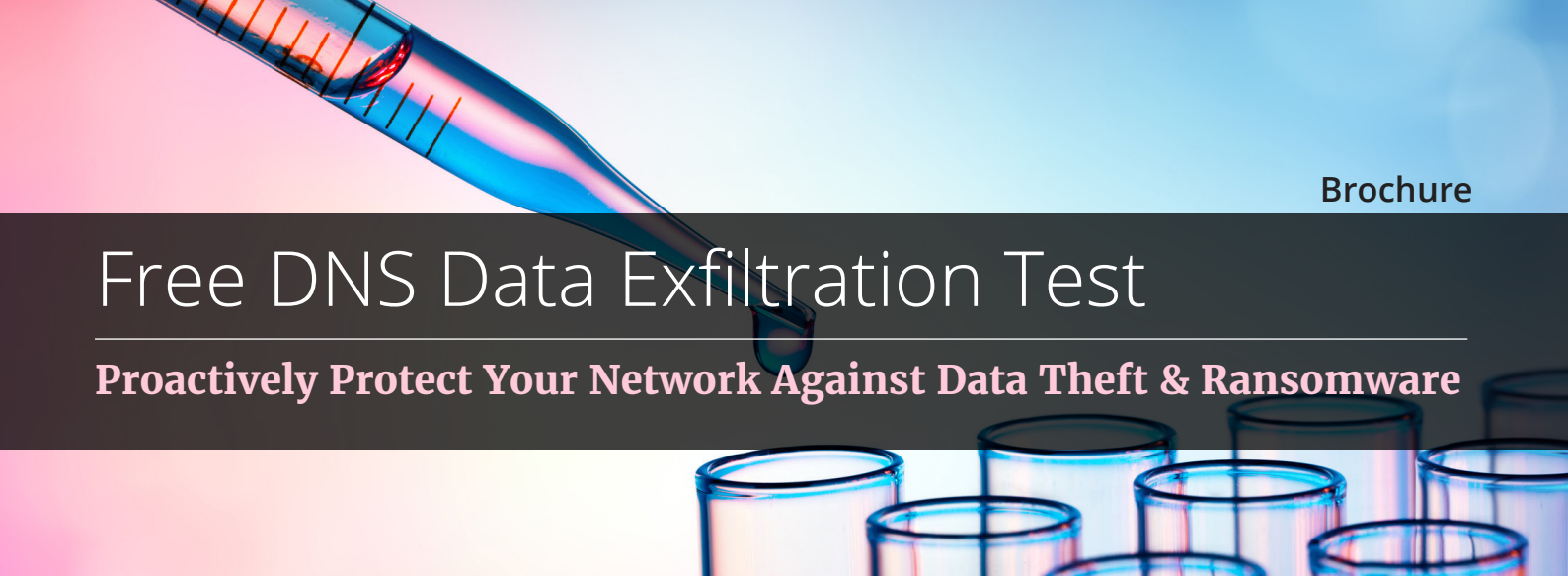


Brochure

# Free DNS Data Exfiltration Test

## Proactively Protect Your Network Against Data Theft & Ransomware

*26% of companies suffer data theft via DNS*

IDC 2021 Global DNS Threat Report

### Test Your Protection Against Data Breaches via DNS

EfficientIP proposes to conduct a test on the target network, and provide a short summary of the results.

The test is a structured "ethical attack" on the DNS system and customer applications to identify potential vulnerabilities. It uses the same tools and techniques that real attackers use to break into networks.

## Benefits

- Detect data exfiltration threats
- Avoid data theft fines (GDPR, US CLOUD, PDPA...)
- Learn from proven security experts about improving reliability of your DNS
- Identify vulnerabilities faster
- Learn about adaptive countermeasures
- Reveal weaknesses in your current security layer, receive recommendations

### Check Your Recursive DNS Infrastructure

Get quick visibility on your recursive DNS infrastructure's capability of detecting & preventing data theft. To verify your protection, EfficientIP offer a rapid assessment of your existing DNS architecture and your protection systems in place.

