

DATA SHEET | ZSCALER WEB SECURITY CLOUD TECHNICAL OVERVIEW

INTRODUCTION

As the leader in cloud web security, Zscaler’s focus is to provide policy based secure web access for any device, anywhere. Through ground-breaking innovations in its massively scalable cloud architecture, the Zscaler Web Security Cloud provides an ultra-low latency cloud security solution that does not need any hardware or software. Three major factors are driving organizations around the world to adopt Zscaler.

Mobility – Laptops, roadwarriors, and homeoffices are impossible to protect with appliances in the enterprise DMZ. Rather than having a perimeter around the office, Zscaler creates a global perimeter around the Internet. Employees must be able to be online risk-free anywhere and on any device.

Complex Threat Environment – Employees cannot be protected from web based threats using just a URL filter. Active content, social networks, and ad networks have resulted in every major site hosting malware at some point in time. Web2.0 risk mitigation requires a technology that can do inline scanning of every page for complex threats and blocks sensitive content from leaving the organization. It is impossible for IT to keep up with constantly evolving threats using a managed security service that can shield vulnerabilities and block zero day exploits is essential.

Consolidation, Simplification, & Reduced Cost – Powered by unique technologies like NanoLog™, PageRisk™, ByteScan™, and a true multi-tenant architecture, Zscaler’s comprehensive cloud service offers advanced security, Web 2.0 controls, and Data Loss Prevention (DLP). Enterprises can simply point their traffic to any of Zscaler’s 40+ datacenters and be risk-free. Administrators have a single console to manage policy and analyze any transactions in real-time for all offices as well as the mobile workforce. There is no hardware or software to deploy and no agents to install. Simplification and economies of scale enable IT to mitigate risk at half the price.

