Data Sheet

Zscaler DNS Security

Protect all users, devices, and workloads, on all ports and protocols, in all locations, all the time.

Superior security, availability, and performance for web- and non-web traffic from the industry's most comprehensive cloud native security service edge (SSE) platform.

The Domain Name System (DNS) is integral to how we use the internet, translating web addresses into domain names to connect users, applications, and machines. But as a decades-old service, it's being tested in the modern digital world. Surging traffic from hybrid and remote work, cloud applications, and IoT/OT devices greatly impacts DNS performance and availability—and DNS is a popular vector for threat actors to exploit.

DNS queries can be pretty much anything—as a website can be called pretty much anything— so DNS filtering policies are typically fairly permissive, if they exist at all. Unfortunately, many security tools do not inspect or monitor DNS traffic whatsoever, and even fewer have visibility into encrypted DNS-over-HTTPS (DoH) traffic, which creates blind spots and leaves organizations vulnerable to attacks such as:

- **DNS tunneling:** Malware authors exploit the DNS request/response system to send and receive commands from the adversary on the compromised system, deliver further malware payloads in multistage attacks, or even exfiltrate stolen data 255 characters at a time.
- **DNS Spoofing:** DNS spoofing—frequently executed using Man-in-the-Middle (MitM) techniques— involves altering the DNS entries on a DNS server or entering false information into the DNS cache, resulting in the targeted user traffic getting redirected to an attacker-controlled fraudulent site. This can be used for phishing or to trick users into installing malicious software like worms or viruses.

Scalable DNS Security for the distributed organization

Zscaler DNS Security routes all DNS traffic through the Zscaler Cloud Firewall, part of the cloud native Zscaler Zero Trust Exchange that delivers services at over 150 edge locations around the world for superior performance. Zscaler is the only security vendor that combines optimal DNS resolution with best-in-class DNS filtering, security, horizontally scalable DoH inspection, and data exfiltration protection.

© 2023 Zscaler, Inc. All rights reserved.

With DNS Security, you can define rules that control DNS requests and responses. DNS Security allows you to detect and prevent DNS tunneling, and enables you to:

- Monitor and apply policies to all DNS requests and responses, irrespective of the protocol and the encryption used. This includes UDP, TCP, and DNS over HTTPS (DoH).
- Define granular DNS filtering rules using a number of DNS conditions, such as users, groups, or departments, client locations, categorization of domains and IP addresses, DNS record types, the location of resolved IPs, etc.
- Enforce condition-based actions on DNS traffic, such as allowing or blocking traffic, redirecting requests to specific DNS servers, redirecting users by overwriting DNS responses, etc.
- Detect and prevent DNS-based attacks and data exfiltration through DNS tunnels.
- Enhance your security posture by using Zscaler Trusted DNS Resolver for domain resolution.
- Translate unencrypted traffic into encrypted DNS to send to protective DNS (PDNS) resolvers, protecting and enforcing all DoH traffic regardless of destination.
- Optimize availability to third-party resolvers by redirecting requests to secondary resolvers if the primary resolver fails.
- Ensure optimal localized user experiences using configurable DNS ECS to ensure that users can experience webpages with the correct language, content, and currency.

Benefits of Zscaler DNS Security:

Complete AI-powered inspection to find hidden attacks. Unlimited inline traffic inspection, machine learning, and native SSL decryption prevent stealthy threats and terminate malicious connections.

Full coverage across ports and protocols. Quickly identify and intercept evasive and encrypted cyberthreats using non-standard ports.

Secure DNS without compromised performance. Localized resolutions sustain superior performance while your users and endpoints stay safe from malicious sites and DNS tunneling.

Cloud-delivered protection with global edge presence. Zscaler Firewall provides unmatched security and user experience, as it is fully integrated with Zscaler Internet Access™ and part of the Zscaler Zero Trust Exchange™.

Best-in-class availability. Ensure users maintain reliable, high-speed access with automatic failover options and configurable error handling.

