DNS SECURITY SOLUTIONS

- DNS Security Overview
- In House vs. ManagedDNS
- Different types of DDoS Attacks
- How Volumetric Attacks Affect Networks
- Balance the load
- Leave it to the DNS Experts
- Proven Reliability

digicert®
DNS Trust Manager

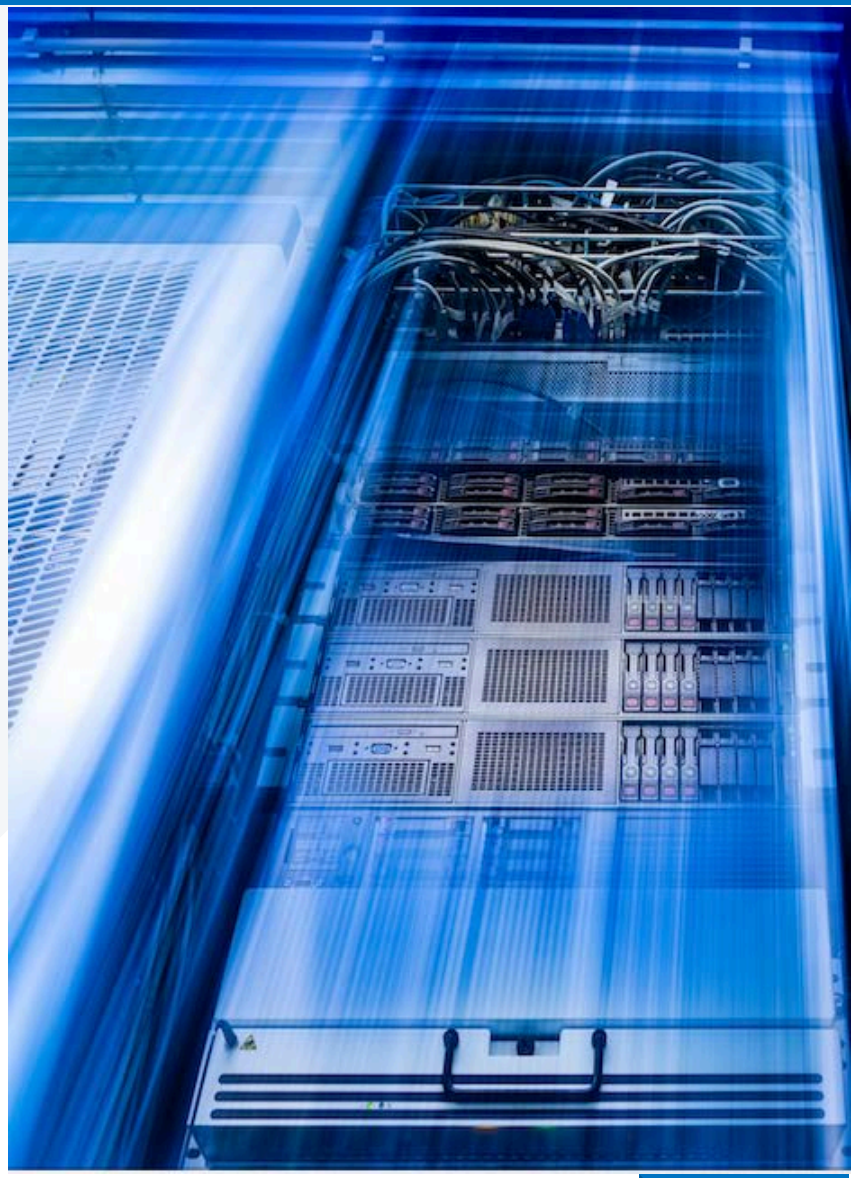
DNS SECURITY INTRODUCTION

DDoS attacks are rapidly growing in magnitude and frequency every year. In fact, the third quarter of 2021 saw a 40.25% increase in smart DDoS attacks over Q3 of 2020. This trend isn't new. In Q1 of 2020, domains experienced a staggering 776% increase in DDoS attacks over 100 GBs from Q1 of 2019 (Comparitech). The majority of these attacks were volumetric, but 53% involved amplification attacks (F5 Application Threat Intelligence), which take advantage of external networks, such as DNS and Cloud providers to bring down a target. The most vulnerable networks are DNS networks that are housed on only a handful of servers at one location.