### What Is Included

**Pre-briefing with your team:**

- ✓ Understand your DNS configuration - authoritative & recursive DNS
- ✓ Explanation of scope and objectives of the test

**DNS data exfiltration test on your DNS servers:**

- ✓ Check for security vulnerabilities related to data exfiltration
- ✓ Read-only actions performed, no configuration modifications
- ✓ Carried out using EfficientIP's specifically-designed toolkit

**Post-briefing:**

- ✓ Explanation of test results
- ✓ Identified vulnerabilities
- ✓ Recommended actions & countermeasures

**Total duration: 180 Minutes / Cost: Free of Charge**

efficient iP®

## Requirements for Execution (Provided by the Customer)

- ✓ Customer IT Operations contact person:  for understanding the network
- ✓ Customer IT Management contact person: for debrief of recommended actions & countermeasures
- ✓ On-site network and internet connectivity

*91% of malware are using DNS*

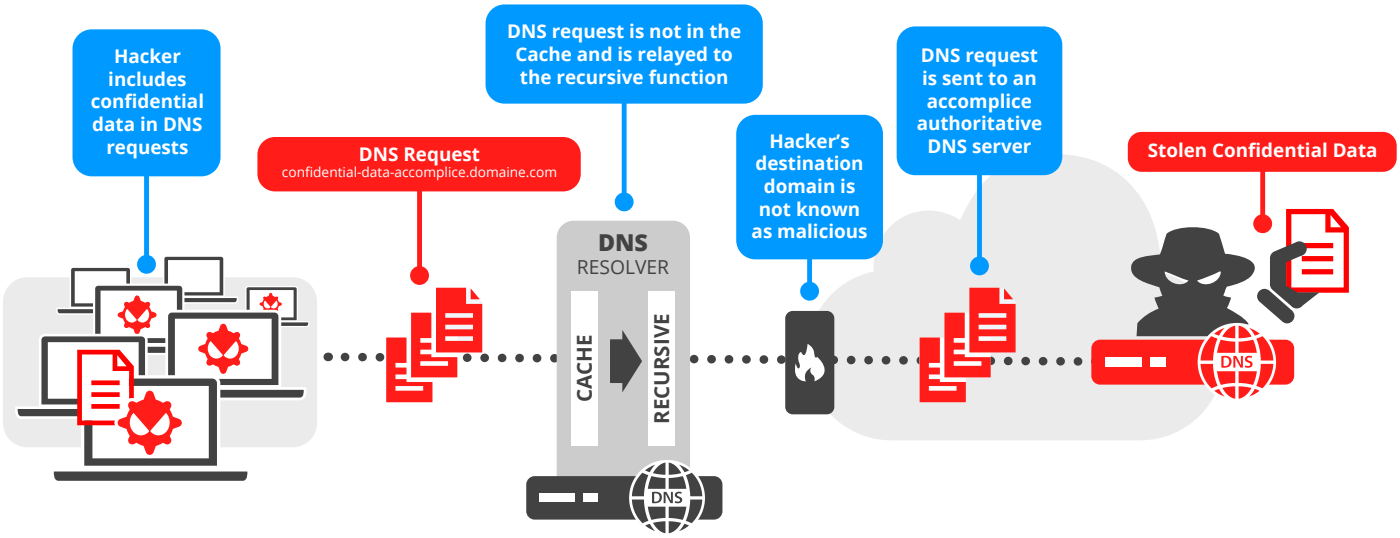
*Cisco 2016 Security Report*

## Understanding Why DNS is a Favorite Target for Data Theft

Since DNS isn't generally associated with data delivery, it is often overlooked. Cyber criminals benefit from this assumption to bypass security mechanisms for transporting sensitive data from inside to outside the enterprise. The DNS protocol is manipulated to act either as a tunneling protocol or as a 'file transfer' protocol.

Firewalls and DLP systems are incapable of detecting this exfiltration, so most businesses don't even know that data is being stolen until it's too late.

**To protect data confidentiality, organizations need to look beyond traditional security solutions which have proven to be ineffective against data exfiltration via DNS.**




*How Data is Exfiltrated via DNS*

**To sign up for your Free DNS Data Exfiltration Test, please contact us.**