FARSIGHT SECURITY

DNSDB

The Security Challenge

Cybercriminals quickly exploit Internet infrastructure to support their campaigns and avoid detection; they rely on DNS. Security teams need to "turn back the clock" to view Internet infrastructure as it was at a certain point in time to see how adversaries have "rolled" through related domains, IP addresses and name servers to conceal their activity.

Security analysts and incident responders need access to real-time and historical DNS intelligence data in order to gain context for their threat data and block bad actors by exposing thier entire infrastructure. A historical view of DNS data also enables security teams to detect patterns of malicious activity and identify phishing or other targeted attacks.

The Farsight DNSDB Solution

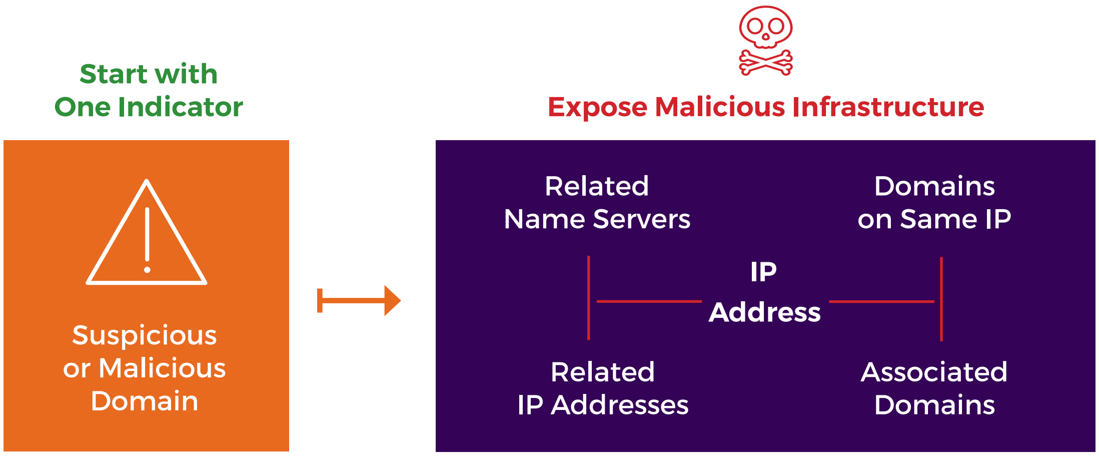
Farsight Security's DNSDB™ is a Passive DNS historical database that provides a unique, fact-based, multifaceted view of the configuration of the global Internet infrastructure. DNSDB leverages the richness of Farsight's Security Information Exchange (SIE) data-sharing platform and is engineered and operated by leading DNS experts.

Farsight collects DNS records data from its global sensor array in real-time. It then filters and verifies the DNS transactions before inserting them into the DNSDB, along with ICANN-sponsored zone file access download data. The end result is the highest-quality and most comprehensive DNS intelligence data service of its kind - with more than 100 billion DNS records since 2010.

> "Farsight's DNSDB is a bridge to new data points in all of our investigations."
>
> **Rich Barger**
> Chief Intelligence Officer,
> ThreatConnect

DNSDB: A Must-Have Tool for Today's Security Teams

Farsight's DNSDB transforms threat feeds into actionable, relevant threat intelligence in real time to increase the value of an organization's existing threat intelligence. Its high-performance, indexed, time-series DNS intelligence data service can ultimately improve visibility for an organization's security program and protect its infrastructure from current and future threats.



Start with One Indicator

Suspicious or Malicious Domain

Expose Malicious Infrastructure

Related Name Servers

Domains on Same IP

IP Address

Related IP Addresses

Associated Domains

Security teams can map out related domains, IPs, and infrastructure for thorough protection.

With DNSDB, security, incident response, SOC and research teams can:

- Accelerate incident research and post-breach analysis.
- Discover associations among threat actors and track and block their activity.
- Perform fact-based risk assessment of domain names and IP addresses.
- Uncover all domains using the same name server infrastructure used by a “known bad” domain.
- Reveal the IPs an adversary is using to conceal malicious activity and avoid takedowns.
- Conduct third-party audits of DNS configurations.

Farsight’s DNSDB is built for ease of use. Chain and pivot capabilities allow security teams to easily swing from one query to another. Time fencing, output tailoring and limiting of record types are among the capabilities that enable investigators to access the exact results they need. DNSDB queries can be automated into

How to Subscribe

For more information, contact **sales@farsightsecurity.com** or call +1-650-489-7919.

About Farsight Security

Farsight Security is the world’s largest provider of historic and real-time DNS intelligence data. We enable security teams to qualify, enrich and correlate all sources of threat data and ultimately save time when it is most critical - during an attack or investigation. Our solutions provide enterprise, government and security industry personnel and platforms with unmatched global visibility, context and response. Learn more about how we can empower your threat platform and security team with Farsight Security DNS intelligence solutions.