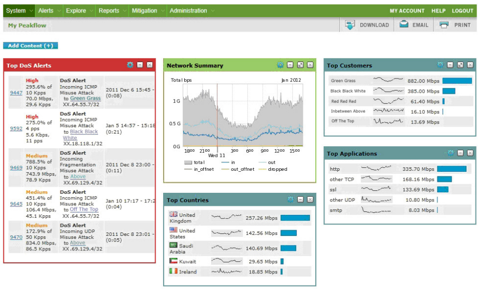
How are you protected from DDoS attacks?

As malicious players relentlessly pursue new means to sharpen their craft and avoid detection, the threats to organisational networks grow exponentially. Botnets composed of hundreds of thousands of compromised devices provide the foundation for tools that can inflict devastating DDoS attacks; this not only impacts revenue, but also damages a company's reputation and reduces customer confidence. Simply stated, the DDoS threat is evolving at an extraordinary rate – and so too must security solutions.



Top DoS Alerts

9447	High 295.6% of 10 Kpps 70.0 Mbps, 29.6 Kpps	DoS Alert Incoming ICMP Misuse Attack to Green Grass XX.64.55.7/32	2011 Dec 6 15:45 - (0:08)
9592	High 275.0% of 4 pps 5.6 Kbps, 11 pps	DoS Alert Incoming ICMP Misuse Attack to Black Black White XX.18.118.1/32	Jan 5 14:57 - 15:18 (0:21)
9469	Medium 788.5% of 10 Kpps 743.9 Mbps, 78.9 Kpps	DoS Alert Incoming Fragmentation Misuse Attack to Above XX.69.129.4/32	2011 Dec 8 23:00 - (0:11)
9645	Medium 451.4% of 10 Kpps 106.4 Mbps, 45.1 Kpps	DoS Alert Incoming ICMP Misuse Attack to Off The Top XX.64.55.7/32	Jan 10 17:17 - 17:2 (0:04)
9470	Medium 172.9% of 50 Kpps 834.0 Mbps, 86.5 Kpps	DoS Alert Incoming UDP Misuse Attack to Above XX.69.129.4/32	2011 Dec 8 23:01 - (0:05)

Top Countries

United Kingdom	257.26 Mbps
United States	142.56 Mbps
Saudi Arabia	140.69 Mbps
Kuwait	29.65 Mbps
Ireland	18.85 Mbps

Top Customers

Green Grass	882.00 Mbps
Black Black White	385.00 Mbps
Red Red Red	61.40 Mbps
Inbetween Above	16.10 Mbps
Off The Top	13.69 Mbps

Top Applications

http	335.70 Mbps
other TCP	168.16 Mbps
ssl	133.69 Mbps
other UDP	10.80 Mbps
smtp	8.03 Mbps

Whatever the deployment, 'RedSpam Guardian Network' uses the latest and leading DDoS technology, filtering the unauthorised and suspicious traffic, providing our customer's 'clean' traffic eradicating malicious content and rate based attacks.

Distributed Denial of Service attacks are seen in the network as a mix of undesirable and legitimate business traffic. Our 'In the Cloud' solution uses a verity of various techniques to identify and filter the undesirable traffic.

The undesirable attack traffic may come in large quantities with the intent of using brute force to overwhelm the victim system or it could come shaped in a well crafted way, designed to disrupt normal service performance. RedSpam mitigations are designed to allow desirable traffic through to the destination while lowering the impact of undesirable traffic. Adversor use various "countermeasures" to target and remove as much of the attack traffic as possible, and to allow our client's service to continue operating.

REDSPAM DELIVERABLES

Function	Action
RedSpam Infrastructure Support	Guardian Network is checked for latest patch levels and Protection Pack updates
RedSpam System Support	Configuration statistics are reviewed, and diagnostic information obtained.
RedSpam In Life Support	Security patches are applied and diagnostics are checked and optimised. (e.g. enabling/disabling IPS rules to obtain optimum protection)
RedSpam Advisory	Applies Network Protection packs (with rule, signature, and block list updates) – HaaS Service Only
RedSpam Monitoring	Constantly monitors the status of the RedSpam network for deviations from its configured baseline
RedSpam Reporting	Portal Access including weekly status reports
RedSpam hardware Support	Initiates Hardware Replacement process in the event of a hardware failure

REDSPAM PROVIDES TWO DEPLOYMENT OPTIONS

- 'In the Cloud' DDoS service oriented architecture proving organisations with the ability to protect their corporate networks and website from multi-faceted sophisticated attacks.
- 'HaaS' - Dedicated hardware solution utilising the leading DDoS architecture, fully managed and supported during the lifecycle of the contract

FEATURES & BENEFITS

DEDICATION

We are dedicated solely to defending organisations from the damage caused by DDoS attacks.

