EBOOK

The Threat Prevention Buyer's Guide

FInd the best AI-driven threat protection solution to stop file-based attacks.

Contents

Rethinking security for today's threat landscape

Perimeter-only security is too risky for today's digital world

The shift to hybrid work and cloud-hosted applications has changed how business resources are accessed. Employees are using unmanaged devices over unsecured networks like public Wi-Fi to remain productive remotely or on the go, effectively making the internet the new corporate network. This expansion of access points renders the old castle-and-moat approach to security inadequate for protecting your users, applications, and data. Relying solely on perimeter defenses introduces risks as network-centric controls are bypassed for direct-to-internet access, often prioritizing ease-of-use over security.

The new generation of cyberattacks easily evade legacy security controls. It's time to put security closer to users and shift from protecting the perimeter to securing users, workloads, and OT/IoT.

Adversaries are taking advantage of the cloud rush

Stuck between a rock and a hard place, security teams have done their best to shoehorn legacy security controls for today's mobile- and cloud-first world. The mismatch has been a win for adversaries. As organizations struggle to protect multiple network edges, doors are inadvertently being left open to malware, as evidenced from Zscaler ThreatLabz findings:

- **86%** of threats are delivered over encrypted channels, with malware accounting for 78% of encrypted attacks.[1]
- Ransomware attacks increased by **40%** year-over-year.[2]
- Payloads observed in the Zscaler Sandbox jumped **58%**.[2]

This rapid evolution of digital threats, compounded by the expanding cloud attack surface, only emphasizes the need for security teams to reassess their strategies and bolster defenses against modern cyber risks.

1. Zscaler ThreatLabz 2023 State of Encrypted Attacks Report
2. Zscaler ThreatLabz 2023 Ransomware Report

An evolution to zero-day malware protection is needed

Adversaries have two key advantages: **speed** and **proliferation**. Malware developers are creating threats faster than defenders can define them, leveraging artificial intelligence (AI) to create variants capable of evading conventional security measures and detection methods.

Phishing with malicious attachments or links remains one of the most common delivery mechanisms today. The pervasive use of encrypted traffic further complicates defense strategies. Modern threats often hide in encrypted traffic, underscoring the importance of inspecting all web and non-web traffic — or you may unknowingly let malware into your network.

As a critical function in the security stack, sandboxes are a preventative measure against malicious files and code executions. They are meant to be an effective defense against unknown file-based attacks that aim to evade EDR and other scans for known malware. Unfortunately, many sandboxes are deployed out-of-band, relying on malware samples to be forwarded to them from NGFWs, cloud security products, or endpoint agents.

This often means detection occurs after the malware has been downloaded onto a user device, allowing patient zero malware or ransomware infections — and certainly not abiding by zero trust concepts. Additionally, many sandboxes do not leverage large-scale AI/ML analysis to automatically detect and quarantine unknown threats and suspicious files — a key factor in delivering inline patient zero defense without disrupting productivity.

Signature-based antivirus and intrusion prevention systems (IPS) alone cannot prevent zero day and polymorphic threats.

Cloud sandboxing requirements

Up until now, adversaries have had the upper hand by exploiting the shifting architecture in the cloud environment.

Choosing the right cloud sandbox is essential to preventing patient zero infections and blocking advanced persistent threats from gaining access to your network.

The following section is intended to help you understand the specific requirements you should consider when selecting a cloud sandbox.

Decryption and inspection at scale

Encryption has become a promising security trend, enabling private communication and sensitive information to be protected and secured. Unfortunately, cybercriminals are taking advantage of encrypted traffic to hide malicious payloads.

Decrypting and inspecting traffic is a compute-intensive process, and can turn high-performing sandbox appliances into sluggish doorstops, interrupting business with unacceptable latency.

When evaluating a modern sandboxing solution, it's important to identify vendors that can provide unlimited, latency-free decryption and inspection inline.

