloud-delivered. There is no need for appliances or out-of-band sandbox analysis. Break free from continuous appliance upgrades, chasing change windows, racking and stacking appliances, dealing with routing protocols, backhauling traffic to network appliances, poor user experiences, and adding more to an already inflated policy. Zscaler provides easy sandbox configuration, making it operational in seconds.

Get unlimited SSL inspection

Zscaler's unique inline proxy architecture allows you to inspect SSL/TLS at unlimited scale and stop hidden threats. Because the majority of internet traffic and applications use SSL as a means of communication, you need a solution that can inspect and detect emerging threats hidden in encrypted traffic without compromising user experience.

Stay ahead of the attackers

Zscaler harnesses the power of the cloud by providing recommended sandbox policies that automatically update with the latest shared protections sourced by new threats uncovered by our sandbox. With over 160 billion transactions processed daily, a team of world-class threat researchers, and intel from seven billion threats blocked across the cloud, users are always protected on- or off-network.

In-depth dynamic malware analysis engine

The Zscaler Cloud Sandbox in-depth dynamic analysis engine takes full advantage of the cloud by checking hashes against a blacklist from threat feeds and other observed samples—pre-filtering samples to optimize analysis and swiftly delivering verdicts with AV, Yara, and AI/ML models. Robust static, dynamic, and secondary analysis pipelines quickly issue actionable verdicts. Post-processing continues to update the Zscaler threat database and updates policies enforced by customers even after the analysis is done.

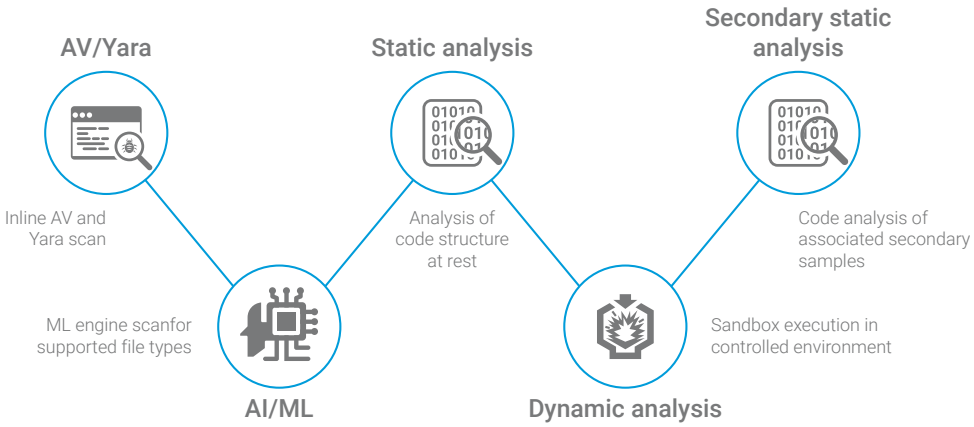

Figure 4: *Zscalers Advanced Cloud Sandbox Threat Analysis Flow*

Zscaler Cloud Sandbox key features

Easy 1-2 configuration

No need to use multiple windows to manage, nor appliances to deploy. Operationalize Zscaler Cloud Sandbox in seconds with a simple two-step configuration: Criteria and action.

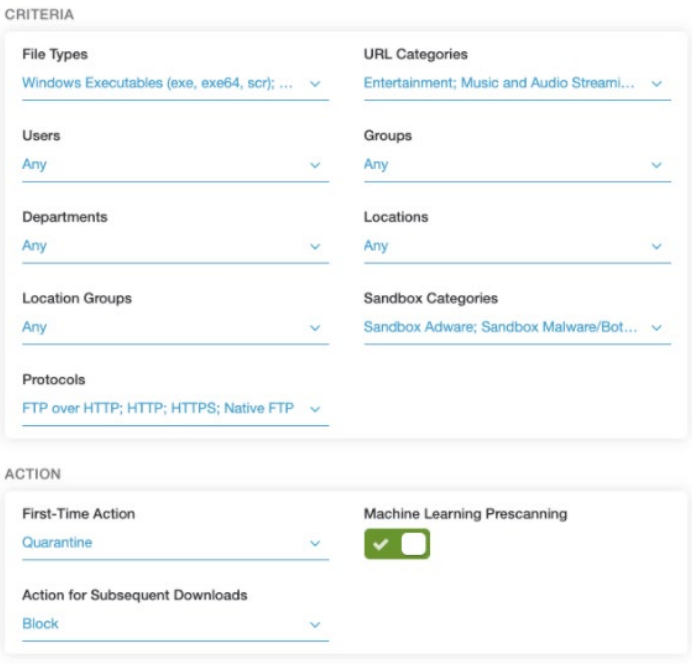

Figure 5: *Zscaler Advanced Cloud Sandbox easy policy configuration*

Granular policies

Create custom and granular policies to support various use cases, take action by holding files for AI-based quarantine, and provide access based on users, location, OS, and other parameters.