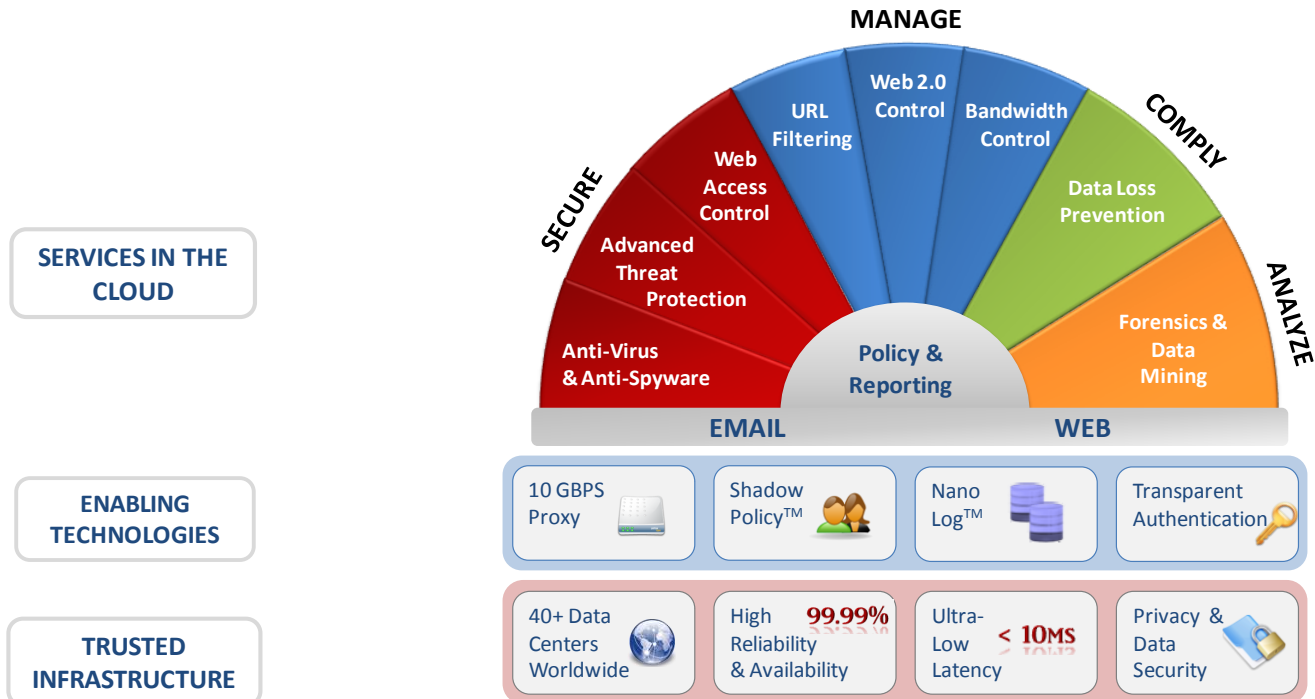


Figure 1: Zscaler Architecture for Comprehensive Web Security and Management

This document provides a technical overview of the Zscaler infrastructure, enabling technologies, services, unified policy, and reporting capabilities, as well as traffic forwarding and authentication methods.

ZSCALER CLOUD OVERVIEW

Zscaler offers four cloud based subscription services that help customers secure and manage every aspect of their employees' web usage. Zscaler Secure, Manage, Comply, and Analyze are offered in various suites and can be deployed without any new hardware or software. Zscaler delivers wire-rate performance with microsecond latencies while all four services are enabled concurrently. Zscaler customers can focus on creating their security and web usage policies, while Zscaler enforces their policies at the finest level of granularity across the enterprise.

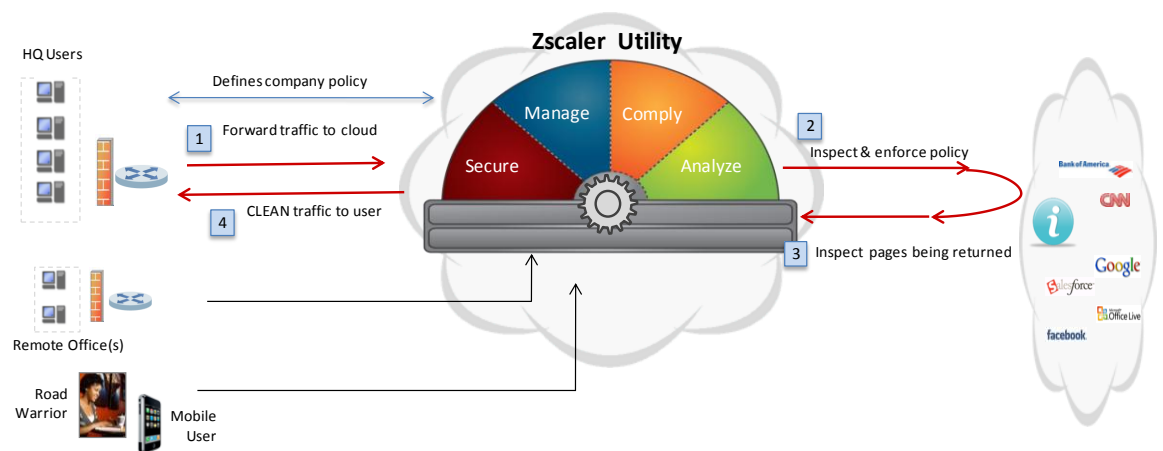


Figure 2: Zscaler Cloud Overview

CLOUD INFRASTRUCTURE

Legacy vendors offer security as a cloud service by creating data centers that host racks of appliances traditionally used within enterprise perimeters. This is not only costly, but customers are bound to only a few datacenters of the provider where their policy is hosted. With each appliance capable of handling only one customer, latency and performance in a multi-tenant environment depend on how many organizations share the appliance. Additionally, transaction logs are spread across many data centers making it difficult to see details in real-time.

Zscaler's greatest achievement is the architecture that was created from scratch to take advantage of being a pure cloud provider, while delivering a truly multi-tenant and highly scalable platform for deep security. The fundamental innovation is in functionally distributing components of a standard proxy to create a giant global network that acts as a single virtual proxy so that any user can go to any gateway at any time for policybased secure internet access. Zscaler infrastructure comprises three key components; Zscaler Enforcement Nodes (ZEN), Central Authority (CA), and NanoLog™ Servers.