DOES INFRASTRUCTURE MATTER?

Benefits of using an enterprise network.

This alarming increase in attacks has triggered administrators and business owners to seek DNS providers with larger and more secure infrastructures. By using enterprise networks, companies don't have to purchase and maintain overpriced routers or firewalls that are incapable of handling modern DDoS attacks. Instead, they can turn to enterprise providers like DigiCert DNS which have a proven track record of reliability and expertise in DNS hosting services.



COST OF ATTACKS:

DDoS attacks cost businesses

$100,000 / HOUR

(60K increase since 2015)
Source: Imperva 2021

IN HOUSE VS MANAGED DNS

What's the difference?

In-house operated networks lack the same capabilities as a managed DNS provider. Most attacks prove successful because in-house systems lack the large bandwidth capacity afforded to enterprise-level providers. Recent surveys have discovered that DDoS attacks are growing at exponential rates. In 2005, the highest reported attack (by NTT) was only 10 Gbps. However, this number has increased drastically over the years.

In 2012, we mitigated an attack that exceeded 200 Gbps—the largest attack at the time. In 2020, the network experienced a 500+ Gpbs DDoS attack, but thanks to its extensive infrastructure, customers were unaffected and all systems remained online.

Mitigating such large attacks is only possible because DigiCert DNS continually invests in its network and infrastructure. To date, the company has 23 PoPs, over 3,200+ peers, 300 Gbps of peering capacity, 730 Gbps of transit capacity, and 4TB of DDoS protection. In 2022, the DigiCert DNS Made Easy network has seen a a new PoP in Stockholm, Sweden, and major upgrades to current PoPs in Miami, Seattle, and London.

Organizations using in-house DNS infrastructures spend thousands of dollars on firewalls to protect their servers. The problem with this is that regardless of how large the firewall is, if network connections for incoming traffic aren't large enough, they will be unsuccessful in mitigating a threat of any size.Nameservers can only handle a finite amount of DNS requests or PPS (packets per second) before they fail. DigiCert DNS solves this problem by setting up hundreds of nameservers worldwide on a triple IP Anycast network. By serving DNS traffic across so many nameservers, our network can manage exponentially more requests than a typical unicast or in-house network.

WHAT'S IN IT FOR YOUR ORGANIZATION?

- 100% Uptime Guarantee
- 30 Day Free Trial
- Competitive Pricing
- DigiCert Backed Security

TYPES OF DDOS ATTACKS

What is a DDoS Attack?

Distributed-Denial-of-Service (DDoS) attacks are designed to deny access to a server or network. DDoS attacks are carried out by cybercriminals who have either assembled a botnet (typically a large group of hacked devices) to attack a specific target or through an amplification/reflection attack, which uses publicly accessible DNS servers to flood a target with lookup requests. When faced with such a large barrage of unexpected traffic, systems can quickly be overwhelmed and taken offline.

DDoS Attack Categories

VOLUME-BASED ATTACKS (VOLUMETRIC)
This type of attack is designed to overwhelm bandwidth and includes attacks such as:

- UDP flood
- ICMP flood
- NTP Amplification
- Reflection Attacks
- NXDomain attacks

