3 Reasons You Need Proactive Protection Against Malware
We’re here to talk about protecting the existing gaps in your security stack.
Cyber crime is on the rise
Targeted Threats are Increasing and Evolving

The prevalence, volume, and sophistication of targeted threats such as malware, ransomware, data exfiltration, and phishing are rising.

Malicious actors are adapting and evolving to bypass conventional security mechanisms.

Organizations are struggling to effectively deal with this deluge.
The Realities of Cyber Crime

In 2016, the number of data records lost or stolen was overwhelming:

- 70% of organizations have had a security incident that negatively impacted their business in the past year.
- Over 390,000 new malicious programs are registered every day.
- Only 38% of global organizations feel prepared for a sophisticated cyberattack.
- Global cost of cybercrime is predicted to hit $6 trillion annually by 2021.
- Average cost of an APT data breach is $18 million; 50% is damage to brand reputation.

- 3,046,456 every day
- 126,936 every hour
- 2,116 every minute
“A Fortune 1000 company will fail because of a cyber breach.”

Excerpt from Forrester’s *Dynamics That Will Shape The Future In The Age Of The Customer*
Malicious actors are increasingly using the Domain Name System (DNS) to bypass defenses.
Why is Recursive DNS Exploited?

Almost every action taken on the Internet begins with a Domain Name System (DNS) request that translates domain names to IP addresses.

The DNS protocol is inherently open and unfiltered.

It has no intelligence and will resolve requests for a good or malicious domain.
Why is This an Urgent Problem?

Cyber criminals have realized just how simple it is to exploit this unprotected security gap to get malware onto the network and extract sensitive data.

The number of attacks utilizing this vector are increasing quickly.
Why Are These Attacks Flourishing?

Despite the acknowledged vulnerability of the DNS infrastructure, the pressure to protect consumer and proprietary data, and the growing number of connected devices, few CIOs and IT teams make protecting the DNS infrastructure a priority.
Securing this vector is difficult
Imagine all the ways malware can enter your network...
All it takes is one employee or visitor on your network to:

- Access a link in a phishing email
- Click a malware-laden advertisement
- Open a compromised URL in a social post
- Navigate to a typosquatter’s site
- Access a homographic domain
- Share infected computer storage media
- Succumb to a social engineering tactic

Over 90% of malware uses DNS to spread the infection, take control of your network, and/or exfiltrate data.¹¹
Volume of Traffic Poses a Problem

There are thousands of devices on a network: laptops, mobile phones, desktops, tablets, printers, projectors, guest Wi-Fi, “smart” IoT devices, and more.

They make hundreds of thousands of DNS requests a day.

This volume often obfuscates abnormal activities. There is often too much good and too little bad traffic to warrant the resources necessary to monitor DNS logs.
Visibility into Global Trends is Vital

Even if you allocate the resources to constantly monitor and dissect your DNS logs, it’s highly unlikely you’ll identify and mitigate an intrusion before it inflicts damage.

This is because your company’s sample size is too small to identify global Internet trends and threats.
Existing security point solutions and appliances aren’t enough.

They’re often ineffective, inconsistent, and reactive.
Layers of Defense are Critical

Products like firewalls, Secure Web Gateways, endpoint antivirus, and threat intelligence services rely heavily on blacklists, manual updates, reactive adjustments, and 100% user compliance.

They are often only as good as the providers’ threat intelligence database.
It’s a Cat and Mouse Game

Given the rate of evolution of malware and the evasive measures bad actors employ to avoid detection—using non-standard ports and protocols, domain generation algorithms (DGAs), fast flux, and DNS exfiltration to name a few—most defense mechanisms lack the agility to adapt alongside a targeted threat and are quickly rendered obsolete.
There is a better way
Grow revenue opportunities with fast, personalized web experiences and manage complexity from peak demand, mobile devices and data collection.

Akamai
Enterprise Threat Protector
Sources