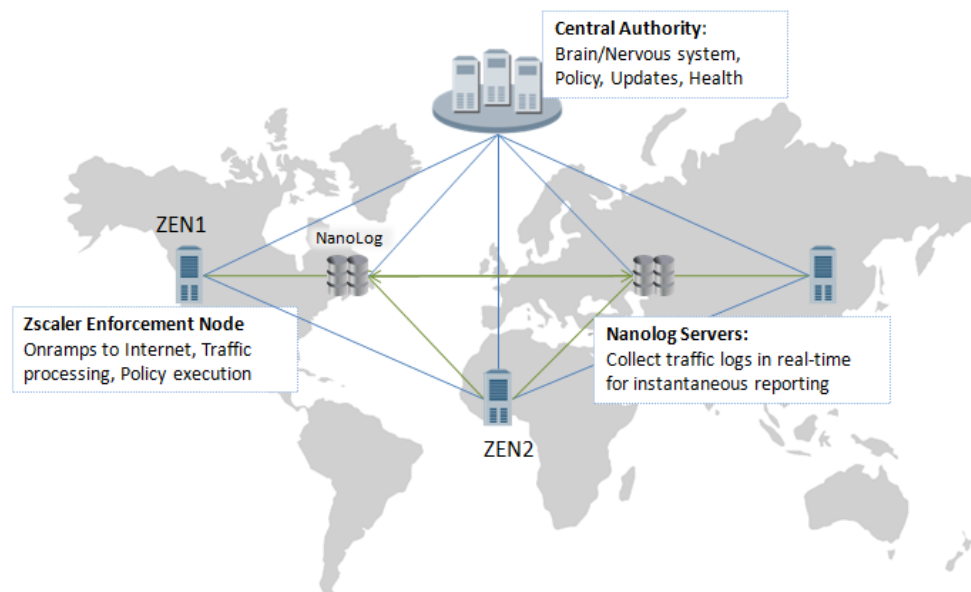


Figure 3: User-policies stored in the CA are enforced on ZENs and logs are stored on NanoLog™

An enterprise forwards all web traffic to the nearest ZEN. Policies governing the user's access to any website are served by the CA and enforced on the ZEN. All transaction logs are stored in a centralized NanoLog™ server for real-time retrieval. Any user can access any ZEN and all components have multiple levels of redundancy to ensure high availability.

Zscaler Enforcement Node (ZEN)

Powered by over thirty patents, each ZEN is a fully featured inline proxy that enforces corporate security, management, and compliance policies at user level granularity. The ZEN incorporates a hardened custom-built OS and a custom TCP/IP stack to deliver 90% of transactions in less than 90 microseconds. Zscaler's ByteScan™ technology enables each ZEN to scan every byte of the web request, content, responses, and all related data for inline blocking of threats like viruses, cross site scripting (XSS), and botnets. This capability also enables Dynamic Content Classification (DCC) of unknown sites. By scanning each page, the ZEN computes a PageRisk™ index for every page loaded and enables administrators to control content served to their users based on acceptable risk.

The ZEN also incorporates Zscaler's unique authentication and policy distribution mechanism that enables any user to connect to any ZEN at any time. This enables enterprises to simply point traffic to any ZEN and ensure full policy enforcement while getting all reports back in real-time.

Central Authority (CA)

The Central Authority complex is the brain of the Zscaler cloud. The CA manages and monitors all nodes and ensures that they are always up-to-date with the latest real-time feeds, software, and synchronized for cloudwide intelligence of threats. The CA directs users to the closest ZEN through DNS and PAC file resolution to ensure minimum latency when users are on the road. Through its multi-tenant architecture, the CA provides each organization with its own portal to self-manage their policy. Any change to the policy is communicated to the ZENs within seconds. The CA provides an enduser authentication framework through integration with Secure LDAP or ID Federation systems.

The Central Authorities are a globally distributed peer-to-peer cluster with an automatically elected master. This ensures all cloud components can always talk to a CA even if there are major internet outages that isolate an entire region.

NanoLog™ Servers

Backed with multiple patents, Zscaler's NanoLog™ technology enables administrators to access any transaction log almost instantly. Each ZEN uses the technology to perform lossless compression of logs by a factor of 50 to 1. These logs are transmitted every second to the NanoLog™ servers over secure connections. Logs are multicast to multiple servers for redundancy. Through an innovative reporting and database framework created specifically for web logs, the NanoLog™ server can support 15 million logs per second. This technology provides an administrator with real-time reports and the capability to query (within seconds) complete transaction level details for any user, department or location at any time. Each server has over 16 Terabytes of capacity, enabling Zscaler to provide multi-year data retention.

