DATA SHEET

Zscaler™ Advanced Persistent Threat Protection

Zscaler delivers defense-in-depth against APTs.

Hackers are coming after your people, systems, and data with tailored Advanced Persistent Threat attacks designed to exploit your vulnerabilities and bypass your existing security. Zscaler provides full lifecycle APT protection that goes far beyond simple "signatureless" detection, with a comprehensive defense-in-depth approach. Because it's delivered on top of the Zscaler Cloud Security Platform, enterprises can protect against APTs at all locations, and for all users and devices, with an easy and cost-effective solution.

KEY BENEFITS

Stops advanced cyberattacks

- Stops sophisticated threats, including zero-day attacks, with a multi-layered defense framework that features advanced sandboxing and forensics capabilities.
- Doesn't just send alerts—automatically blocks identified zero-day attacks as well as inbound malware, outbound botnet communications from infected devices, and outbound data exfiltration.
- Leverages over 25 billion transactions a day to deliver the most comprehensive threat analysis, the highest catch rates, the lowest false positives, and the fastest time to block threats across all 15+ million Zscaler users.

Protects headquarters, branches, and road warriors

- Closes critical gaps in protecting remote offices, mobile workers, devices, and Internet-connected things, typically the most vulnerable parts of your infrastructure targeted by APT attackers.
- Sits inline with your Internet traffic—including SSL traffic—bidirectionally inspecting every byte for all of your users.

Improves your security posture while lowering costs

- Delivers multi-layered security from the cloud, consolidating a broad set of security solutions into a single integrated Security as a Service platform.
- Saves money by improving administrator productivity, reducing CAPEX and OPEX, improving network performance, and reducing security event expenditures.
- Eliminates complexity and security gaps associated with the traditional appliance-based approach to enterprise security, involving stacking security appliances at each of your Internet gateways.

FEATURES

High-speed bidirectional inline inspection

Leveraging a purpose-built architecture capable of high-speed bidirectional content inspection, Zscaler scans all Internet traffic in real time, automatically blocking threats when they are identified.

Integrated SSL traffic inspection

Zscaler, as a 100% cloud service, seamlessly integrates SSL traffic inspection into its bidirectional inline scanning without any deterioration in performance or requiring any additional hardware or software.

Behavioral analysis with automatic blocking

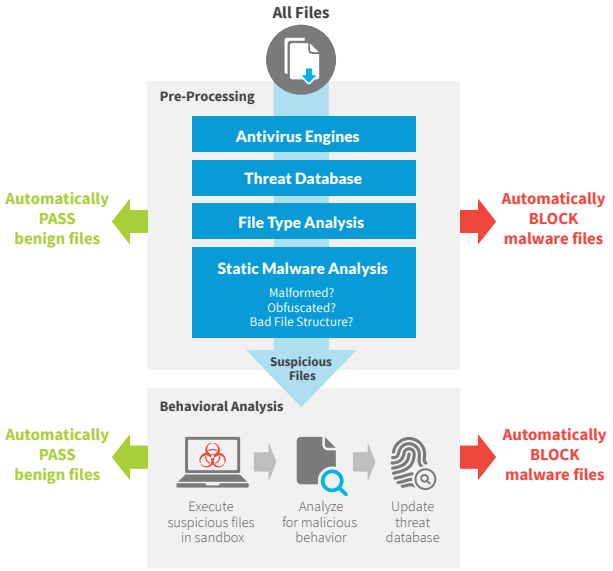
Suspicious objects are automatically executed and monitored in a controlled sandbox and any malicious behaviors, including zero-day malware, are recorded, analyzed, and blocked across all 15+ million Zscaler users.

High-performance protection against malware and malicious URLs

Zscaler identifies requests to known malicious URLs and inspects and protects against known viruses and worms using multiple signature and heuristic technologies. Our cloud architecture provides high-speed full protection without introducing material latency.

Data exfiltration and unauthorized communications defense

Zscaler automatically blocks all Internet-bound traffic (including SSL) containing unauthorized content, and locks down unauthorized ports, protocols, and cloud applications to make sure attackers can't use these channels for communications or data exfiltration. Inline scanning identifies and automatically blocks communications by infected machines, including botnet command and control ("C&C") servers.



Browser control

To avoid exposing known vulnerabilities to potential attackers, Zscaler browser control enforces policies that limit Internet access to specific browser versions, patch levels, allowed plug-ins, and applications.

BEHAVIORAL ANALYSIS	STANDARD	ADVANCED
What gets sent to the Zscaler cloud-based sandboxes	Files that remain suspicious after being processed by multiple layers of Zscaler security are automatically sent to the sandboxes	Same
What file types are sent to the Zscaler cloud-based sandboxes	• Windows 32-bit and 64-bit executable files • Windows 32-bit and 64-bit dynamic link libraries, system files, ActiveX controls, and screen savers	• Windows 32-bit and 64-bit executable file • Windows 32-bit and 64-bit dynamic link libraries, system files, ActiveX controls, and screen savers • Microsoft Office documents • Adobe PDF files • Adobe Flash files • Java apps and applets • ZIP and RAR archives with up to five levels of compression • Android APK files
What types of traffic are protected	Files originating from suspicious Internet locations	Files originating from all Internet locations
Cloud Effect: What happens when you encounter files already identified as malicious on behalf of other Zscaler clients	• Malicious Windows 32-bit and 64-bit DLLs and EXEs are instantly blocked • Other malicious files are passed but flagged	All malicious files can be instantly blocked, quarantined, or flagged based on policy
Quarantine capability and quarantine policy	• No quarantine capability • No quarantine policy	• Full quarantine capability—protect event patient zero • Granular quarantine policy—by file type, location, user, etc.
Access to portal where you can submit suspicious files to Zscaler cloud-based sandboxes for inspection	No	Yes
Logging, reporting, and analytics	Comprehensive	Same
Forensic reporting and analysis	None	Detailed—full information on all malicious files detected by our cloud sandboxes that were encountered by your organization

About Zscaler

Zscaler is revolutionizing Internet security with the industry's first Security as a Service platform. As the most innovative firm in the $35 billion security market, Zscaler is used by more than 5,000 leading organizations, including 50 of the Fortune 500. Zscaler ensures that more than 15 million users worldwide are protected against cyberattacks and data breaches, while staying fully compliant with corporate and regulatory policies.

Zscaler is a Gartner Magic Quadrant leader for Secure Web Gateways and delivers a safe and productive Internet experience for every user, from any device and from any location—100% in the cloud. With its multi-tenant, distributed cloud security platform, Zscaler effectively moves 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. Zscaler delivers unified, carrier-grade Internet security, next-generation firewall, web security, sandboxing/advanced persistent threat (APT) protection, data loss prevention, SSL inspection, traffic shaping, policy management, and threat intelligence—all without the need for on-premises hardware, appliances, or software. To learn more, visit us at **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