Protocol and Application Layer Attacks

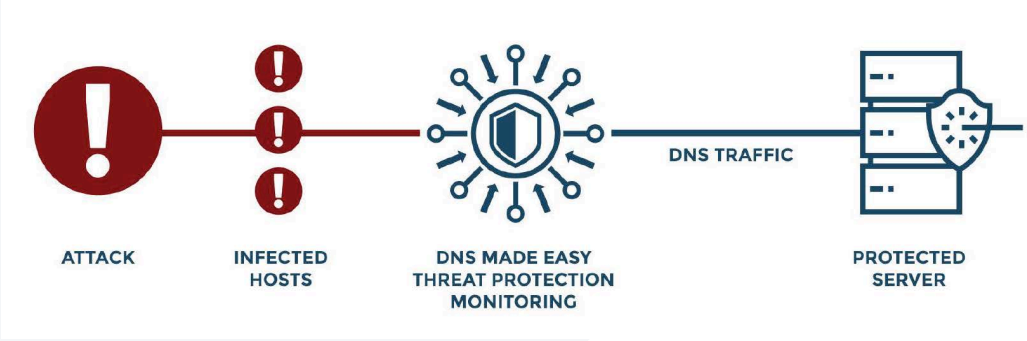
Protocol attacks target equipment and server resources, as well as firewalls and load balancers with flood attacks like:

- SYN flood
- Ping of Death
- TCP State Exhaustion

Application layer attacks are geared toward applications like Apache, OpenBSD, and Windows and are designed to bring down web servers with innocent-looking requests.

- Slowloris
- HTTP(s) flood
- Low and Slow attacks
- GET floods
- POST floods

The graphic below demonstrates how DigiCert DNS Trust Manager protects against volumetric attacks:



100% UPTIME:

Choose a provider with 100% uptime, and has options for redundancy at every point of failure.

HOW VOLUMETRIC ATTACKS AFFECT A NETWORK?

As volume-based attacks are the most frequently used DDoS attack, we will use this as an example to show the difference between how in-house and unicast systems handle DDoS attacks compared to managed, anycast+ networks.

Attacks on a Unicast or in-house network:
The attacker floods the target with query traffic. Bandwidth connections have limited capacity, which eventually leads to system failure when they become overwhelmed by an influx of unexpected traffic. You can think of an incoming bandwidth connection as a pipe—the larger the pipe, the more data the network can receive. The problem is, no matter how large the pipe, it will eventually become clogged as traffic increases. When the pipe is clogged, firewalls can't see the traffic and can no longer protect your network.

BALANCE THE LOAD

Take a look at the difference a managed DNS makes when faced with an attack.

1. The attacker floods the target with malicious query traffic, which drowns out the good traffic.

2. At DigiCert DNS, malicious traffic is cleaned via a proprietary scrubbing algorithm before it is sent through our network. Traffic is dispersed to many Points of Presence (PoPs) to distribute and balance the load.

3. Each PoP then filters traffic through our comprehensive system of firewalls and intrusion detection services.

4. Once filtered, clean traffic is pushed to our nameservers, which direct and answer query traffic. In contrast to many of our competitors who run on a handful of virtual private servers (VPSs) per PoP, we use strategically placed bare metal servers.

NETWORK FACT:

The DigiCert DNS network is also engineered to protect against many other attacks including TCP State Exhaustion attacks (protocol abuse), Reflection/amplification attacks, and Application attacks (DNS).

DDoS ATTACK SOLUTIONS

Smart Monitoring

Solutions: Monitoring is Key to Preventing DDoS Attacks
Most companies put themselves in a defensive position when it comes to DDoS threats, which ultimately prolongs the attack. With the right tools, however, you can put your organization in an offensive position that allows you to identify threats and stop them before they have a chance to cause damage to your domain.

REAL-TIME TRAFFIC ANOMALY DETECTION AND ADVANCED ANALYTICS STOPS:

DDoS Attacks and NXDomain Attacks

DNSSEC STOPS:

DNS TUNNELING
DNS POISONING
DNS CACHE POISONING

WHAT DOES THE AVERAGE DDoS ATTACK COST?

More than $114,000

Source: NTT Best Practices Against DDoS Attacks

WHAT IS THE COST FOR 24/7/365 MONITORING?

Less than $5 /year

Based on a 2 minute interval per record per year.