Threats over HTTPS grew by 24.3% year-over-year, representing 30 billion encrypted attacks in 2023.[3]

Purchasing checklist:

- ☐ Requires no additional hardware or virtual machine (VM) installation to decrypt SSL traffic
- ☐ Inspects and analyzes the following file types without latency or capacity limits:

EXE	DOC(X)	TAR
DLL	XLS(X)	TGZ
SCR	PPT(X)	GTAR
OCX	APK	RTF
SYS	ZIP	PS1
CLASS	RAR	HTA
JAR	7Z	VBS
PDF	BZ	script files in ZIP files
SWF	BZ2	

3. Zscaler ThreatLabz 2023 State of Encrypted Attacks Report

Purchasing checklist:

- ☐ Immediate enforcement of policies across all users with identical protection, whether on or off the corporate network
- ☐ Advanced quarantine rules and capabilities for all files from suspicious destinations
- ☐ Centralized policy management that enables granular control over sandboxing operations, including file type allowances and automated holds from suspicious destinations

Centralized policy management and rules

Avoid mismanaging rules and manually configuring sandboxes at each gateway with cloud-delivered, centralized policy management and rules. Consider solutions with adaptive and dynamic policies that follow zero trust tenets outlined by **NIST 800-207**. By establishing access and security policies based on context — including the user's role and location, device posture, and the data requested — zero trust minimizes attack surfaces. Solutions that are cloud-delivered have additional benefits that may allow you to block threats across all users in the organization. Doing so means no more file retrospectives (examples: out-of-band inspections and applied protections after the fact) for security that is more in sync. A critical aspect of sandbox policy is that it offers the flexibility to support the business, with granular rules for different sets of users, locations, URL categories, or actions. Granular controls allow you to align policies with your organization's risk tolerance and performance expectations.

Aligning policies with risk tolerance and performance expectations

A cloud sandbox solution should control risks and enforce policies that conform to your organization's unique needs. Start by determining whether you have:

- **Low tolerance for malicious files:** For risk-avoidant organizations, you can choose Quarantine for First-Time Action for unknown or suspicious files that will ensure there are no patient zero infections because the sandbox will analyze the file before it can be downloaded.
- **Low tolerance for quarantining files:** For risk-tolerant organizations that want to avoid delays and interruptions, you can choose Quarantine and Isolate for First-Time Action. This action integrates the sandbox with cloud browser isolation capabilities, providing users with immediate access to a read-only PDF with no active content while the sandbox analyzes potentially harmful files in the background.

Regardless of your specific needs, policies should be easy to apply to all users, groups, departments, locations, and location groups from a single platform.

Intelligent analysis and threat intel

Adversaries are known to reuse successful attacks, so it's essential to share protections with the security community to quickly stop threats in their tracks. Cloud sandboxes play an important role in this by capturing telemetry data and sharing insights from newly identified threats with threat feeds and the security community.

AI-driven malware prevention engine

Cloud-delivered sandboxes are able to manage compute-heavy AI/ML models to drive superior protection.

Look for a sandbox that intelligently identifies, quarantines, and prevents unknown or suspicious threats inline using advanced AI/ML without requiring further analysis:

- **Instant file verdicts:** By instantly understanding which files are very likely malicious, users are not kept waiting for a verdict.
- **Zero-day prevention:** While hard to believe, not every sandbox prevents patient zero infections by quarantining unknown threats before allowing them to be downloaded.

SOC workflows with threat intelligence

Analysts can spend many hours a day researching a single threat. Look for a cloud sandbox that reduces this burden and accelerates investigation and response by sharing behavioral insights and threat intelligence on malicious payloads. Security teams should be able to support investigations with direct file analysis in the sandbox via out-of-band API submissions. Be sure that threat feeds integrate with your existing security tools. They should include: updated context on reported URLs, extracted indicators of compromise (IoCs), and tactics, techniques and procedures (TTPs) that align to cybersecurity frameworks such as MITRE ATT&CK®.

