Global Secure Layer

DDoS Protection

When Milliseconds Matter

Our Solution - Goliath

Distributed denial-of-service (DDoS) attacks are one of the most complex security challenges of the modern internet. At Global Secure Layer, we understand the magnitude of these attacks and the impact they can have on our customers if not mitigated quickly and efficiently.

Our patent-pending DDoS mitigation solution, Goliath, was built on the principle of detecting complex, multi-vector denial-of-service attacks with high precision, leveraging our global anycast network to share state intelligently across every site worldwide. Through rigorous engineering and research, we have developed some of the most cutting edge algorithms in the industry.

Our global protection currently stands at multi-terabits of mitigation capacity. With our expansive network reach, and strategic access to key networks, we are positioned to scrub large scale assaults as close to the source as possible. Our platform allows for rapid horizontal scaling capabilities, enabling us to keep pace with the ever-evolving attack landscape.

When it comes to protecting your network, milliseconds matter.

DDoS key features

Inline and automated
Goliath operates inline at the network edge - detecting and mitigating attacks in real-time. Our inline protection exceeds offsite mitigation architectures as it ensure all packets that enter our secure network are analysed with precision, guaranteeing only legitimate traffic reaches its destination with no added latency.

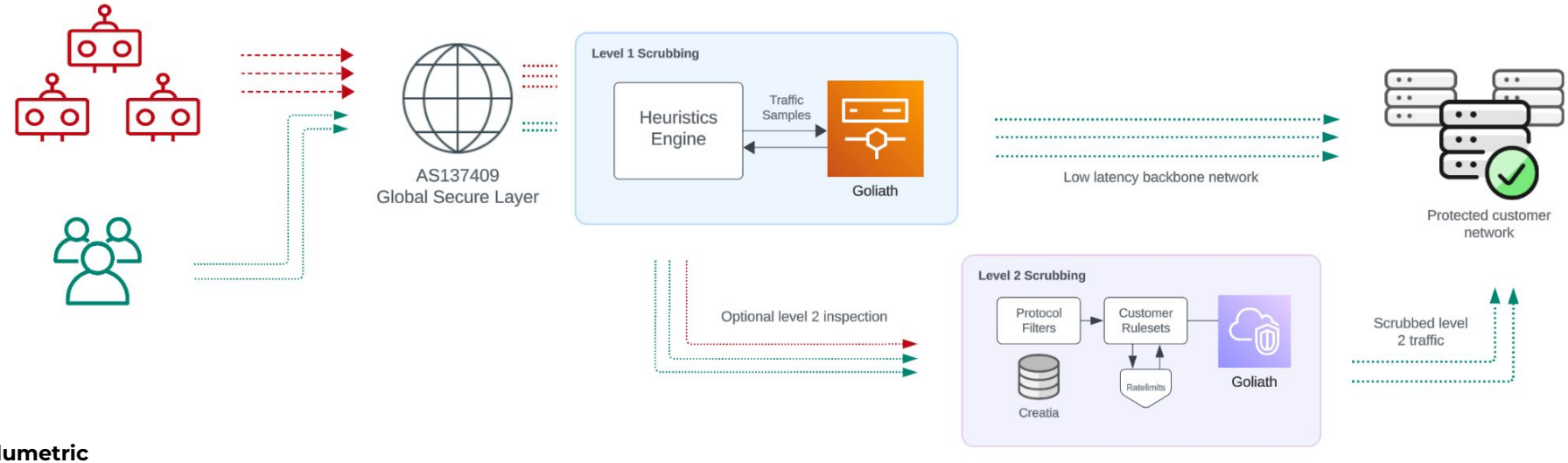
Baseline Traffic Profiling
Our DDoS mitigation establishes a baseline traffic profile, by sampling every packet at the appliance level in real time, and once sampled, features within those packets are further extracted and profiled for baseline usage for surgical blocking of specific vectors. For instance, a sharp increase in source port reflection allows for blocking of zero days with **no manual intervention**.

Stateful Filtering
Customers who have elected their prefixes for SYN proxy benefit from a fully stateful inspection across our entire global network. When a prefix is placed in this state, all TCP connections are tracked in real time and marked as solicited or unsolicited at the appliance level. This allows for incredibly fine grained filtering even when egress traffic is not served through our network.

Time to mitigate
Goliath offers one of the lowest time to mitigate in the industry at **50ms or less** with a guaranteed 200ms worldwide propagation.

Learn once, block everywhere (LOBE)
Our patent-pending DDoS algorithms use a unique shared messaging architecture where a threat learned in one site is known to all within 200ms. This allows for a uniform and consistent mitigation experience worldwide, no matter which sites you are present in with GSL.

Mitigation engineers
Global Secure Layer has a dedicated NOC providing 24/7 assistance. Our team of industry-leading mitigation engineers are always available to assist you with specific attacks, from provisioning and writing of rulesets to best practices regarding Level 1 settings.



Volumetric

Global Secure Layer has focused on building our own international network to ensure we have the necessary border capacity and interconnectivity required for absorbing and filtering large volumetric attack traffic.

The goal of volumetric attacks is to flood the victim with enough malicious traffic to impact legitimate traffic.

While these attacks are more common, the size of volumetric attacks can quickly saturate interconnections if sufficient port capacity isn't available. This highlights the benefit of our highly distributed DDoS mitigation architecture, as malicious traffic is inspected and scrubbed as close to the source as possible.

Zero days are effortlessly mitigated as well due to our appliance level heuristics engine, which samples per-destination packet features in real-time.

Reflective & Amplification

Reflective and amplification attacks leverage a small amount of traffic from a spoofable source, which is then amplified towards unsuspecting servers and reflected towards a victim's infrastructure. This often results in a produced response much greater than the initial request.

