Don't let Cyber criminals catch you by surprise.

Protect your business from cyber attacks with
MainOne's NEW Managed Security Solution

www.mainone.net

MainOne

PROTECT YOUR BUSINESS FROM SOPHISTICATED DDoS ATTACKS

HACKERS across the globe can at the push of a button cripple your organization's network and prevent legitimate customers from accessing your service. This type of cyber-attacks known as DDoS has cost organizations millions of dollars in losses; arising from network downtime, website unavailability, customers dissatisfaction and churn, settlement cost to hackers, as well as reputational brand damage to affected organizations.

With MainOne's Advanced DDoS protection solution, your organization is assured full protection that covers all aspect of threat prevention, detection, correlation and response today, and as those threats evolve.

MainOne Advanced DDoS Solution is powered by Radware's recently introduced line of DefensePro, the ultimate in "IoT botnet killer" platforms. It provides the industry's most advanced, automated protection from fast-moving threats, including recent and emerging IoT-based attacks, as well as next-generation DNS attack protection, SSL-based attack protection with built-in SSL module and recurring burst attack protection.

SOME OF THESE ADVANCED THREATS include:

IoT Botnets:
Most notable is the Mirai botnet, used to carry out the largest DDoS attack in history in the fall of 2016. With additional botnets uncovered in 2017, it is clear that the impact botnets will have in cybersecurity has just begun.

DNS Attacks:
Sophisticated attackers take advantage of the DNS protocol behavior to generate more powerful attacks — including DNS Water Torture and DNS Reflection/Amplification attacks. Mitigating these attacks requires tools that can learn and gain a deep knowledge of the DNS traffic behavior.

Burst Attacks and Advanced Persistent Denial-of-Service (APDoS) Campaigns
include short bursts of high-volume attacks in random intervals and attacks that can last weeks, involving multiple vectors aimed at all network layers simultaneously. These types of attacks have a tendency to cause frequent disruptions in a network server's service-level agreement (SLA) and can prevent legitimate users from accessing services.

SSL/Encrypted Attacks:
Attackers are using SSL protocol to mask and further complicate attack traffic and malware detection in both network and application-level threats. Many security solutions use a passive engine for SSL attack protection, meaning they cannot effectively differentiate encrypted attack traffic from encrypted legitimate traffic and can only limit the rate of request.

Ransom Denial of Service:
A ransom denial-of-service (RDoS) attack is one form of ransombased attack in which the perpetrator sends an email threatening to attack an organization — rendering its business, operations or capability unavailable — unless a ransom is paid by the deadline. These attacks have increased yearly since 2010 and typically come in the form of a volumetric DDoS attack. RDoS attacks are particularly insidious because they do not require the attacker to hack into the target's network or applications.

MainOne Advanced DDoS solution is uniquely built to overcome both the complexity and scale of today's sophisticated IoT-based botnets to deliver guaranteed protection to businesses.

Customers Requirements on DDoS Solution	MainOne Advanced DDoS	Other DDoS Providers
First-in-class behavioral-based algorithm to protect from known and unknown DNS flood attacks	✓	✓
In-the-box, patented SSL attack mitigation to provide the lowest latency, most efficient SSL attack protection	✓	Nil
Fully Managed Service with Real Time Insight and Reporting before, during and after attack.	✓	✓
Behavioral-Based Detection For Highest Accuracy with minimal false positives	✓	✓
Dedicated Hardware (On-premise) to fight-off Attacks	✓	Nil
Burst attack protection to provide detection and mitigation from one of today's top threats	✓	✓
24/7DDoS Attack Monitoring and Blocking with 10-minutes response SLA. Covers IOT Botnets, Burst attacks, SYN Floods, etc.	✓	✓
ERT Under Attack service provides 24/7 access to a Radware security expert within 30mins to take the lead, mitigate attacks and share post-mortem reports with customers	✓	Nil
Continuous protection from the most recent known attacks and vulnerabilities	✓	✓
Location based mitigation. Detection, alerting and blocking of malicious traffic based on source countries and provision of heat map on hostile regions	✓	✓

Make the call NOW to safeguard your enterprise network and ensure your business is never disrupted even during attacks.

Send a mail to **info@mainone.net** or **call 08090404000** to speak to our enterprise customer representatives.

@MainOneService MainOne