Figure 6: *Zscaler's Advanced cloud sandbox granular policy control*

AI-based quarantine

Stop patient-zero infections before they reach their target. Zscaler's proxy architecture allows you to quarantine suspicious files inline, perform real-time AI-based analysis, and issue instant verdicts without delays.

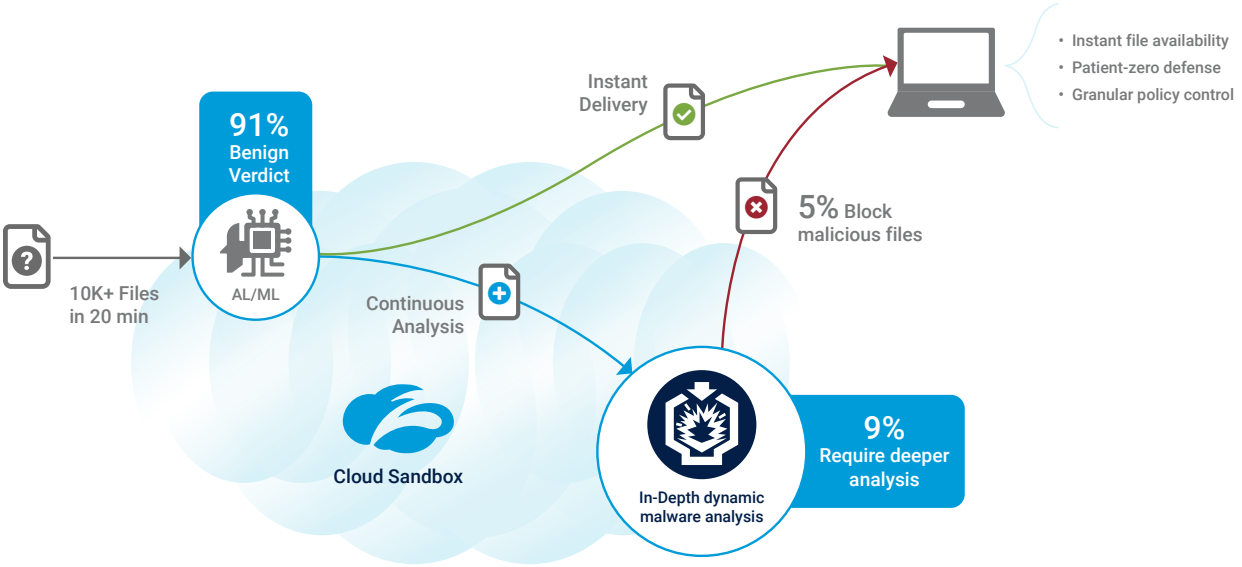

Figure 7: *Zscalers Advanced Cloud Sandbox AI-Based quarantine analysis workflow*

AI in action: Within twenty minutes of deployment, one customer that was leveraging Zscaler Cloud Sandbox saw 91 percent of unknown files get an instant AI-based benign verdict before being quickly delivered to users. The remaining nine percent of files underwent dynamic, in-depth analysis to reveal that five percent of the files were malicious. These dangerous files were instantly blocked for all Zscaler global users, thanks to the cloud effect.

Detailed reporting

In-depth reporting for issued verdicts allows security operations teams to accelerate threat hunting and investigations, enabling security leaders to strengthen security quickly.