TECHNOLOGY

RedSpam's solution is based on a combination of world class hardware and software solutions combined with our own mitigation technologies encompassed within a single management framework to offer you a world class protection service.

RESILIENCE

Each PoP is located in safe and secure data centre environment, managed by some of the world's leading data centre providers.

LOCATION

Our scrubbing centres are located in central London and London Docklands, ensuring minimal latency and flexible peering for the EMEA market.

INNOVATION

Our continual monitoring of traffic and mitigation of attacks enables our experts to identify ever changing attacks, improving mitigation solutions to the most complex attacks.

FLEXIBILITY & AFFORDABILITY

Fixed cost with no additional 'overage' or hidden extras irrelevant of the size or duration of an attack.

SIMPLICITY

The needs of organisations differ and we have therefore designed a range of service packages priced to meet a range of budgets making the protection accessible to all.

ISP AGNOSTIC

RedSpam are truly ISP and hosting company agnostic, no matter who you choose for your hosting or bandwidth.

RedSpam – DDoS Protection Packages (CLOUD)

DDoS attacks work so effectively because the attacker is able to muster such a huge volume of firepower to fling at your system. RedSpam protection against DDoS attacks is offered in a number ways, all of which can be tailored rapidly to individual circumstances and requirements.

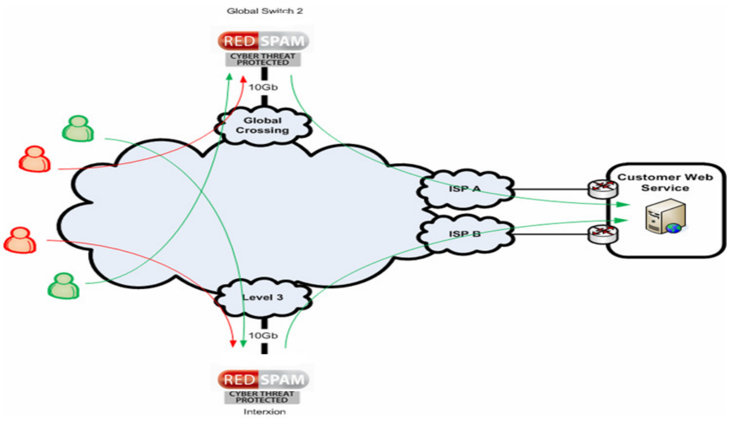
DDoS PROTECTION PACKAGES (CLOUD)

EMERGENCY: this service deals with attacks that are already in-flight. It can be implemented in minutes using DNS change to divert the attack to RedSpam cleansing and scrubbing centre. This service is available to any company using HTTP or HTTPS protocols and there is no requirement to be contracted to RedSpam.

HOSTED/MANAGED PROXY: this is a pre-emptive, always-on service where customers locate their own hardware in the RedSpam mitigation PoP or use a virtualised proxy platform. It provides 24/7 DDoS threat detection monitoring, secure VPN access, and traffic return to customer data centres can be via routing, tunnelling, physical interconnect or managed VPN. Daily, weekly and monthly reports, including anomaly detection, are provided.

BGP ROUTED: this is a usage-based DDoS mitigation service, analagous to a Clean Pipe ISP. No on-premises equipment is needed, and there is secure access to a customer management portal. As with the hosted/managed proxy service, BGP routing provides 24/7 DDoS threat detection monitoring and traffic return to customer data centres. This can be via routing, tunnelling, physical interconnect or managed VPN.

RedSpam - ‘In the Cloud’ Topology



FEATURES & BENEFITS

ALWAYS UP TO DATE

RedSpam ensures that the solution is always up to date, running at peak performance, and automatically protecting the IT infrastructure and ensuring incident response and corrective action is carried out

ALWAYS MONITORING

RedSpam actively monitors the Guardian Network (In the Cloud or HaaS) from our Security Operating Centre. Working to the highest security standards, the service offers active prevention on 24 hour alert basis

ALWAYS PROTECTED

RedSpam ensures you have the peace of mind that your organisation is protected and always up to date. As new threats are detected, the service automatically puts in place the necessary security defences. No action needed to upgrade as technology changes, you can relax without having to make any changes yourself.

ALWAYS SUPPORTED

RedSpam maintains your security defences always on the alert. We stay dedicated to your business and information outcomes with full accountability and reporting. When you choose to work with us, you have access to highly trained engineers that have considerable experience in configuring, deploying and supporting devices globally, adhering to rigid Service Level Agreements and standards.

ALWAYS

RedSpam removes the need for capital purchases on equipment and software.