One such example of this vector is 'Memcached', which targets port 11211 and, and results in an overwhelming amplification factor of up to 51,200x the original request size.

While simple to execute, the volume of these attacks are staggering, as a threat actor generating 10 byte responses on a commodity server can easily overwhelm the edge port capacity of large enterprise networks.

Resource Exhaustive

These types of DDoS attacks are an attack on the protocol level, which aim to overwhelm system resources, particularly exploiting how OS network stacks handle of out-of-state TCP traffic.

When executed correctly, these attacks can easily choke a customer's network or infrastructure. Our patented stateful challenge-response approach ensures that only clean, stateful traffic reaches your protected network.

Our TCP mitigation was designed under the premise where attackers continue to evolve and adapt in ensuring their attacks resemble as closely to legitimate traffic as possible. In an environment where attackers are evolving, defences must equally be on the forefront of innovation as well.

Application Specific

Application (layer 7) specific attacks, while similar to resource exhaustive attacks, target unique and often undisclosed vulnerabilities in the end application.

Our unified management portal, Creatia, allows for end customers and the SoC team to impose payload matching BPF rulesets, which are executed just before the customer handoff. This allows for swift reaction and response to novel application-specific attack vectors, where traditional layer 4 scrubbing methods are infeasible.

BPF rulesets can be executed in a linear chain, where the highest priority rules are executed first, with rate-limiting optional where tolerance is needed.

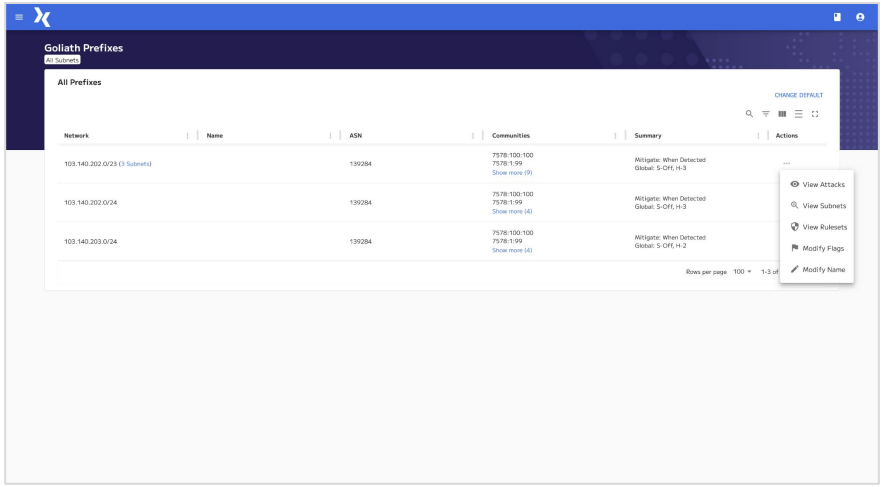
Security coverage

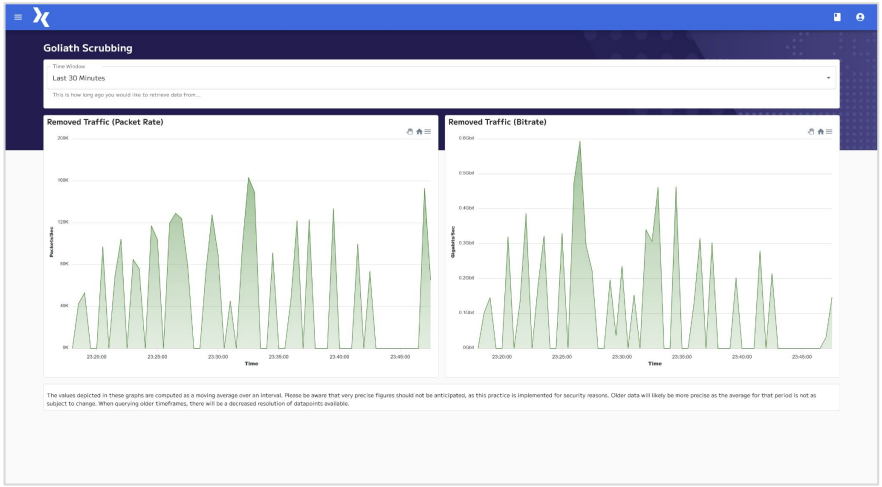
ATTACK COVERAGE			
Volumetric Coverage	**Reflective & Amplification**	**Resource Exhaustion**	**Protocol Specific**

• TCP Floods
  ○ ACK (+in-session)
  ○ PSH (+in-session)
  ○ SYN
  ○ RST
• UDP Floods
• IP Fragmentation
• ICMP Flood
  ○ Ping of Death
  ○ TTL exceeded
	• NTP Amplification
	• SSDP/UPnP
	• SNMP
	• Chargen
	• Smurf
	• Fraggle attack DNS
	• DNS Amplification
	• LDAP
	• RIP
	• TFTP
	• Memcached
		• Malformed & truncated packets
		• IP fragmentation
		• Invalid TCP segment ID's
		• Bad Checksums
		• Illegal TCP/UDP flags
		• Invalid TCP/UDP ports
		• Reserved IP address
			• A2S source Flood
			• A2S GETSUM
			• FiveM Exhaustion
			• RTFM Request
			• TS3INIT
			• NetBIOS
			• RakNet
			  ○ FiveM
			  ○ Rust
			  ○ Minecraft

Real-time protection in action

Inquire today about Creatia, our unified self service portal for all resource management and protection needs





Sean Aikins
Sales Director

Email: sean@globalsecurelayer.com
Phone: +61 459 469 489