According to a recent report, “In addition to new potential means for staging attacks, late 2018 saw the arrival of a various DDoS launch platforms which have made attacks with a capacity of over 420G a reality.”

- Advanced attacks will include diversionary, application layer, and multi-vector/ multi-layer, helping drive growth in the market throughout the forecast period as more businesses see the value in robust defense.
- Hybrid defense scenarios (single solutions that pair on-premises equipment with cloud services) will continue to grow and augment defense-in-depth scenarios (similar solution components from multiple vendors that are not integrated) as organizations seek to defend themselves against all vectors of DDoS attacks.

**Distributed Denial-of-Service (DDoS) Protection**

Validating your DDoS mitigation strategy is more than just flooding your security infrastructure with a ton of traffic to see what happens. CyberFlood, leveraging its unique and industry-leading architecture, combines both legitimate/normal traffic with DDoS attack traffic, emulating what happens in the real world. When validating DDoS protection, you need to confirm your DDoS solution can not only mitigate the DDoS attack, but also not inadvertently impact your legitimate users.

Statistics are provided within CyberFlood, in real-time, allowing you to interactively measure both user experience and security mitigation. With this capability, you now have full visibility into how your security infrastructure is performing. Need more scale or only DDoS traffic? CyberFlood offers attack-only and extreme scale test types allowing you to emulate large-scale DDoS attacks targeting large industry verticals and service providers.

**DDoS Categories—Volumetric & Protocol**

CyberFlood helps you validate today. Deploy your DDoS mitigation strategy at scale with multi-10G line-rate attacks, generating tens of million of packets-per-second. Confirm legitimate user traffic is not inadvertently impacted by your DDoS protection, all of which is measured accurately by CyberFlood within one single test methodology. Maximize network uptime, minimize costly service disruptions and customer churn using our solutions, which include:

- Scalable DDoS capability
- Vast attack coverage
- Simple to set up and execute tests
- Huge scale and performance to push any device to its limits

Spirent CyberFlood
DDoS | Applications and Security Test Solutions

Spirent Services
Spirent Global Services provides a variety of professional services, support services and education services—all focused on helping customers meet their complex testing and service assurance requirements.

For more information, visit the Global Services website at www.spirent.com or contact your Spirent sales representative.

Attack Samples
- Internet Control Message Protocol (ICMP)
- User Datagram Protocol (UDP)
- Spoofed IP
- Malformed IP
- Malformed UDP
- Malformed ICMP floods
- Ping of death
- Synflood (millions-per-second)
- Smurf attack

Volumetric: As the most common type of DDoS attack, volumetric assaults are relatively easy to deploy via botnets which can overwhelm a website and/or infrastructure with minimal experience on the attack-side.

Protocol: Many protocols such as DNS were designed long before DDoS attacks emerged, when networking was fairly straightforward with terrestrial, rudimentary hardware in place. Since then, popular network protocols like DNS have been shown to be vulnerable to DDoS abuse. As a consequence, developers and administrators are challenged to manage real-world exposure and vulnerabilities that can be punishing if gone untested.

DDoS Test Types

One-armed DDoS (Client only)
Targeting Real Services: Create advanced tests with a mixture of DDoS and legitimate traffic to test the efficacy of mitigation policies and its impact on non-attack user traffic. Percentages of attack vs. normal traffic can quickly be adjusted to find the exact point where security services impact application performance and access.

AssaultMode™ DDoS for Multi-10G

Ordering Information

<table>
<thead>
<tr>
<th>Description</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyberflood Base License for C100</td>
<td>CF-SW-BASE</td>
</tr>
<tr>
<td>Cyberflood Volumetric DDoS Suite</td>
<td>CF-SW-DDOS</td>
</tr>
<tr>
<td>Cyberflood Protocol DDoS</td>
<td>CF-SW-PDDOS</td>
</tr>
<tr>
<td>Cyberflood Global IP Traffic Selector-1YR</td>
<td>CF-SW-IANA-1YR</td>
</tr>
</tbody>
</table>

Other CyberFlood options are available for specific hardware platforms and Advanced Fuzzing options, please contact Spirent sales for more information.