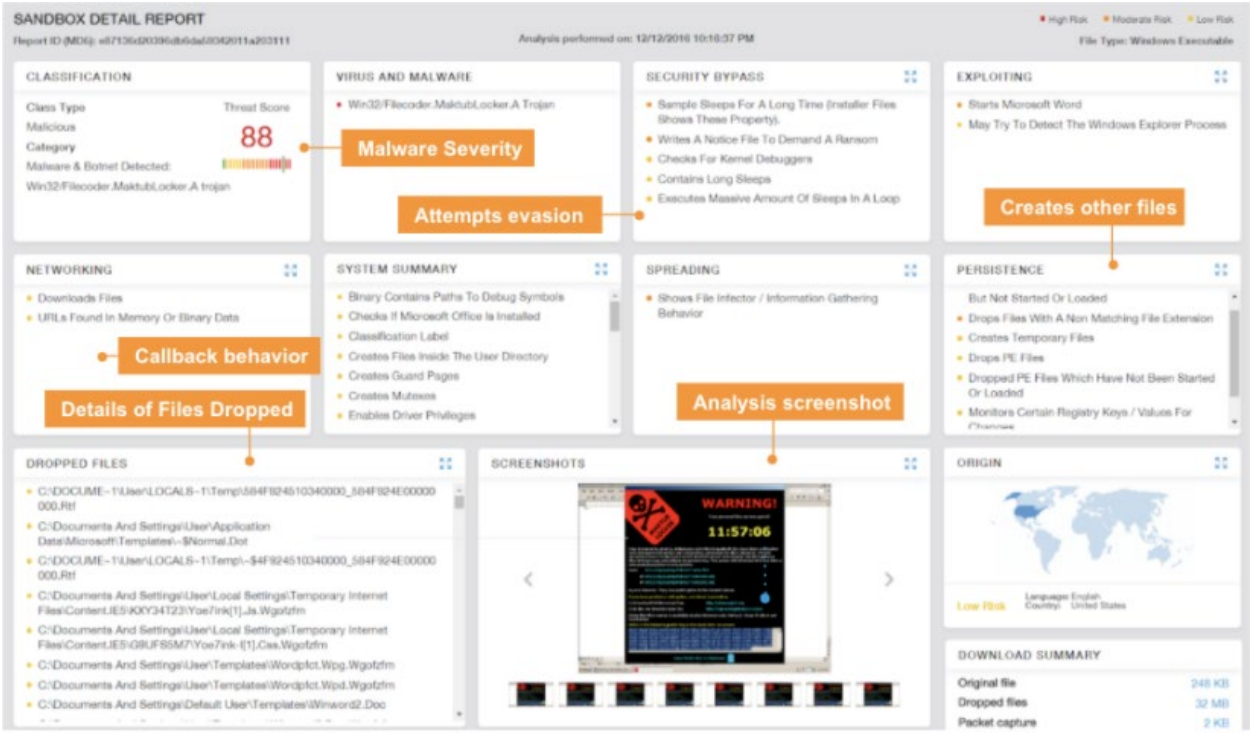

Figure 8: *Zscaler's Advanced Cloud Sandbox detailed forensic report*

Cloud Sandbox features

Features	Details
Analysis engine	Prefiltering: AV, Yara, ML/AI; Analysis: static analysis, dynamic analysis; Post Analysis: code analysis, secondary payload analysis
File support	.exe, .dll, .scr, .ocx, .sys, .class, .jar, .pdf, .swf, Office documents, .apk, .zip, .rar, .7z, .bz, .bz2, .tar, .tgz, .gtar, .rtf, .ps1, .hta, .vba, script files in zips
SSL inspection	Unlimited SSL/TLS inspection
OS support	Windows XP, Windows 10, and Android
Protocol support	HTTP, HTTPS, FTP, FTP over HTTP
Files per day	Unlimited
Deployment model	Cloud-native
Threat intel integration	40+ security partner threat intel feeds
Management and reporting	Centralized web UI
Forensics	Initial sample, secondary payloads, PCAPs
API support	Robust API support
Granular policies	Users, location, location groups, file types, user groups, departments, URL categories, protocols

Prerequisites:

- Need to have Advanced Threat Protection (ATP) and SSL decryption license

Zscaler licensing model:

- ZIA Professional Edition: includes Standard Cloud Sandbox
- ZIA Business Edition: includes Standard Cloud Sandbox, Advanced Threat Protection (ATP), and SSL decryption
- ZIA Transformation Edition: includes Advanced Cloud Sandbox, Advanced Threat Protection (ATP), and SSL decryption

Zscaler Cloud Sandbox as an add-on module

- ZIA-Sandbox: requires Business or Professional Edition license

	Standard Cloud Sandbox	Advanced Cloud Sandbox
File support	.exe, .dll	.exe, .dll, .scr, .ocx, .sys, .class, .jar, .pdf, .swf, Office Zscdocuments,.doc(x), .xls(x), .ppt(x), .apk, .zip, .rar, .7z, .bz, .bz2, .tar, .tgz, .gtar, .rtf, .ps1, .hta, .vba, script files in zips
AI-based quarantine	✗	✓
Granular policies	✗	✓
Reporting	✗	✓
API	✗	✓

Get more details about our advanced cloud sandbox by visiting **https://www.zscaler.com/products/sandboxing**

Take our advanced cloud sandbox for a virtual test drive by registering for **"Zscalers Hands-on workshop"**

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com