Defend your network against threats on the internet.

DNS Safeguard
DNS was designed for usability

Domain Name System (DNS) servers keep everything that’s connected to your network and the internet communicating.

What’s DNS?

• DNS translates domain names into IP addresses.
• DNS requests are made before IP connections.
• Every port and connected device uses it.
• It’s designed to make connectivity work.
DNS Variants

Authoritative DNS
Owns and publishes the “phone books”

Managed By:
• IANA (Root DNS Servers)
• TLD Registries
• Entity who has registered the domain or their provider

Recursive DNS
Looks up and remembers the #s for each name

Managed By:
• ISP
• End User Directly
Don’t ignore Recursive DNS in your security strategy

- 91% of malware variants use DNS\(^1\).
- 68% of organizations don’t monitor recursive DNS\(^1\).
- 15% of malware BYPASS port 80 & 443\(^2\).
- 99% of malware was sent via email or webserver\(^3\).

\(^1\)Cisco Security research
\(^2\)Lancope Research
\(^3\)2017 Verizon Data Breach Investigations Report (DBIR)
Build a first line of defense

It all starts with DNS.

- Malware Distribution
- Command and Control
- Visiting Risky Sites
- Ubiquitous

Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.
Block bad traffic as it approaches

Step 1
Screens DNS request—Where did it come from? Which policy to apply?

Step 2
What’s the request and where should it be sent?
- Safe or whitelisted? Route request as usual.
- Malicious or blacklisted? Route request to block page.
- Risky? Route request to cloud-based proxy for URL inspection.

DNS Safeguard
- Only sends suspicious domains for review.
- No noticeable performance issues due to added latency and complexity.
Enterprise-wide deployment in minutes

1. Signup
2. Point your DNS
3. Done

On-network coverage
With one setting change
Optional:
- NAT Rules to enforce DNS
- Active Directory Integration

Off-network coverage
Client Agents Available
AnyConnect VPN client integration
Take control of the internet experience

Enforce company-wide acceptable use polices through web content filtering.

• Restrict outbound browsing activity based on categories and custom block lists.

• Enforce consistent policies across different locations and different technology sets.

• Manage polices on an easy-to-use cloud console.

• Add automatic, customized block pages.
## Do USE and Enterprise Grade Solution

### Reliability

- 99.999% Uptime
- High Performance Requirements

**Requires:**
- Redundant Architecture
- International Deployment

### Intelligence

Security is only as good as the intelligence:

- **Malware Distribution Category**
  Attempts to distribute Malware

- **Command and Control**
  Indicate compromise on your network. Can contain the compromise

- **Categorization Feeds**
  Limit Risk and reduce False Positives

### Reporting

Get the reports you need to take action:

- **Identity report**
  Review malicious activity.

- **Destination report**
  Investigate malicious domains, URLs and file hashes.

- **Cloud services report**
  Uncover activity in the cloud and on Internet of Things (IoT) devices.
TLS 1.3 – It’s coming

Introduction of **Perfect Forward Secrecy (PFS) ciphers**

- **Pros:** Much greater level of security for SSL connections
- **Con:** Will essentially blind passive network analysis appliances relying on DPI such as those used for performance monitoring, IDS, and DLP.

**DNS does not rely on DPI**
Thank you.
## Select the package that meets your requirements

<table>
<thead>
<tr>
<th>Package</th>
<th>Basic</th>
<th>Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protection</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defend against internet-based malware, phishing and C2 callbacks over any port.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Enforce acceptable use policies using 60 content categories.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Protect any laptop or mobile device on your network.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Protect virtually any internet-connected laptop off-network.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Policy and reporting granularity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View activity by each network circuit.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>View activity from a user level (Microsoft Active Directory).</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Enforcement</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block malicious domain requests and IP responses at the DNS layer.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Proxy risky domains for URL inspection.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Get Verizon and Cisco threat intelligence feeds.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Visibility and intelligence</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get detailed logging and reports.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Integrate with Verizon Managed Security Services (MSS-Analytics).</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Support</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get support from Security Operations Centers (SOCs).</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
Intelligence to see attacks around the globe

Verizon + Cisco data

• Verizon Threat Research Advisory Center threat feeds.
• Cisco Talos feed of malicious domains, IPs and URLs.
• Cisco data—100B Internet requests /connections per day.

Models

• Automatically uncover malware, ransomware and other threats.
• Identifies and removes low confidence data, escalates high confidence data.
• Continuously analyze millions of live events.

Security researchers

• Experienced researchers.
• Threat linkage and attribution data.
• Models to identify/classify domains and IP reputations.
Defend users when they’re on the go

DNS Safeguard gives you the visibility you need to protect your network from internet threats where your users work.

Across offices  Any device on your network  Roaming laptops  Cloud services monitoring  Network ports and HTTPS destinations
Get a better view of internet threats*

Cisco:

- 100B+ Daily internet requests or connections
- 60K+ Daily malicious destinations identified
- 3M+ Daily new domain names discovered
- 7M+ Malicious destinations enforced at any given time

Verizon:

- 61B+ Security events annually (average)
- 550M 550 million incidents annually (average)

VTRAC Data

- VTRAC Data
- Verizon Intelligence

24x7 support

- 24x7 support
- Verizon SOC support included

*Cisco research

Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.