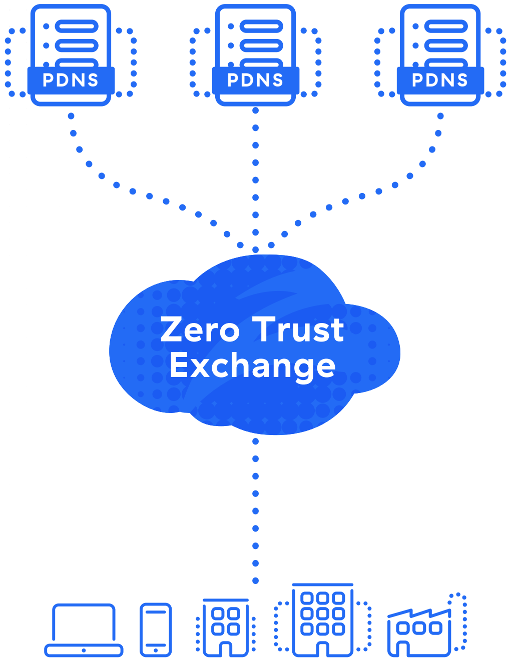
Exceptional user experience. Requests are resolved at the edge and content is delivered by the optimal CDN and in local language and currency for fast, seamless user experience.

Complete visibility over all DNS traffic. Investigate all DNS transactions with confidence through context-rich data and forensically complete logs.

Protections powered by Zscaler customers everywhere. Threat intelligence and ML algorithms are informed by the world's largest inline security cloud and updated in real time.

© 2023 Zscaler, Inc. All rights reserved.

DNS Gateway improves best-in-class availability and security



Any user, device, or workload. Any port or protocol.
Any location. Any time.

1. Forwards all DNS traffic to Zscaler for visibility and policy enforcement at over 150 points of presence
2. Encrypts plaintext DNS into DNS-over-HTTPS (DoH) for privacy and security
3. Directs DoH traffic to Protective DNS (PDNS) resolvers that analyze and block requests to malicious domains
4. Provides failover to secondary PDNS resolvers, ensuring high availability
5. Delivers improved, configurable error handling

Overview: Threat protection and DNS pains solved

DNS Security Challenge / Pain Area	Threat/Pain Detail	DNS Security Solution
Secure, Optimized DNS Resolution		
Users, Devices, Workloads, Servers	Authenticated and unauthenticated users, headless IOT devices, servers, and workloads all need secure DNS resolution	DNS Security deployment architecture addresses all types of traffic forwarding to ZIA DNS Security
Uncertain recursive DNS availability, DoS request flood, NXDOMAIN attack	Remote and hybrid employees and those at offices or company locations need secure, reliable, and low latency DNS resolution	Highly available, optimized DNS resolution using Zscaler Trusted Resolver (ZTR) closest to the user
Untrusted, unsanctioned resolvers or DNS hijacking	Clients going to third-party DNS resolvers internationally or via broadband router or coffee shop hotspot. Device compromised and uses malicious DNS	Direct DNS requests to trusted public resolver, protective DNS resolver, or Zscaler Trusted Resolver
Cache poisoning, DNS spoofing	DNS resolver points to a malicious IP address for a legitimate domain	Separately categorize IP responses. DNSSEC resolutions in Zscaler Trusted Resolvers.

© 2023 Zscaler, Inc. All rights reserved.

DNS Security Challenge / Pain Area	Threat/Pain Detail	DNS Security Solution
DNS Security and Filtering		
Encrypted DNS over HTTPS (DoH) bypassing security	Threat actors encrypting DNS to bypass security and/or using DoH to point to an unsanctioned third-party resolver	Decrypts all DoH, inspects, applies DNS policy
DNS tunneling	DNS tunnels used by threat actors to exfiltrate data or using similar methods to communicate with command-and-control servers	Identify DNS tunnels and categorize into good/bad/unknown. IPS detection for certain tunnels like dnscat and iodine
Risky web content	Users going to web categories that put the company at risk and/or decrease productivity: e.g., hate, porn, illegal content	Categorize both domain on request and IP on response, and block risky categories
Newly registered domains	New domains often used for risky or malicious content or for attack campaigns (<30 days)	Categorized and policy applied
Redirect to sinkhole	Send requests or responses matching configurable conditions to a sinkhole or deception location	Override A/AAA response to selected locations for sinkholing as policy action
Newly observed domains, strategically aged domains, newly revived domains	Long existing domains suddenly becoming active for malware or attack campaign, active then dormant (>10 days) then active again domains	Domains categorized and policy applied
Phantom domains or domain lookups	Deliberately slow authoritative nameservers acts as DoS on DNS resolver	Zscaler Trusted Resolvers are highly available, protected to nameservers. Cloud-based architecture for DNS monitoring allows for infinite scale
Botnet callbacks or discovered/known malicious	Compromised endpoints attempt to connect to botnet for instructions, or for other malicious intent	ThreatLabz and machine learning algorithms, threat feed monitoring to detect, categorize, and block malicious domains. IPS detections for C2/botnet communication identification
Non-standard DNS or DNS masquerading	Modified DNS traffic or non-DNS traffic posing as regular DNS. Can be used for both infiltration and exfiltration or bypass intents	Monitors DNS for RFC spec compliance. DPI-based detection for traffic masquerading as DNS

