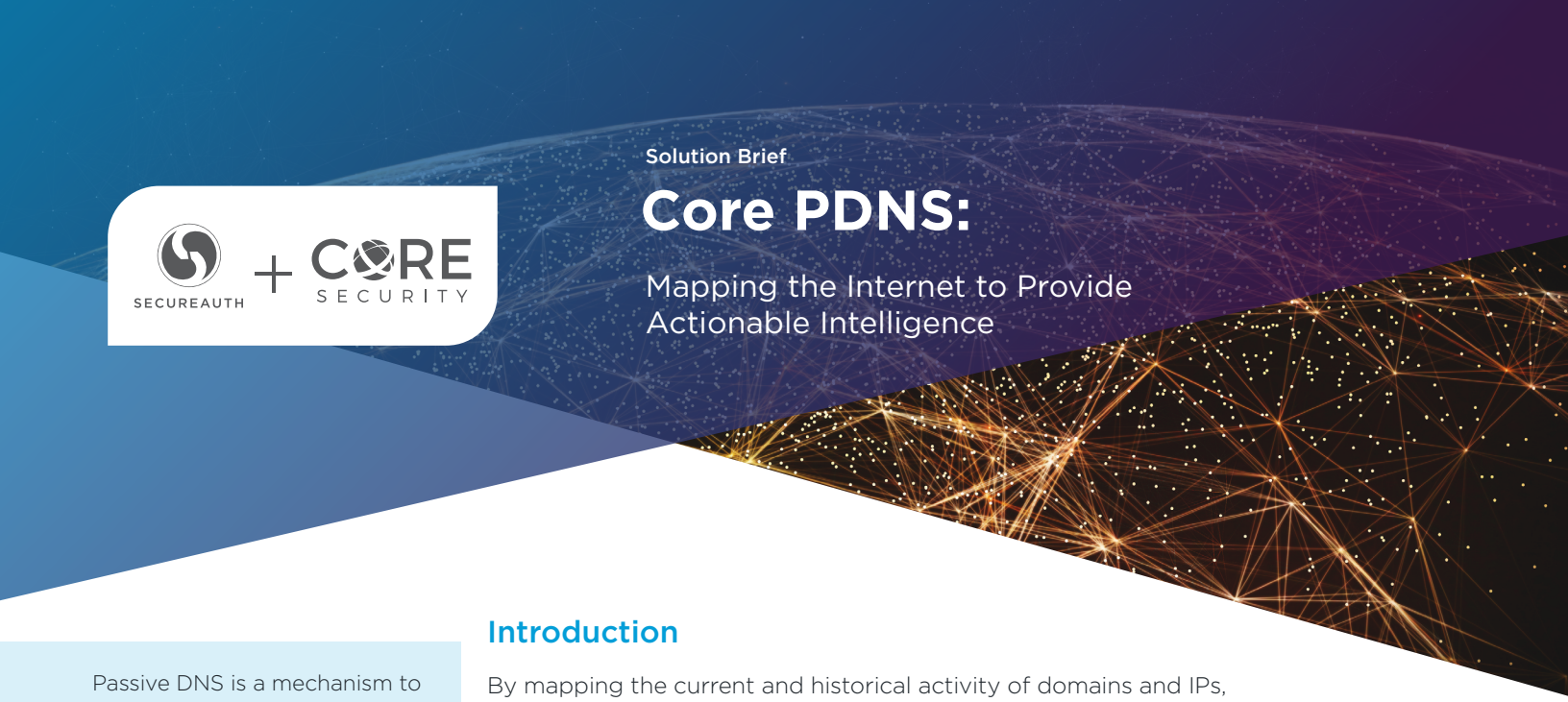
Solution Brief

Core PDNS:

Mapping the Internet to Provide Actionable Intelligence



Passive DNS is a mechanism to capture which sites are being visited at what times, with what volumes, and by how many devices. using sensors located at major DNS clusters on the Internet, Core's PDNS system observes real-time DNS queries from 750 MILLION devices cataloguing:

+ The fully qualified domain being queried (e.g. not.just.toplevel.domains.com)
+ The response data (e.g. an IPv4 address for an A record query)
+ The timestamp of the query / response
+ The queries coming from unique devices or subscribers
+ The volume of queries observed for a domain response pair (RRSet)
+ The type of record queried (A, AAAA, MX, CNAME, NS, etc..)

This data is stored in Core's Hadoop database systems, providing Core's PDNS customers with the current and historical relationships and activity of domains and IPs on the Internet.