Purchasing checklist:

- ☐ AI-based quarantine capabilities that can leverage AI/ML to deliver an instant verdict on files to stop threats without requiring file analysis
- ☐ Autonomous contribution to daily threat protections shared across users and networks regardless of location
- ☐ Threat feed integration with existing security tools
- ☐ Programmatic, API-driven "out-of-band" sandbox file submissions with separate queue for API-submitted files

Be sure to choose a sandbox that can provide more than a threat score. Consider a sandbox that can outline evasive techniques used, such as:

- Delaying code execution to avoid sandbox detection
- Capturing and viewing traffic as it's passed along the network
- Opening ports to allow remote connectivity
- Attempting lateral movement to find higher value targets
- Trying to allow remote control

Reporting

Security solutions with reporting are only as useful as they are actionable. Cloud sandbox reporting should be:

- Inclusive of the entire malicious attack lifecycle
- Simple to use and easy to navigate
- Easy to digest
- Available via an application programming interface (API) so it can be correlated with existing logs
- Part of a larger platform that also supports compliance reporting

Improving your SOC with the MITRE ATT&CK framework

When evaluating reporting capabilities, consider sandbox intelligence that can be mapped to the **MITRE ATT&CK framework**. With this capability, SOC teams can apply the insights provided to building tactical defenses in other parts of the security stack. In this way, the sandbox is an integral part of security operations workflows.

Depending on your maturity with the framework, you can use the reporting in multiple ways:

- Reduce the burden of labeling by using provided taxonomy
- View stealth techniques that may be evading your endpoint detection and response (EDR) solution
- Compare and contrast other controls
- Focus on the most common TTPs targeting your organization instead of aimlessly preventing all tactics and techniques
- Perform a reverse engineering report

Questions to ask before you buy

To help guide your decision-making process, here's a roundup of the key questions to ask and why you should ask them:

Does the sandbox allow initial patient zero infections — even just one?

Sandboxes that allow an initial patient zero infection while a file is being analyzed are failing at keeping the organization safe.

Does the solution cover all users and their devices, regardless of location?

Your users may be accessing corporate resources on the go, on their own devices, or over unsecured networks. It is critical to secure all devices that are essential to their jobs.[4]

Does the solution detect inline or require out-of-band file submissions?

Solutions that work inline can identify threats and block them directly without having to rely on NGFW network flows or implicate endpoint EDR software.

Does the sandbox examine traffic across all HTTP, HTTPS, FTP, and FTP over HTTP protocols? Are there limitations?

It's important to examine traffic to unveil stealthy malware. A cloud-delivered sandbox may be better for inspecting all traffic without latency.

Does it comply with relevant laws and regulations, including zero trust requirements?

Compliance regulations may have strict requirements on how sandboxing is handled and on file retention/privacy matters. Finding a solution that operates only in memory and strips identifiable information during analysis helps you meet these requirements. Additionally, consider if solutions adhere to the tenets of zero trust as laid out by NIST 800-207 global standards and use them as guidance for reducing attack surfaces and protecting data.

What other security modules does the sandbox work with?

No single product can protect entirely against advanced persistent threats (APTs). Instead, a multilayered approach of threat prevention, mitigation, detection, and response is required. Sandboxing is one integral layer, and, as such, it must work well with other solutions and modules.

4. us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing_Mobile_Value_2022-Final.pdf

