



# The CISO's Threat Prevention Guide

Find the best advanced and file-based threat protection solution for you.

EBook



# Contents

<b>Rethinking security for today's threat landscape</b>	<b>3</b>
Perimeter-only security is too risky for the digital world	3
Adversaries are taking advantage of the cloud rush	3
<b>An evolution to zero-day malware protection is needed</b>	<b>4</b>
<b>Cloud sandbox requirements</b>	<b>5</b>
Decryption inspection at scale	6
Centralized policy management and rules	7
Aligning policies with risk tolerance and performance expectations	7
Intelligent analysis and threat intel	8
AI-driven malware prevention engine	8
SOC workflows with threat intelligence	8
Improving your SOC with the MITRE ATT&CK Framework	9
Questions to ask before you buy	10
<b>Zscaler Cloud Sandbox and Advanced Threat Protection</b>	<b>11</b>
It's time for a true inline cloud-native sandbox	11

# 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 have changed how business resources are accessed. Users are using unmanaged devices over unsecured networks like public Wi-Fi to remain productive remotely or on the go, making the internet the new corporate network. This expands your one perimeter to thousands, making the castle-and-moat approach to security inadequate for protecting your users, applications, and data. Continuing to rely solely on perimeter-based controls introduces risks because network-centric defenses are bypassed for direct to internet access and ease-of-use.

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:

- Ransomware attacks have **increased by 80%** year over year.<sup>1</sup>
- Multifaceted extortion techniques are on the rise, and double extortion ransomware has increased by **117%**.<sup>1</sup>
- Phishing attacks **rose 29%** in 2021 compared to 2020.<sup>2</sup>
- **85%** of organizations experienced a successful cyberattack in 2021.<sup>3</sup>
- **63%** of ransomware victims paid ransoms in 2021, encouraging cybercriminals to scale up their attacks.<sup>3</sup>

1. <https://www.zscaler.com/resources/industry-reports/2022-threatlabz-ransomware-report.pdf>

2. <https://www.zscaler.com/resources/industry-reports/2022-threatlabz-phishing-report.pdf>

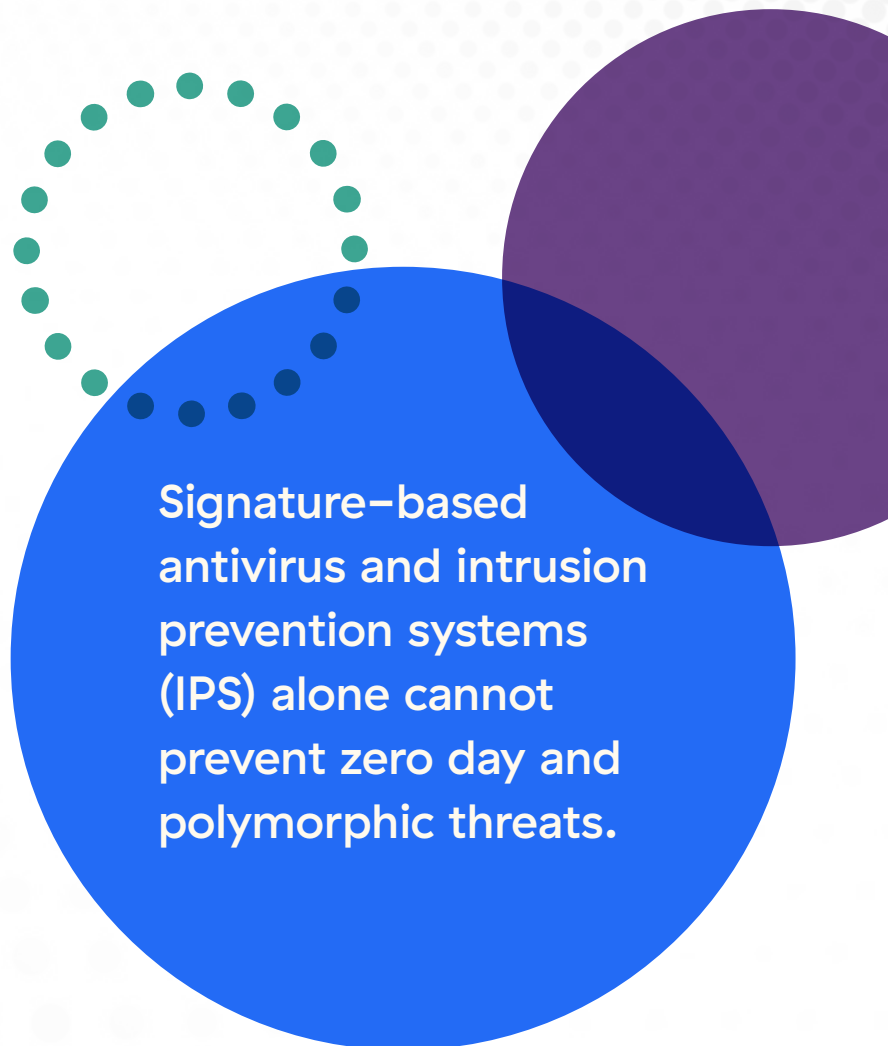
3. <https://cyber-edge.com/cyberthreat-defense-report-2022/>

# An evolution to zero-day malware protection is needed

Adversaries have two advantages: **speed** and **proliferation**. Malware developers are creating threats faster than defenders can define them, spreading and shapeshifting to evade detection.