© 2023 Zscaler, Inc. All rights reserved.

DNS Security Challenge / Pain Area	Threat/Pain Detail	DNS Security Solution
Domain Generation Algorithms (DGAs) or dictionary DGAs	Generated domains used for C2 or other malicious activity	Categorized and policy applied — could be botnet, malicious, phishing or other domain-side category
Illegitimate or unusual record type	Certain endpoints need certain DNS record types but not all endpoints (users, printers, mail servers) need to be able to use call record types or suspicious, added attack surface	Conditionally take action on any DNS record type (typically blended in policy: if user endpoint then no need to permit MX record types, for example)
Undesired A/AAAA responses	Resolver returns unwanted or unspecific IPs for any given domains, request type, categories, etc.	Overwrite A/AAAA responses based on DNS policy
Fast flux	Quickly cycle through domains and IPs	Categorized and policy applied — could be botnet, malicious, phishing, or other domain or IP-side categories
Undesired country domain hosting	Any given domain hosted in a country considered risky	Block geo-IP resolved countries
DNS Visibility and Reporting		
Logging and dashboards	Visibility into regular and malicious DNS activity, usage	Forensically complete logs for requests, responses, error handling, notifications

Compliant with rigorous commercial, government, and industry standards

© 2023 Zscaler, Inc. All rights reserved.

Zscaler fulfills all criteria for safe transit encryption to Protective DNS resolvers recommended by CISA and the NSA.

- ✓ Blocks malware domains
- ✓ Blocks phishing domains
- ✓ Malware Domain Generation Algorithm (DGA) protection
- ✓ Leverages machine learning or other heuristics to augment threat feeds
- ✓ Content filtering
- ✓ Supports API access for SIEM integration or custom analytics
- ✓ Web interface dashboard
- ✓ Validates DNSSEC
- ✓ DoH/DoT capable
- ✓ Enables customizable policies by group, device, or network

Feature overview

As a fully integrated part of Zscaler Internet Access (ZIA), Zscaler DNS Security is included in ZIA and Zscaler for Users Essentials and Business editions. Advanced features of Zscaler Firewall and DNS Security are included in ZIA and Zscaler for Users Transformation and Unlimited editions, as well as part of the Advanced Cloud Firewall add-on to Essentials and Business editions:

DNS Security Functionality	Standard	Advanced
Zscaler Trusted Resolver (ZTR)	✓	✓
DNS policy & filtering criteria:	Up to 64 rules	✓
User identity, time, location, source & destination IP Addresses (including IPv6)	✓	✓
General domain categorization & filtering (adult, gambling, violence, etc.)	✓	✓
Security categorization & filtering (malware, command & control, botnet callback, DGA domains, malicious content, phishing, newly registered & observed Domains etc.)	✓	✓

© 2023 Zscaler, Inc. All rights reserved.

DNS request types: All DNS attributes including but not limited to A, AAAA, MX, NS, CNAME, TXT	✓	✓
Resolve based on country of resolution	✓	✓
Inspect TCP, UDP or DNS over HTTPS	✓	✓
Failover using DNS gateways for high availability	✓	✓
Resolve to sinkhole	✓	✓

