Stop DNS Attacks

CloudShield DNS Defender® is a carrier and enterprise-grade DNS (Domain Name Services) security solution that protects against DNS attacks, enhances overall DNS performance, provides insights in DNS traffic, and delivers the flexibility you need to protect your DNS infrastructure from evolving threat actors.

Without DNS, Business is Paralyzed

Organizations spend heavily on cybersecurity, while leaving the most vulnerable infrastructure, DNS, unprotected. Without DNS, users and business are paralyzed. DNS protocols and infrastructure were not architected for security, and threat actors take full advantage of DNS vulnerabilities. Every year, ISPs, financial institutions, and high-profile enterprises report more frequent and higher bandwidth DNS attacks. They include DNS-specific distributed denial of service (DDoS) threats such as floods, amplification, and reflection assaults, and protocol-specific attacks such as cache poisoning, source spoofing, no-recursion, and more.

For DNS, the Firewall and IPS Fall Short

Firewalls and IPSs have their role in network security, but fall short for protecting DNS. The general-purpose firewall must keep port 53 open and cannot track state for UDP-based protocols like DNS. DNS-based DDoS or advanced persistent threats against DNS servers require DNS Defender.

Unmatched Seven-Layer DNS Security

DNS Defender is the first dedicated DNS firewall designed specifically to safeguard DNS systems. It can intercept, block, and counter DNS attacks with sophisticated measures that leverage the power of CloudShield Deep Packet Processing technology. DNS Defender examines fully every DNS packet, including payloads, to identify malicious content and respond at line speed before attackers can impair or take down the network.

KEY BENEFITS

Seven-Layer Security

Seven layers of security from DNS Defender can deliver rapid return on investment by stopping attacks that could damage your business.

Fast Performance

You can postpone DNS infrastructure upgrades with DNS Defender performance acceleration from a fast cache that answers up to 250,000 DNS queries per second.

Rich Insight

DNS Defender includes DNS Defender Management Analytics, or DMA. DMA enables a new pane for your SOC or NOC along with analytics to help you understand both DNS traffic and threats.

Custom Flexibility

Only DNS Defender allows you to add custom security countermeasures as needed, enabling rapid defenses against new cyber assaults.

DNS Flow Optimizer

Prevents collateral damage from botnet attacks on DNS.

Transaction Tracking Filter

Prevents amplification attacks like DDoS and cache poisoning.

DNS Type Filter

Prevents cache poisoning and poison pill attacks while helping with policy enforcement.

Validation Filter

Prevents buffer, fragmentation, covert channels, malformed names, and flag issues.

Attack Filter

Blocks known threats like the ‘Christmas Tree’ attack.

Source/Destination Filter

Prevents late binding, cache poisoning, and address attacks. Helps policy enforcement. Drops spoofed IPs.

Protocol Filter

Blocks non-DNS traffic and helps with policy enforcement.
The Internet of Things Will Only Increase DNS Traffic

Each year smartphones, tablets, CCTV, VoIP, and many additional new endpoint types create hundreds of millions of new DNS requests. IPv6 will increase risk to your DNS infrastructure. Can you handle the increasing traffic without compromising security?

Handle Growth with Fast DNS Performance

DNS Defender can help defer upgrades to your DNS infrastructure by offloading DNS servers and accelerating DNS performance, answering approximately 80 percent of queries from its hardware cache with latency under 0.2 milliseconds.

The Insight You Need to Manage Mission-Critical DNS

DNS Defender Management Analytics, known as DMA, offers information and analysis tools to aid network and security technicians in identifying DNS network issues such as attacks or dramatically increased traffic. DNS experts can take steps to address DNS anomalies before network disruption.

DNS Information

DNS Analysis

Add Defense Measures When Needed

DNS Defender helps mitigate risk, enabling you to identify and understand new threats, and add new custom defenses with a simple-to-use development environment.

DNS Optimization on Every CloudShield Platform

DNS Defender gives you security, performance, insight, and flexibility based on CloudShield deep packet processing (DPP) technology, available on every CloudShield platform, depicted at right.

SYSTEM SPECIFICATIONS

CloudShield CS-4000
Trusted Network Security Platform

CloudShield PN41 Blade
Deep Packet Processing Module for IBM® BladeCenter®

CloudShield CS-2000
Content Processing Platform

Lookingglass is the leader in threat intelligence management, empowering confident real-time actions through focused and verified multi-source information. Lookingglass provides a unique lens to information customers may already have, creating active intelligence for effective decisions.

Visit www.lgscout.com for more information.
Or call 888.SCOUT.93