Phishing with malicious attachments or links remains the most common delivery mechanism today. Since threats hide in encrypted traffic, if you are not inspecting all web and non-web traffic, including file transfer protocols and SSL/TLS, you may unknowingly let malware into your network and allow adversaries to exfiltrate sensitive data or demand ransom.

As a critical function in the security stack, sandboxes are a preventative measures against malicious files and code executions. They are meant to be the last line of defense and the first point of detection for investigations against unknown threats. Unfortunately, legacy sandbox appliances are out-of-band and require add-on devices for SSL decryption and inspection. Since protection is applied once the malware has already passed through to the user or device, zero trust cannot be achieved.



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.

As a newer practice, decrypting and inspecting traffic is a compute-intensive process. Legacy sandboxes with passthrough

architecture unintentionally allow malware to sneak in among uninspected traffic. Dedicated, bolted-on SSL inspection devices can help, but like all appliances, they lack the ability to scale, causing costly device sprawl while patient zero infections continue to permeate networks.

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 have increased more than 314% year-over-year, exceeding 250% growth for the second straight year.<sup>4</sup>

4. <https://info.zscaler.com/resources-whitepaper-threatlabz-the-state-of-encrypted-attacks>

## 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	XLX(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	



### 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
- Granular controls for greyware and adware files

### 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 once a threat has been identified. 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.

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.
- **Low tolerance for quarantining files:** For risk tolerant organizations that want to avoid delays and interruptions, you can choose Allow and Scan for First-Time Action. For additional protection, consider integrating with cloud browser isolation capabilities to render the file as an image and avoid data leakage and delivery of active threats.

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 rescanning benign files.

This ensures:

- **Faster file verdicts:** By routing benign files immediately and analyzing suspicious or unknown files, you can benefit from less hands-on work.
- **Zero-day prevention:** By quarantining unknown threats without additional work, you can stop zero-days from becoming a larger threat to your environment.

## 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 accelerate investigation and response by sharing behavioral insights and threat intelligence on malicious payloads. 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:

- ML/AI capabilities that tightly integrate with the analysis process
- AI-based quarantine capabilities that can leverage ML/AI to hold potentially malicious files, analyze them, and issue rapid verdicts at machine speed
- Autonomous contribution to daily threat protections shared across users and networks regardless of location
- Ability to share forensic data and file verdicts through a platform
- Threat feed integration with existing security tools



**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 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.<sup>5</sup>

### ❖ Does the solution work inline or in test access point (TAP) mode?

Solutions that work inline can identify threats and block them directly without having to create new rules through third-party devices such as firewalls.

### ❖ 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.

### ❖ Does the solution complement vendor-provided sandboxes or EDR sandboxing?

A true defense-in-depth strategy may need complementary solutions and layered protection to adequately disrupt the malware kill chain that could devastate your organization. If one level in your ecosystem fails, you can count on another. Endpoint, network, and policy control should work harmoniously together to stop adversaries.

---

5. [https://image-us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing\\_Mobile\\_Value\\_2022-Final.pdf](https://image-us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing_Mobile_Value_2022-Final.pdf)



# Zscaler Cloud Sandbox and Advanced Threat Protection

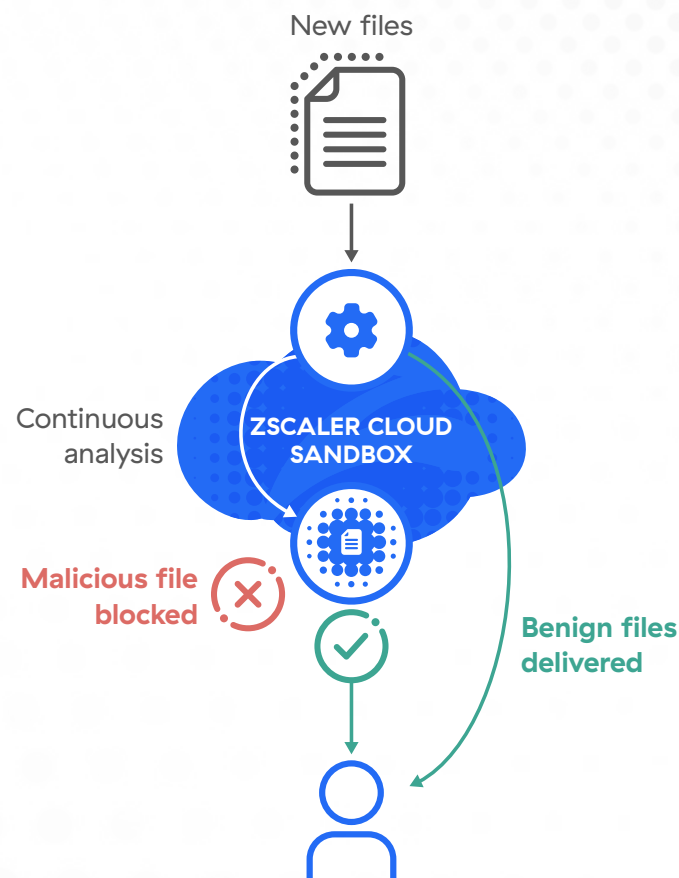
## It's time for a true inline cloud-native sandbox

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.

## 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 allows Zscaler to integrate with more than 60+ threat feeds, in addition to the Zscaler own threat 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.<sup>6</sup>

- 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 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/custom-product-demo](https://zscaler.com/custom-product-demo).

6. <https://info.zscaler.com/resources/industry-report-esg-economic-validation>





| Experience your world, secured.™

#### 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](https://www.zscaler.com) or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

© 2022 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at [zscaler.com/legal/trademarks](https://www.zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.