SOLUTION BRIEF

Zero Trust

Service-Level Zero-Trust Enforcement Powered by Pure Signal™ IP Reputation Data

Zero-trust projects come with cost, complexity and accuracy challenges. Whether you're looking to address flaws in your zero-trust environment or you lack the budget and resources to begin, adding service-level enforcement with Team Cymru is an affordable path to big impact.

Network-Based Challenges

Network-based approaches, such as a firewall performing real-time lookups as IPs attempt to gain access, is expensive and requires specialized hardware.

Detection Challenges

Threats evolve too rapidly for technology to keep pace, and threats can emerge from anywhere across the internet—not just from identified enemies, but from sources you trust.

Remote Workforce Challenges

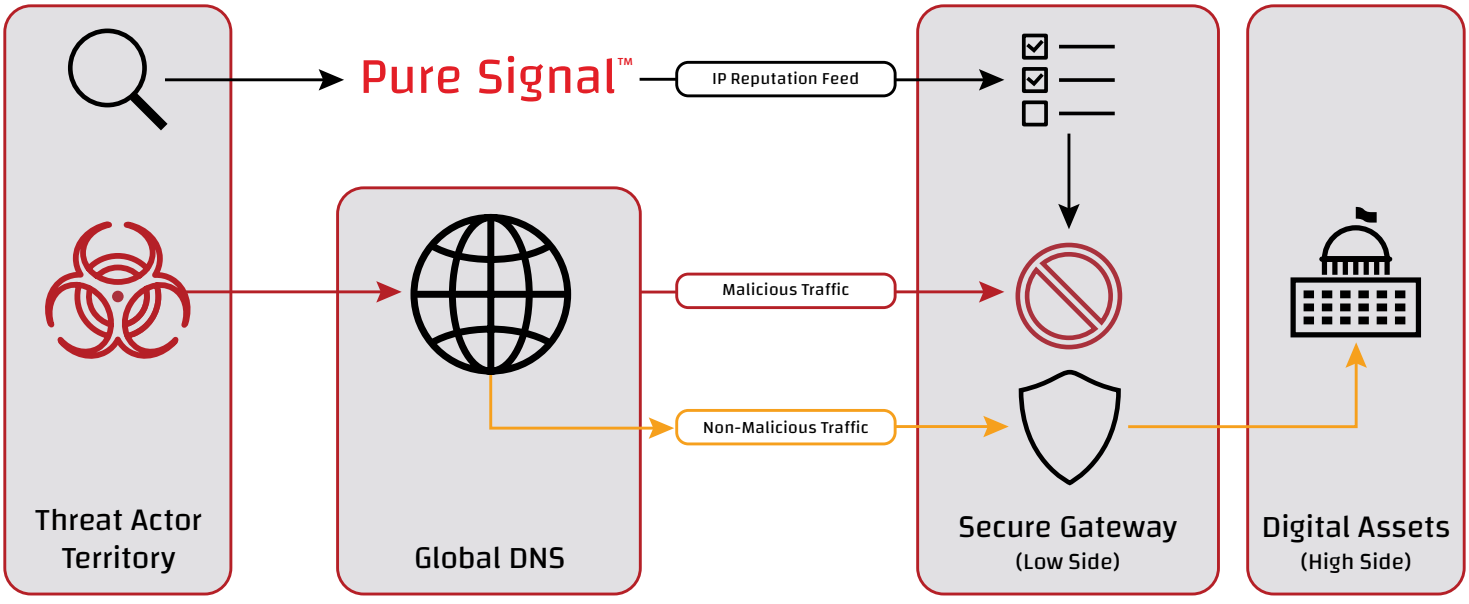
You have no control over the security posture of your work from home employees, and while there are many tools available to assist with this challenge, they are reactionary and produce too much noise.

An Affordable Way to Begin or Augment your Zero-Trust Program

A more comprehensive IP-address-based approach to zero trust is a must. With Team Cymru and some internal knowhow, you can lay a powerful foundation with lower cost and complexity.

We see activity across every AS on the internet, observing and scoring both IPv4 and IPv6 addresses.

- 4.3bn IPv4 addresses connect to networks on the internet. We oberve **almost 100%** of them every 30 days.
- Only 24% of networks advertise being IPv6 compliant, indicating a high risk of misuse of non-compliant gateways.



TEAM CYMRU. COPYRIGHT © 2021. ALL RIGHTS RESERVED.

sales@cymru.com

An Affordable Way to Begin or Augment your Zero-Trust Program

Not just a block list...

Our IP Reputation Feed us not simply a “block list” feed. It is every IP address we observe and score, updated in near-real-time. So, you can set your threshold of acceptable reputation and use this information to enrich your other prevention and detection tools, as well.

The feed is updated hourly and includes an aggregate of the prior 24 hours of activity.

Where does the data come from?

In addition to a global network of sinkholes, honeypots, darknets and sensors, we work with ISPs, hosting providers and over 130 CSIRT teams across 86+ countries to make the Internet safer place. We deliver free services to these partners, and in exchange, they enrich our threat intelligence. As a result, we are observing activity across every ASN on the Internet and scoring that activity to deliver unparalleled reputation data.

What malicious or suspicious behavior does the data show?

- Command and control servers
- Bots
- IP addresses interacting with a honeypot
- Scanners
- Proxies
- IP addresses associated with phishing sites or emails

What metrics and measures are used to score the IP?

Every IP address in the feed is scored using several different categories of patterns observed over the past 30 days. The key used to calculate the score is included in the feed and can be used to reconstruct the behavior patterns observed for each individual IP address in the feed.

- Number of days in feed
- Number of active detections
- Number of passive detections
- Detection type
- Controller behavior:
  - –Non-standard port
  - –# controllers on same IP
  - –# unique domains on same IP
  - –Instructions decoded
  - –DDoS Activity
  - –SSL usage
  - –Malicious IPs in /24

What do you need to make a big impact at low cost...

Team

Required Skills

- Scripting (Bash, Powershell, Perl/Python, etc.)
- Working DNS knowledge
- HTTP server configuration

Resources

What you need on premises

- Working DNSBL instance
- Web and other services able to use DNS RBL services

Infrastructure

What you'll need to connect

- Internet facing network
- Web server
- DNS server

CONTACT US
tel: +1 847-378-3300
fax: +1 407-878-7833
sales@cymru.com

EMERGENCY CONTACT
+1 847-378-3301
support@cymru.com

TEAM CYMRU