Introduction

By mapping the current and historical activity of domains and IPs, Core's Passive DNS (PDNS) provides Incident Response, Fraud, and Security Operation Center teams the richest source of contextual, factual DNS activity data to investigate, mitigate, and protect against cyber threats. Core's PDNS database is the industry's largest, mapping 13.8 Billion domains to IPs with over 1.2 Trillion DNS queries observed a day from over 3/4 Billion devices. Armed with facts on the activity of the Internet, security professionals can:

+ Identify when a domain or IP has become malicious
+ Correlate with threat intelligence to provide context to a security event
+ Enumerate fast flux C&C infrastructure
+ Classify entire IP blocks to be treated as malicious
+ Track threat actors as they change their infrastructure
+ Spot patterns in operators / actors using shared infrastructure and hosting
+ Estimate volumes of victims, rate of growth, and if a domain is still active C&C
+ Discover specific malicious activity, especially for malicious use of dynamic DNS providers' infrastructure
+ Investigate fraudulent use of corporate branding

How Core PDNS Is Delivered

Core's PDNS System is a dynamically available hosted service with no deployment costs. Core's PDNS can be accessed via:

+ **RESTful API:** A RESTful API license key provides an automated query interface. The RESTful API is fully documented and constructed for simple interaction.
+ **Web Console:** A web console interface is provided for a seat license query interface. The web console provides analyst with straightforward answers to their investigative questions.
+ **Admin Console:** Both the RESTful API and Web Console are administered through a hosted Admin Console to assign and manage your license keys and account usage.

Core's Passive DNS system is sold as an annual subscription with pricing of the API License based on query volume and the Web Console Seat License based on number of seats.

PDNS Empowers Your Team By:

Making Threat Intelligence Actionable

You've just learned PIGLYEUTQQ.COM is a TeslaCrypt domain. Core's PDNS reveals all the IPs the domain has ever resided on:

+ 37.123.101.74
+ 46.246.126.108
+ ....
+ 91.196.50.241

Core's PDNS then shows you the related domains that have pointed to those IPs. You immediately identify more domains to block along with context on the actor's network infrastructure.

+ HELLOMENQQ.SU
+ HELLOWOMENQQ.SU
+ ITSYOURTIMEQQ.SU
+ ....
+ HELLOWORLDQQQ.COM

Enhancing Forensic Discovery

You are investigating an incident where a device is potentially compromised. The device's communications are reaching out to the domain amouc.com. Core's PDNS shows:

+ amouc.com has only had activity on it for two days
+ global query volumes are close to the amount of your local activity

You immediately know this is a new domain and potentially targeted uniquely to you. Further investigation reveals customer data is being exfiltrated using a form of DNS exfiltration.

Core's PDNS provides you the context needed to respond quickly.

Providing Visibility Into Fraudulant Use Of Brand

Your company is ACME Inc. You already receive reports from brand protection firms for anyone creating 2LD domain names like MYACME.COM, but you have no visilbity into other abuse.

Core's PDNS allows you to have routine reports of abuse for sub-domain activity such as:

+ acme.myweb.com
+ acme.email.com

Armed with knowledge of the abuse, activity metrics for the fraudulant site, and duration of the activity you can promptly take action to have the domain taken down.

Enhancement Offerings

Combine Core's PDNS offering with Core's C&C Threat Intelligence, an Operator based threat intelligence service, enumerating the network infrastructure (Internet destinations) used by individual threat actors and malware families covering:

+ APTs
+ Nation-state Actors
+ Cyber Espionage
+ Ransomware
+ RATS
+ Banking Trojans & Financial Fraud
+ Information Stealers
+ Spam, DDoS, Clickfraud, and Adware

Core's C&C Threat Intelligence details the complex relationships between threat actors, their network infrastructure, and the malware samples they use and includes detailed threat research reports on the intent of the threat actor and their historical intentions.

750 MILLION
Devices Observed

13.8 BILLION
Domains Catalogued

1.2 TRILLION
DNS Queries / Day

About SecureAuth + Core Security

SecureAuth and Core Security have merged to create a new company and a new category: Identity-Based Security Automation. Core Security is a leader in vulnerability discovery, identity governance, and threat management, while SecureAuth is a pioneer in identity security. Together our mission is to accomplish what no other security technology vendor can claim: Secure the enterprise across all major threat vectors with an identity-based approach to the attack life cycle.