Zscaler Cloud Sandbox and Advanced Threat Protection

It's time for a true inline cloud-native sandbox

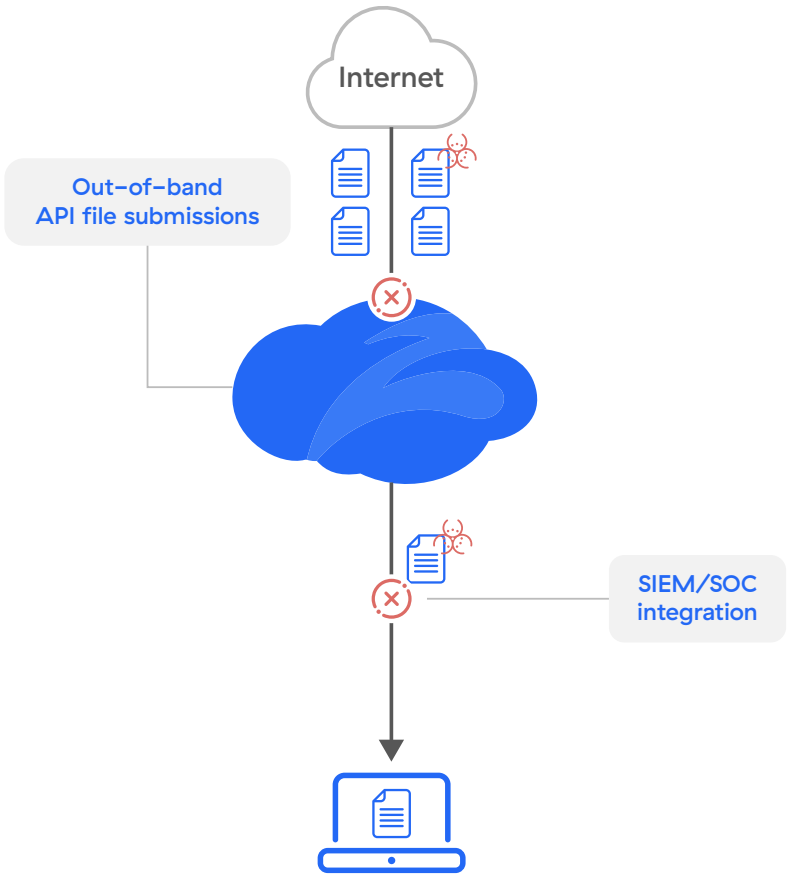
As organizations grapple with expanded attack surfaces and adversaries take advantage of legacy security stack gaps, there's never been a better time to choose a true in-line cloud-native sandbox. Zscaler Cloud Sandbox is purpose-built to catch and stop modern threats while ensuring zero-day malware protection for all users, in all locations.

Built on a cloud-native, proxy-based architecture, Zscaler Cloud Sandbox is the world's first AI-driven malware prevention engine that automatically detects, prevents, and intelligently quarantines unknown threats and suspicious files inline. The unlimited, latency-free inspection across web and file transfer protocols (FTP), including SSL/TLS, allows the cloud sandbox to perform in-depth, real-time dynamic analysis, ensuring no unknown file reaches the user as a malicious file download.

Zscaler Sandbox AI advantage: Trained with more than 500 million samples, with real-time security updates sourced from 300 trillion daily signals.

AI-driven quarantine stops never-before-seen malware

Inline protection with instant benign file delivery, patient-zero defense, and granular policy controls



Reduced complexity and cost

- Easy to deploy, no hardware or software to manage
- Remove redundant and disjointed point products
- Eliminate backhauling internet traffic over MPLS or VPN

Immediate, adaptive protection for all users and locations

- Define global policies in a single, centralized console
- Enforce policy changes immediately
- Identify threats once and block immediately for all customers

Uncover hidden threats

- Stop patient zero infections from known and emerging threats with AI-driven quarantine
- Upload files for analysis (file check portal)

Integrated platform service

- Pre-filtering of all known bad threats using antivirus, hash blocklists, YARA malware classification rules, automated JA3 fingerprinting detections, and ML/AI models
- Collective Intelligence Framework (CIF) feeds allow Zscaler to integrate with more than 60 threat feeds in addition to Zscaler's own thread feed, powered by billions of transactions across its customer base
- Layer a cloud sandbox with an EDR solution to increase security efficacy and mitigate against initial access, execution, and persistent tactics

An ESG Economic Validation study found that Zscaler Zero Trust Exchange created a 90% reduction in security appliances.[5]

- Static, dynamic, and secondary analysis, including code analysis and secondary payload analysis
- Unlimited, latency-free SSL inspection
- Protection for inbound and outbound traffic
- Enhance security investigation and response with API file submissions rich forensics, including user, location origin, evasive tactics, and more

Zscaler Cloud Sandbox™ is a fully integrated capability of Zscaler Internet Access™ and part of the Zscaler Zero Trust Exchange™.

For more information, visit
zscaler.com/technology/cloud-sandbox

5. info.zscaler.com/resources-industry-report-esg-economic-validation

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. To learn more, visit **www.zscaler.com**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com