Full Protection from a Range of Known and Unknown Threats

Security threats have evolved from desktop-based viruses to email-based worms, and now are largely becoming browser-based threats. Zscaler inspects all inbound and outbound web traffic to protect enterprises from the following threats.

Threats

Viruses

Zscaler's solution protects against known viruses and worms using signature and heuristic technologies. Existing anti-virus products are designed to look for viruses at the desktop and within email messages. Zscaler is the only solution specially designed to look for viruses within HTTP (web) transactions. Zscaler's architecture provides inspection at 40 times the speed of traditional products, ensuring full protection without introducing any notable latency.

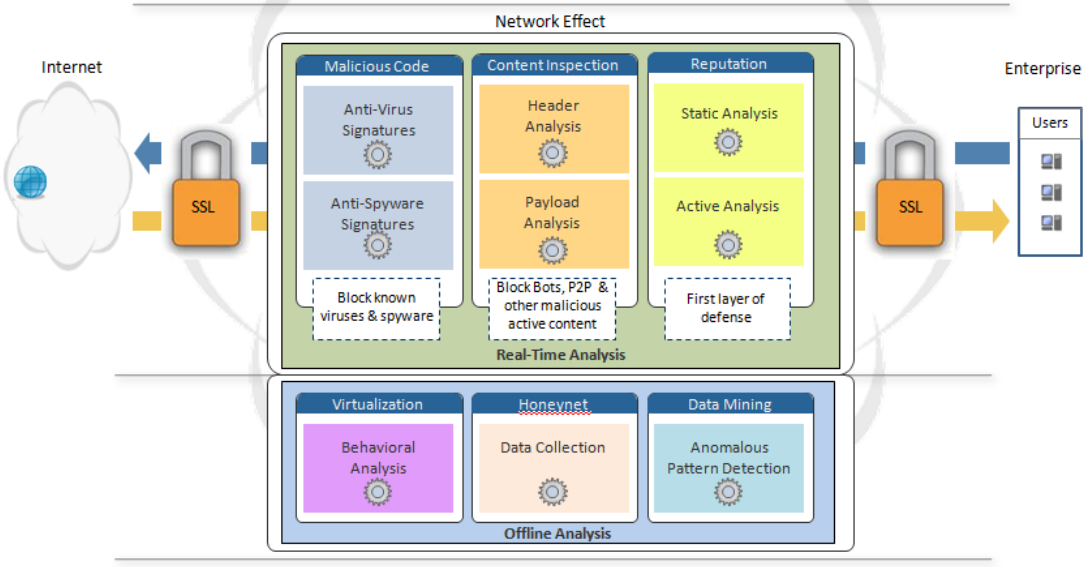
Spyware

Spyware is a pervasive and significant security risk. Zscaler anti-spyware technology detects and stops a wide range of spyware, including Trojans, backdoor proxies, keyloggers, and adware.

Bots, Peer-to-Peer, Malicious Content, Phishing

Zscaler inspects outgoing web traffic for threats such as botnets, which use end users' computers to send spam or phishing attacks. Our solutionalso prevents users from visiting fraudulent sites and disclosing sensitive personal information. Zscaler protects users from malicious content in today's Web 2.0 applications. For example, active content, such as ActiveX, Ajax, Flash, or JavaScript, can easily be used to transport malicious code. Additionally, Zscaler can also detect and block peer-to-peer applications (P2P), which can consume internet bandwidth and create security as well as liability risks for your organization.

"Zscaler's architecture provides inspection at 40 times the speed of most competitive products."



Zscaler Technology

Single-Scan, Multiple-Action Technology

Zscaler uses a number of technologies and correlates the results to ensure accurate detection of threats while minimizing false positives. To minimize the latency introduced, Zscaler performs a single scan, with multiple actions, (SSMATM) on each web request.

Application Analysis

Signature-based technology is used for the detection of known virus and spyware. Application analysis includes header and payload analysis to detect and block bots, peer-to-peer applications, and other malicious content. The reputation of domains and IP addresses, correlated with dynamically computed page reputation, allows Zscaler to protect against new, unknown threats.

Decrypting SSL Traffic

Web traffic is increasingly being encrypted using SSL. Zscaler can decrypt SSL traffic by using man-in-the-middle technology to detect and block hidden malicious content.

Zscaler Benefits

Full Protection Against Inbound and Outbound Threats

The Zscaler cloud isthe first line of defense against known and zero-day threats—blocking them before they even reach your network. Using a wide range of technologies, we ensure accurate detection against inbound and outbound threats. Zscaler is able to leverage the network effect because of its in-the-cloud architecture to protect against outbreaks in any part of the world as soon as they occur.

Zscaler, Inc.

392 Potrero Avenue,
Sunnyvale, CA 94085
USA

+ 1 408.533.0288
+1 866.902.7811

sales@zscaler.comwww.zscaler.com