

DNS SECURITY.

Every connection starts with a name lookup — **DNS security makes sure that lookup can't be silently redirected, poisoned, or turned into a covert exfiltration channel.**

- DNS SPOOFING & CACHE POISONING
- DNSSEC VALIDATION
- DNS TUNNELING
- PROTECTIVE DNS FILTERING

01 THE MECHANISM



Recursive Resolution

A resolver walks from root to TLD to authoritative server to answer a name lookup, and **any point in that chain can be spoofed, hijacked, or intercepted.**



Cryptographic Chain of Trust

DNSSEC signatures let a resolver verify that a response actually came from the authoritative source **and wasn't altered in transit.**



Protective DNS Filtering

Resolvers check every lookup against threat intelligence before returning an answer, **blocking malicious destinations before a connection ever starts.**

02 THE FLOW

The Validated Lookup VERIFIED

1

A client requests a domain's IP address; the resolver queries the authoritative nameserver.

2

The resolver validates the DNSSEC signature chain from the root down to the domain before accepting the response.

3

Because validation happens on every hop, **a forged or tampered response is rejected instead of returned to the client.**

The Unvalidated Lookup POISONED

1

A client requests the same domain's IP address; the resolver queries what it believes is the authoritative source.

2

An attacker injects a forged response into an unvalidated cache or session, and the resolver has no cryptographic way to detect it.

3

The client is silently redirected, and **every subsequent connection to that domain goes to an attacker-controlled server.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
DNSSEC Signing & Validation	Cryptographically signs DNS zone data and requires resolvers to verify that chain before trusting a response.
Protective / Recursive DNS Filtering	Blocks resolution of known-malicious or newly registered suspicious domains before a connection is attempted.
DNS Query Logging & Monitoring	Captures lookup patterns to detect tunneling, beaconing, and exfiltration hidden inside DNS traffic.
Registrar & Zone Access Controls	Locks down who can change a domain's DNS records, preventing hijacking through a compromised registrar account.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Firewall / Endpoint Controls Alone	No	Inspects network and host traffic but typically doesn't parse or validate DNS response authenticity.
DNS Without DNSSEC Validation	No	Resolves names but accepts any response that arrives, with no cryptographic check that it's genuine.
Blocklisting Known-Bad Domains Only	No	Misses newly registered or previously clean domains repurposed for a fresh campaign.
Logging Without Behavioral Analysis	No	Captures the data but doesn't surface the unusual query volume or entropy patterns that indicate tunneling.
DNSSEC Validation + Protective Filtering + Query Analytics	Yes	Confirms authenticity, blocks known threats, and catches anomalous exfiltration patterns.

DNS SECURITY.

RESOLVE · VALIDATE · MONITOR

05 PROGRAM OPERATIONS

DNSSEC protects integrity, not confidentiality. Signed DNS responses can still be observed in transit; DNSSEC proves a response wasn't altered, it doesn't encrypt it.

Most DNS traffic is invisible to standard security tools. Firewalls and EDR inspect application traffic; DNS often bypasses that scrutiny by design.

DNS tunneling doesn't need malware to succeed. Encoding data in query subdomains is enough to exfiltrate through most default configurations.

A single compromised registrar account can hijack a domain despite hardened infrastructure. DNS security depends on registrar-level access control, not just resolver configuration.

06 CONTROL MAPPING

NIST SP 800-81

Secure Domain Name System deployment guidelines covering DNSSEC and secure resolver configuration.

CISA PROTECTIVE DNS

Federal guidance recommending protective DNS resolvers as a baseline defense against malicious domains.

MITRE ATT&CK (T1071.004 / T1568)

Documents DNS as both a C2 channel and a dynamic resolution technique used by adversaries.

CIS CONTROLS (CONTROL 9)

Email and web browser protections that extend to DNS filtering as a network-layer control.

07 WHAT THIS DOES NOT SOLVE

Endpoints Using Hardcoded IPs

Malware that bypasses DNS entirely by connecting directly to an IP address **evades DNS-layer controls completely.**

Application-Layer Attacks

DNS security confirms where a connection goes, **not whether the application at that destination is itself secure.**

Encrypted DNS Bypassing Resolvers

DNS-over-HTTPS configured in a browser can **route lookups around monitored, filtered resolvers entirely.**

Domain Reputation Lag

A newly weaponized but previously legitimate domain **may not yet appear on any threat intelligence feed.**

08 MYTHS VS. REALITY

MYTH "DNSSEC encrypts DNS traffic."	REALITY DNSSEC only proves a response wasn't tampered with; it does not encrypt or hide the query itself.
MYTH "DNS is too low-level to be a real attack surface."	REALITY DNS tunneling and hijacking are established, actively used techniques for both command-and-control and data exfiltration.
MYTH "Blocking known-bad domains is enough."	REALITY Attackers register new domains constantly specifically because blocklists lag behind first use.
MYTH "Signing our domain with DNSSEC protects our users."	REALITY Signing your domain protects people looking you up; it does nothing for your users' lookups of everyone else unless their resolver also validates.
MYTH "DNS-over-HTTPS is purely a privacy feature."	REALITY The same encryption that protects user privacy can also let traffic bypass enterprise DNS filtering and monitoring entirely.

09 SPEAK THE PROGRAM — KEY TERMS

DNSSEC

Cryptographic signatures that let a resolver **verify a response actually came from the claimed authoritative source.**

CACHE POISONING

Inserting a forged DNS response into a resolver's cache so it **returns an attacker-controlled answer** for a legitimate domain.

DNS TUNNELING

Encoding data inside DNS queries and responses to **exfiltrate information or maintain command-and-control** through a rarely inspected channel.

PROTECTIVE DNS

A resolver service that checks every lookup against threat intelligence, **blocking malicious destinations pre-connection.**

DNS-OVER-HTTPS (DOH)

A protocol that encrypts DNS queries inside HTTPS traffic, improving privacy but **potentially bypassing network-level DNS monitoring.**

DOMAIN HIJACKING

Taking unauthorized control of a domain's DNS records, typically through a **compromised registrar or DNS provider account.**