SECURITY SERVICES IN THE CLOUD

Zscaler Security Services consist of Zscaler Anti-Virus and Anti-Spyware, Advanced Threat Protection, and Web Access Control.

Anti-Virus & Anti-Spyware

Zscaler provides an inline, ultra-low latency Anti-Virus and Anti-Spyware (AV/AS) solution that protects users from file based attacks. Files of any size including multi-level archives are scanned in real-time. Blocking malware in the cloud is instantaneous and universal, saves bandwidth costs, and obviates the need to patch endpoints or multiple appliances to effectively protect users. Zscaler's enforcement nodes also scan every web page for embedded viruses, malicious javascript, or advertisements that may lure users to download fake AV software. Compared to an inline UTM, IPS, or firewall, Zscaler – being a true proxy – provides superior protection because the entire file is downloaded, assembled, uncompressed, and scanned for millions of viruses before it is delivered to the enduser. By sharing intelligence of infected as well as clean content across the entire cloud, the ZENs are able to deliver fully scanned files without the user noticing any latency. In addition to its inline AV/AS, Zscaler also uses multiple commercial AV/AS engines concurrently in offline mode to uncover any additional threats. Zscaler also offers granular file-type control that is based on true file type detection for over 300 file-types rolled up into classes and sub-classes.

Advanced Threat Protection

Web has become dynamic with active content on every site, and well reputed sites sourcing content from various sites including numerous advertisement networks. Hackers now use SQL injection attacks not to deface websites, but to surreptitiously insert hidden iframes that infect unsuspecting users through drive by downloads. It is impossible for administrators to block "bad sites" because most of the reputed sites have served malware at some point in the recent past, either by getting compromised or using an infected advertisement network. Most websites serve dynamic content that changes based on the user's login or surfing history. The only way to protect the user is to inspect the content they are being served EVERY TIME, and not relying on content scanned by a crawler in the cloud. Asking another appliance to scan content does not work because the appliance does not have the user's password.

Zscaler's advanced security uses the ByteScan™ technology to scan every byte of all requests and responses. This enables Zscaler to detect hidden iframes, cross site scripts, signs of phishing attempts, cookie stealing, and botnet command and control traffic. This unique capability also enables Zscaler to block anonymizers hosted in Facebook even if Facebook itself is allowed.

For each page served, Zscaler computes a PageRisk™ Index that takes into account use of suspicious techniques like javascript obfuscation and zero pixel images. This information is correlated with other factors such as GeoIPbased location of the website and its reputation to compute a dynamic risk index. Administrators can then define a policy to block content beyond their acceptable risk level.

Web Access Control

Old browsers and plugins with known vulnerabilities are the easiest attack vector. Zscaler allows administrators to be proactive with security by enforcing users to use only acceptable browser types and versions. Zscaler also warns users when they are using browsers or plugins with older patch levels if the versions they are using have known exploits in the wild.

MANAGEMENT SERVICES IN THE CLOUD

Zscaler's Manage services consist of URL Filtering, Web 2.0 Controls, and Bandwidth Control.

URL Filtering

Zscaler's URL filtering leverages multiple databases to ensure global coverage. Organizations have complete flexibility to override any classification done by Zscaler. You can add and remove URLs from Zscaler's predefined 90 categories, 30 super categories, and 6 classes to keep reporting and rules consistent. The three level hierarchy makes it easy to create rules and look at reports at the appropriate granularity. Web access policy can be set for specific users, groups, and locations or any combination. Actions include the ability to block, caution, allow, or provide timebased access and quotas in terms of time or volume. Zscaler's inline Dynamic Content Classification (DCC) engine ensures pages are classified by their content if the URL is not sufficient.

Web 2.0 Controls

Web 2.0 is changing how enterprises do business. The challenge with Web 2.0 is to ensure it helps business, but does not hinder productivity. For example, it is desirable that marketing can post a video on YouTube, while others can only view the posts. Zscaler provides granular control over Web 2.0 applications like webmail, streaming media, social networking, and instant messaging. Zscaler understands the protocols used by individual Web 2.0 applications to provide granular control over actions such as posting an update to LinkedIn. The administrators can configure policies by users or groups to enable organizations to take advantage of the latest Web 2.0 platforms without compromising productivity or security of critical data.