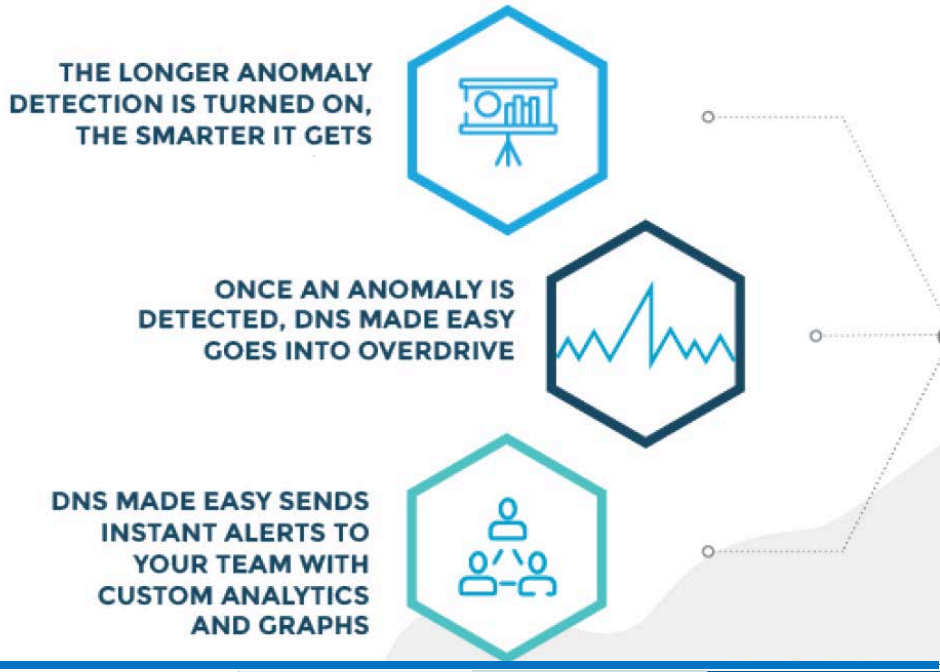
SECURITY SOLUTIONS

✓ REAL TIME TRAFFIC ANOMALY DETECTION (RTTAD)

Real-time Traffic Anomaly Detection uses machine learning to detect and predict suspicious or unusual activity for your domain. By continuously analyzing your unique traffic, RTTAD learns what is and isn't normal for your domain and sends instant notifications to IT teams if it notices anything out of the ordinary. The longer RTTAD has been enabled, the more accurate it becomes. With real-time alerts and clear visualizations of activity, teams can quickly determine if detected anomalies are legitimate or a threat, and take action accordingly.

WHAT HAPPENS WHEN AN ANOMALY OCCURS:

Multi-level updated technology masterfully designed to push DNS



digicert®
DNS Trust Manager

FULL DNS AUDIT LOG HISTORY:

Query logging and advanced analytics

With DigiCert DNS advanced Query logging and Analytics platform, you can view your web traffic's real-time and historical patterns. With this unique data at their fingertips, your IT team will be able to spot unusual behavior and take appropriate measures before things spiral out of control.

