Global Cyber Attack Mitigation

Defending at the Point of Attack

Attacks against the internet continue to grow in impact and sophistication. The National Institute of Standards and Technology (NIST) noted in their publication 800-189, “Large-scale distributed denial-of-service (DDoS) attacks on servers using spoofed internet protocol (IP) addresses and reflection-amplification in the data plane have also been frequent, resulting in significant disruption of services and damages.” Attackers have been using DDoS methods for decades, but attacks are larger and more prevalent than ever. In 2008, one of the largest DDoS attacks to date was a few tens of megabits per second[1], while modern day attacks are as large as several hundred gigabits per second (Gbps). Globally, there was a 776% growth in attacks between 100 Gbps and 400 Gbps from 2018 to 2019, and the total number of DDoS attacks is expected to nearly double from 7.9 million in 2018 to 15.4 million by 2023[2]. This increase in attack bandwidth and volume, along with increasing attack vectors with the use of vulnerable Internet of Things (IoT) devices, leave federal agencies and organizations at risk of compromised mission-critical services, loss of sensitive data, and financial damage. SAIC’s Global Cyber Attack Mitigation (GCAM) is an as-a-service offering that stops DDoS attacks immediately near the point of attack with exceptional reliability proven over decades.

1 https://www.dhs.gov/sites/default/files/publications/FactSheet DDoSD FINAL 508 OCC Cleared.pdf

2 https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

SAIC®

GCAM HAS SUCCESSFULLY MITIGATED SOME OF THE LARGEST DDOS ATTACKS EVER SEEN ON THE INTERNET FOR OVER TWO DECADES WITHOUT FAILURE.

Capability Highlights

- Unparalleled stability and reliability are demonstrated by over 20 years in operation. GCAM has never failed to mitigate a DDoS attack and continues to announce DNS.
- GCAM is delivered as a service with no new hardware, software, or license investments.
- GCAM defends against emerging DNS-based attacks, including HTTPS DNS and other attacks designed to steal certificates by using fragmented packets.
- The speed and performance of GCAM surpasses that of any other DNS system, answering DNS requests in less than a millisecond, even in the midst of a DDoS attack.
- GCAM eliminates the need for cumbersome filters, the need to pay for surge bandwidth, and the need for surge response teams.
- Operations are automated for Domain Name System Security Extensions (DNSSEC) roll-overs for lower labor cost.
- Customers are able to keep existing DNS systems until satisfied with GCAM's performance.

PROVEN PERFORMANCE

Our as-a-service solution has proven itself in some of the internet's largest DDoS attacks, including the 2016 DNS attack against Dyn that brought down DNS across the U.S. During this attack, our technology helped keep the Internet in the U.S. up and running. In addition to mitigating large DDoS attacks, it also blocks smaller, targeted DNS-based attacks like the recent DNS-based attacks that exploit DNS over HTTP. In every case, GCAM blocked the attack without failure, and our clients were not affected. In one instance, a DDoS attack occurred on July 8, 2019. This zero-day attack went undetected by traditional systems, but was detected by SAIC's GCAM.

SAIC partners with Cyber Defense Networking Solutions, the premier global DNS and cybersecurity products provider, to deliver proven DDoS mitigation using a global set of DNS nodes. SAIC has a unique approach to defending against DDoS and other types of DNS-based cyberattacks. Unlike other technologies that filter or absorb the attack, GCAM stops the attack at the point of the DNS request so it never reaches the client and doesn't impact client operations. Users never see the attack, their systems continue to operate and remain available, and they don't experience the latency issues associated with traditional DDoS mitigation approaches.

GCAM uses a robust, military-grade custom platform with the potential to hold every resource record of today's growing internet. The architecture is comprised of DNS nodes placed in countries across the globe in an anycast cloud. Each node has at least two hardened servers that use SAIC's Adaptive Mitigation Algorithm. In a millisecond or less, the algorithm determines if the request is malicious, and if it is, the DNS node simply doesn't answer the DNS request, mitigating the attack. GCAM not only allows you to defend forward; it does so with unmatched reliability. The algorithm is over 99% accurate, and SAIC offers "seven nines" SLA uptime for our integrated DNS service. This technology is also the fastest available so we can reduce DNS latency, sometimes by orders of magnitude. It is used in 48 countries and more than 60 locations, handling more than 200 thousand transactions per second – or more than 17 billion per day.

SAIC is the only American company using this technology, and we quickly deliver this capability to clients as a service. SAIC tailors the solution to conduct DNS operations and protect client information for government organizations or American-based companies with security requirements at the unclassified and classified level. GCAM can support the largest top-level domains (TLD), like .gov, or a single client's domains and subdomains. GCAM has an extremely low risk for implementation, and it does not require the client to purchase any hardware, software or licenses. Our capability is sold as-a-service so clients can start using the capability immediately while continuing to operate their legacy systems. Because of the speed of the GCAM system, our DNS nodes will respond faster than legacy systems, and quickly and seamlessly become your primary source for DNS and protection.

Contact

Russell Smith
703.676.4398
russell.j.smith@saic.com

Nancy Wright Grady, PhD
865.604.6733
nancy.w.grady@saic.com

Arthur Wachdorf
210.789.0707
arthur.l.wachdorf@saic.com

21-0587