Bandwidth Control

Ninety percent of enterprise traffic is on HTTP/HTTPS. The Web is used for business as well as recreation. A few users watching a movie excerpt on Hulu can completely disrupt a customer presentation on WebEx. IT administrators need the ability to control bandwidth by specific web applications rather than ports and protocols.

Zscaler supports bandwidth control by application "class". Administrators can define a transaction to fall in a bandwidth class based on a diverse set of criteria. Large file transfers from any fast website can clog bandwidth. Depending on the size of file being transferred, the transaction can be put in a bandwidth constrained bucket. The same policy can be applied to streaming media sites. On the other hand, transactions to business applications such as WebEx, LiveMeeting, Salesforce, or NetSuite can have a minimum reserved bandwidth regardless of other web traffic. Bandwidth control policies can be set per application class, in terms of the maximum sessions as well as maximum and minimum bandwidth per class, location, and time of day. Bandwidth policy is enforced without dropping any packets, by leveraging Zscaler's custom TCP/IP stack that enables modulating the throughput on each side of the ZEN proxy.

DATA LOSS PREVENTION (DLP) SERVICES IN THE CLOUD

Zscaler is the industry's first fully integrated cloud based web DLP solution. Employees can now send out data over webmail, social networks, blogs, or instant messaging. Zscaler's enforcement nodes scan every byte leaving an organization to look for sensitive data. They provide a variety of dictionaries and engines so that enterprises can enforce compliance policies and protect its Intellectual Property (IP).

DLP Dictionaries

Zscaler provides three forms of dictionaries; special dictionaries that identify a specific type of number or content type, Artificial Intelligence (AI) engine based dictionaries that identify types of documents, and phrase based dictionaries.

Special Dictionaries – Special numbers such as creditcards (with full checksum validation), social security numbers (SSN), Singapore NRIC, and Canadian Social Insurance Numbers.

AI Dictionaries – Types of documents such as financial statements (balance sheets, cashflow statements, income statements, etc.), medical statements, source code (C, Java, etc.), and documents saved from Salesforce.

Phrase Based Dictionaries – Custom dictionaries created by administrators containing company specific keywords (e.g., "Zscaler Confidential"). Zscaler's dictionaries use fuzzy matching techniques to ensure phrases match regardless of capitalization, spacing, and noise words.

DLP Engines

A DLP engine combines one or more dictionaries to match specific compliance requirements. Zscaler provides sample templates for HIPAA, GLBA, and PCI. Administrators can create their own engines by combining dictionaries. For example, a DLP engine containing a dictionary for source code with custom phrases for copyright notices can prevent Intellectual Property loss.

All content leaving the organization is scanned. In addition to HTTP postings, Zscaler can decode all Microsoft documents, PDFs, and content inside a zipped file. Granular rules can be specified for applying specific DLP Engines to a group of users, web application types, or locations.

ANALYTIC SERVICES IN THE CLOUD

NanoLog™ technology enables administrators to get complete transaction level detail in real-time for any user, located anywhere, and on any device. Zscaler's unique real-time reporting capability enables administrators to instantly drill into any sequence of events as they unfold. For forensic investigations, administrators can instantly access specific transactions that occurred at any time in the past, filtering by user, time, location, URL categories, malware types, transaction size, and a number of other parameters. Zscaler's base offering provides six months of detailed log storage and two years of summary data at individual user granularity and over 1500 different views.

Traditional web filtering solutions require administrators to install databases or third party correlation tools to manage their web logs. Zscaler's cloud service takes away the burden of log management by providing detailed log archiving capability that can be expanded to as long as 10 years.

UNIFIED POLICY AND REPORTING SERVICES IN THE CLOUD

Zscaler's policy and reporting does not require training. Zscaler offers diverse functionality and granular policy control with a web based self managed interface that is designed to be intuitive for administrators and easy to read for auditors. Changes to policy can be tracked at the individual rule level. Administrators can create checkpoints to be able to roll back to an earlier state of the policy with a click of a button. As a cloud service, the administrator simply defines a policy for the entire organization in one place and it is applied to all users regardless of whether they are in the office or on the road. This policy can encompass all aspects of web access: Security, Access Management, and Data Loss. The policy can be applied at the granularity of groups, users, locations, time of day, and daily bandwidth or usage quotas.