VIEW TRAFFIC IN REAL-TIME

MONITOR BEHAVIORS

STOP THREATS AND ISSUES BEFORE THEY CAUSE PROBLEMS

DNS SECURITY BENEFITS

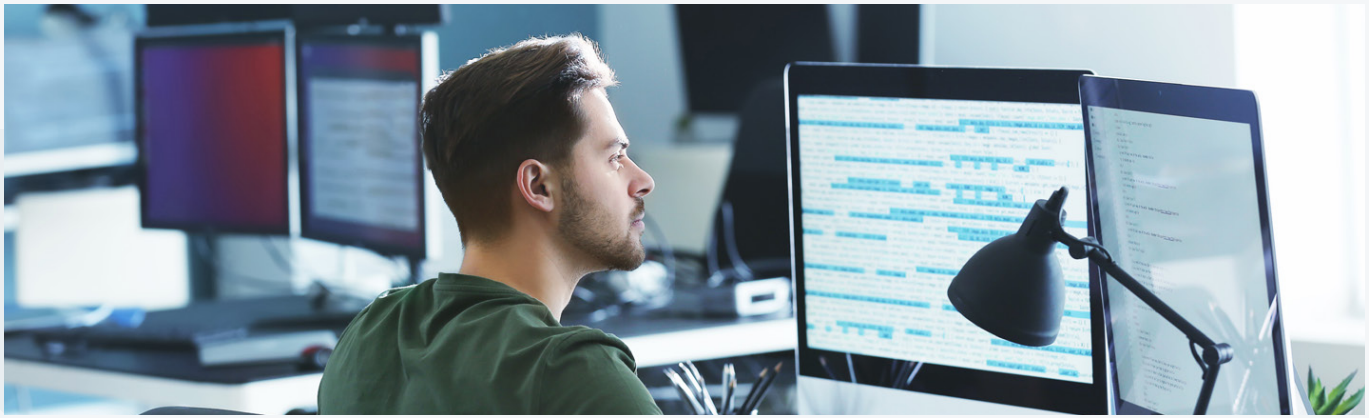
Our Legacy in DNS Network Security.

For over 20 years we have set the record for the longest history of uptime in the industry, all the while mitigating attacks and maintaining only top tier standards. We accomplish this by staying up to date with the latest security threats, our staff of industry experts, and exceptional customer care.

THE TRUSTED PLATFORM

Monitoring is vital to avoid some of the internet's most devastating attacks.

The DigiCert DNS platform is constantly monitoring query traffic for influxes and possible threats. In the event of an attack, our fleet of engineers are always ready 24/7/365. Our core team of developers are the industry experts, handpicked from governmental and financial institutions. Experts in BIND and DNS infrastructure, we are constantly on top of the latest security threats and upgrade our system for the latest updates and patches to ensure 100% uptime.



LEAVE IT TO THE SECURITY EXPERTS.

Ensure Success for your Business.

For over 20 years the DigiCert DNS network has set the record for the longest history of uptime in the industry, all the while mitigating attacks and maintaining top-tier standards. We accomplish this by staying up-to-date with the latest security threats, our expertly trained staff, and exceptional customer care.

The DigiCert DNS platform is constantly monitoring query traffic for influxes and possible threats. In the event of an attack, our highly skilled engineers are always ready—24/7/365. Our core team of developers comprises seasoned industry veterans with backgrounds in top-level government and financial sectors. With our expertise in BIND and DNS infrastructure, we are able to continuously upgrade our system with the latest updates and patches to ensure 100% uptime for our customers.

Our custom-developed attack prevention tools are designed to thwart malicious traffic at the firewall and nameserver levels. Each feature is developed and maintained in-house, and our support staff is trained to answer any unique and complex DNS question.

DID YOU KNOW?

DigiCert DNS Trust Manager

ENSURES 100% UPTIME

24/7/365

TO ALL CUSTOMERS

PROVEN RELIABILITY:

Globally Trusted Network

DigiCert DNS is a world leader in digital trust and providing global IP Anycast enterprise DNS services. DigiCert DNS implemented the industry's first triple independent Anycast cloud architecture for maximum DNS speed and DNS redundancy.

Originally launched in 2002, our DNS services have grown to manage hundreds of thousands of customer domains receiving more than 180 billion queries per day.

Today, DigiCert DNS builds on a proud history of uptime—12-plus years and zero outages—and is the preferred DNS hosting choice for major brands around the world.

digicert®
DNS Trust Manager

READY TO SWITCH? GET PROACTIVE ABOUT YOUR DNS MANAGEMENT.

Streamline your DNS management and focus your time on your business. Learn how DigiCert DNS Trust Manager can help you migrate your existing DNS. Email sales@dnsmadeeasy.com today to discuss your DNS management needs or visit dnsmadeeasy.com to sign up for a live demonstration or a complementary 30 day trial.