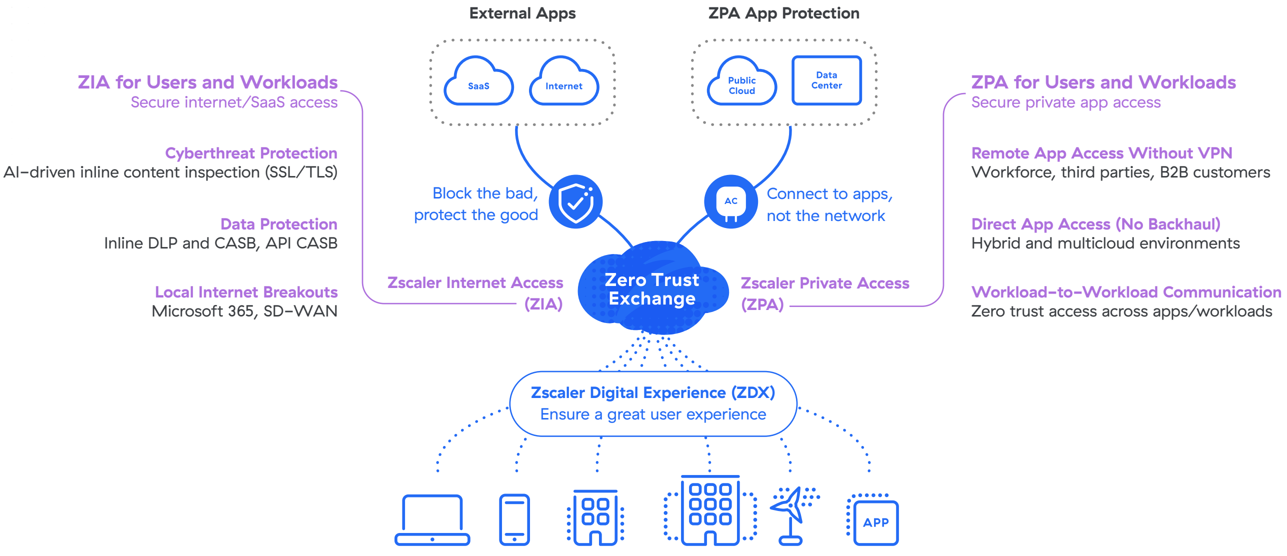
Dashboard & reporting	✓	✓
Detailed, forensically rich logging per transaction	✓	✓
Actions: Allow, Block, Redirect Request, Response	✓	✓
Translate cleartext DNS to DNS over HTTPS (DoH)	✗	✓
DNS tunnel detection & categorization	✗	✓
Application and DNS provider categorization (E.g: Google DNS, NextDNS, DoHUnknown)	✗	✓
Configurable ECS injection for geo-local DNS resolution	✗	✓
	Included with ZIA Essentials, ZIA Business, and Zscaler for Users Business editions.	Included with ZIA Transformation, ZIA Unlimited, Zscaler for Users Transformation & Unlimited editions. Or as an add-on through Zscaler Firewall SKU.

“DNS-only requests” SKU available to provide standalone DNS protection for unauthenticated users. Excludes user identity and time-based rules, DoH inspection, failover to third-party resolvers, translation of cleartext DNS to DoH, and configurable ECS injection.

© 2023 Zscaler, Inc. All rights reserved.

Zscaler DNS Security and DNS Firewall are part of the holistic Zero Trust Exchange

The Zscaler Zero Trust Exchange enables fast, secure connections and allows your employees to work from anywhere using the internet as the corporate network. Based on the zero trust principle of least-privileged access, it provides comprehensive security using context-based identity and policy enforcement.


External Apps
SaaS
Internet
ZPA App Protection
Public Cloud
Data Center
Block the bad, protect the good
AC
Connect to apps, not the network
Zscaler Internet Access (ZIA)
Zero Trust Exchange
Zscaler Private Access (ZPA)
Zscaler Digital Experience (ZDX)
Ensure a great user experience
APP

ZIA for Users and Workloads
Secure internet/SaaS access

Cyberthreat Protection
AI-driven inline content inspection (SSL/TLS)

Data Protection
Inline DLP and CASB, API CASB

Local Internet Breakouts
Microsoft 365, SD-WAN

ZPA for Users and Workloads
Secure private app access

Remote App Access Without VPN
Workforce, third parties, B2B customers

Direct App Access (No Backhaul)
Hybrid and multicloud environments

Workload-to-Workload Communication
Zero trust access across apps/workloads

Any user, any devices, any app, any location

zscaler™ | 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 SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2023 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** 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.

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