Leveraging the NanoLog™ technology, Zscaler offers administrators a real-time view into every transaction performed by enterprise users regardless of where they are in the world. Logs are available a few seconds after the actual transaction takes place. This enables administrators to resolve in real-time any internet surfing concerns a user may have even if the administrator is in a coffee shop in Singapore and the user is on a flight over the Atlantic. Zscaler's reporting is organized to help administrators easily navigate and locate interesting patterns or behaviors to help in policy formulation. Through over 1500 unique views into the data, administrators can also quickly perform forensic investigations to find offending transactions.

DEPLOYING ZSCALER

Zscaler's solution is a true SaaS offering making deployment easy; **No Hardware, No Software, No Agents**. The administrator uses existing network equipment to forward traffic and secure the enterprise. It is literally that simple.

Zscaler supports diverse set of traffic forwarding mechanisms that include *GRE tunnels, firewall port forwarding, proxy chaining, or PAC Files*. Zscaler is unique in the Security as a Service space by allowing administrators to enforce user level policies without requiring any software or hardware deployment. Zscaler's patent pending authentication mechanism identifies users through browser tokens and enables enforcement of a consistent policy regardless of whether the user is at the office or on the road, and irrespective of what device they are using.

Administrators can synchronize users, groups, and departments from Microsoft Active Directory, OpenLDAP, iPlanet, Novell eDirectory, or any other directory that supports secure LDAP. Zscaler also offers a fully featured hosted directory option. For enterprises that have deployed ID Federation, users do not need to authenticate to the service as Zscaler supports SAML version 2.0 based authentication and authorization.

BENEFITS SUMMARY



SECURITY

- Eight fully integrated security modules
- Granular Web 2.0 controls – keep the good, block the bad
- Traditional and dynamic real-time URL filtering



GLOBAL CLOUD FOOTPRINT

- Largest web security cloud in the world – customers in 140 countries
- Four 9s availability – local, regional, and multi-continent redundancy
- No measurable latency



COST SAVINGS

- No appliances, no software, no desktop clients
- No upfront costs, pay as you go
- No buying excess capacity – cloud scales as you need capacity



SIMPLICITY

- Eliminates complex point solutions
- Global policy manager – single policy follows user across the world
- Pointing traffic to the cloud is quick and simple



COMPLIANCE & REAL-TIME REPORTING

- View any transaction, by any user, from any location within ten seconds
- Comprehensive Data Loss Prevention (DLP) across ALL devices

ONLY FROM ZSCALER

Traditional security vendors will tell you that they have embraced the cloud, but look deeper. Building and running a cloud is complicated. Zscaler is the largest company in the world focused solely on cloud security. Our R&D centers span three continents, our cloud operates at four 9s availability, and our cloud specific patents stand at 30 and growing. Join the companies from 140 countries, who have thrown away their hardware and software, and moved to the Zscaler Web Security Cloud. **Security made simple!**

MORE INFORMATION



eSec Managed Security
 Bagsværdvej 70B
 DK-2800 Lyngby
 tlf. +45 7020 5585

www.esec.dk

USA & Canada
 +1-408-533-0288
 usc-info@zscaler.com

Latin America
 +52-1811-2551670
 latam-info@zscaler.com

Middle East & Africa
 +33-1-4561-3272
 mea-info@zscaler.com

Japan
 +81-3-6206-8535
 jp-info@zscaler.com

Northern Europe
 +44-845-00-99-531
 neur-info@zscaler.com

Central Europe
 +49-89-9544998-20
 ceur-info@zscaler.com

Southern Europe
 +33-1-4561-3272
 seur-info@zscaler.com

Eastern Europe
 +7-495-287-13-61
 eeur-info@zscaler.com

South East Asia
 +65-9796-5851
 sea-info@zscaler.com

Australia & New Zealand
 +61-3-9653-9088
 anz-info@zscaler.com

India
 +91-80-2667-2127
 india-info@zscaler.com

Greater China
 +65-9796-5851
 china-info@zscaler.com

Zscaler[®], and the Zscaler Logo are trademarks of Zscaler, Inc. in the United States. All other trademarks, trade names or service marks used or mentioned herein belong to their respective owners.