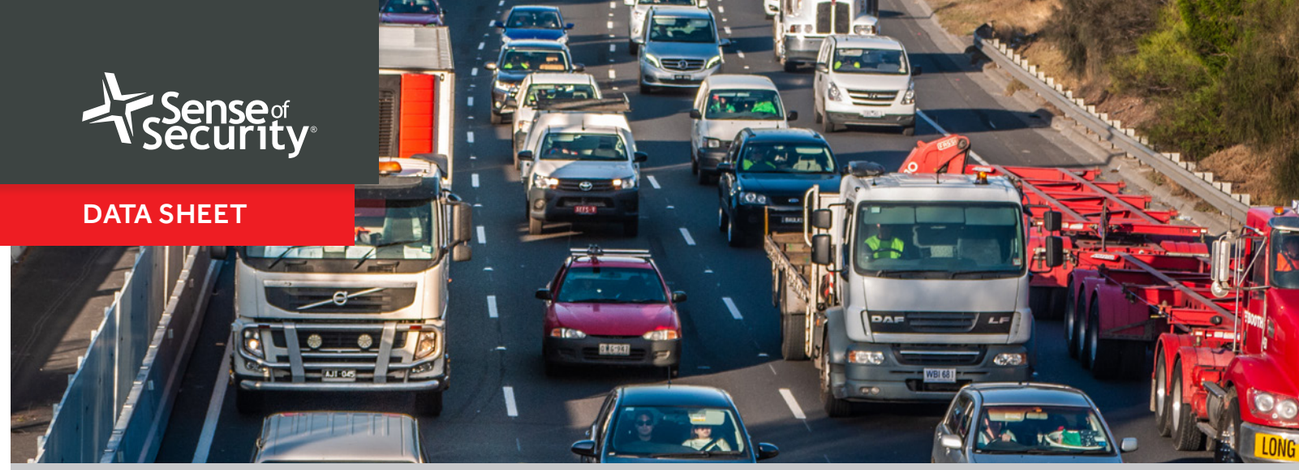
DATA SHEET



Denial of Service testing services

In recent times, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks have continued to gain media attention. High profile organisations are coming under attack, globally, regionally and locally, across the spectrum of Government, large corporates and any entity being hosted on cloud platforms.

DDoS is now considered one of the primary threat types facing every industry and business that is exposed to the public Internet.

Denial of Service attacks have evolved from single-source (e.g. sending overwhelming volumes of email), which are relatively easily detected and defeated, to attacks that come from many thousands of compromised agents (bots) acting on behalf of threat actors.

DDoS testing service key benefits

- **Validate your DDoS defences** – make sure your investment in denial of service protection is being realised and proven to be within expectations.
- **Proactively avoid downtime** – peace of mind by preventing downtime from protection that may be sub-optimal or not to your requirements.
- **Test vendor SLA's** – ensure your vendor responds within agreed timeframes during a denial of service test exercise.
- **Detect configuration issues** – identify denial of service exposure at layers 3, 4 & 7 that can reveal configuration issues in your environment for improvement.
- **Train your team** – learn what it's like to respond to a real-world DDoS situation for better cyber resilience outcomes.

Who is exposed?

DDoS attacks are so easy to launch and so difficult to defend against that DDoS is now considered a common attack method for which all companies need an appropriate response.

All Cyber Resilience Programs should take into consideration the need for DDoS protection and appropriate testing to ensure effectiveness.

Business impact from DDoS

While traditional DDoS attacks have relied upon a single attack method, the pattern across recent attacks demonstrates the escalating use of advanced techniques to maximise disruption, indicating an overall increase in sophistication.

Australia's premier Cyber Resiliece, Information Security and Risk Management consulting practice.

For help and tailored assistance, call Sense of Security right now on

1300 922 923 or +61 (2) 9290 4444

info@senseofsecurity.com.au

senseofsecurity.com.au

The number and types of attack vectors around today is simply staggering. Organisations are susceptible to outages across the stack at multiple layers, from web applications to the platforms and networks delivering them.

Attackers are now using an array of changing attack methods; continually recalibrating attacks dynamically based on responsiveness of target systems and can also launch attacks from a range of sources distributed across the globe.

DDoS & cyber attacks

For the motivated attacker and cyber-criminal, DDoS is becoming a common tool in their arsenal, resulting in expensive downtime and disruption to legitimate business.

DDoS attacks are also often employed as diversions to other attack methods, because they generally redirect organisational focus to the disruption leaving other parts of the environment exposed and less likely to be monitored.

With more and more systems becoming internet-connected on a daily basis, hackers are building larger and larger networks of compromised endpoints (bot-nets). The Internet of Things phenomena has spurned the most popular growth area for bots, and not surprisingly the scale of the DDoS problem continues to escalate.

Why test market solutions?

There are a number of technical solutions in the market to assist organisations with identifying and responding to these types of attacks. Coverage of these solutions can be limited, because they're generally expensive offerings with costs increasing for the volume and types of attacks you need to protect against.

Solutions can include Telco/ISP bundled services, Cloud absorption, Content Delivery Networks (CDN), On-premise hardware and Hybrid models.

No matter what the technological approach is, testing and validating the level of protection you have employed is essential, because our experience indicates that you cannot always rely on vendor promises.

DDoS testing is designed to simulate DDoS attacks against your IT infrastructure in a controlled and planned manner to validate if your DDoS defences work as expected; and to allow you to anticipate how you'll respond during a genuine cyber-attack.

Our DDoS testing is a methodology designed to proactively validate the capability and coverage of your DDoS defence, and the service provider's or vendor offerings that you may have employed to mitigate such attacks.

Why choose Sense of Security?

Sense of Security is Australia's premier pure play Cyber Resiliece, Information Security and Risk Management consulting practice.

For over 18 years, SOS has provided expertise in governance & compliance, strategy & architecture through to risk assessment, technical assurance testing and training.

Experience and focus – our consultants are experienced security specialists with a business focus, creating security solutions that mitigate risk and maximise results.

Trusted advisors – major names in the Banking & Finance, Insurance, Healthcare, Retail, Service Provider sectors as well as Resources, Utilities & Telecommunications rely on Sense of Security. We also conduct business with Local, State and Federal governments.

Service offering

DDoS Services

- Advisory service to assist in target selection, test planning and execution
- Over 300 unique DDoS attacks, IPV4/6, HTTP, DNS, SSDP, NTP, IPSEC & more
- Real-time monitoring of performance of all targets and over 140 metrics collected
- Unlimited sources, unlimited attack sizes, vast array of attack vectors
- Control of the live DDoS test exercises in real-time.

Testing Coverage (non-exhaustive)

- Cloud DNS
- Cloud DDoS
- Content Delivery Network (CDN)
- Web Application Firewall (WAF)
- Firewall Testing
- IDS/IPS Testing
- SIP and VOIP Testing
- SMTP Testing
- DNS Server Testing
- Web Server Testing & Optimisation
- IPSEC and SSL VPN Testing
- DDoS Appliance Testing

Service Models

- Platform Access and Self-service
- Delivered-as-service by Sense of Security