JOINT SOLUTION BRIEF

Stop Automated Bot Attacks With Gigamon and Cequence Security ASP

The Challenge

Deployed in either the cloud or the datacenter, organizations public-facing applications are under attack by malicious bot networks intent on committing fraud, through account takeovers, fake account creation and API abuse. Most problematic is that the attacks are difficult to detect because each transaction looks legitimate.

Integrated Solution

The Cequence Application Security Platform (ASP) uses machine learning and heuristics to classify whether traffic is legitimate or from an automated bot. Malicious bot traffic can be mitigated based on policy, or it can be offloaded for enforcement or added analysis. The Gigamon Visibility and Analytics Fabric™ (VAF) speeds deployments and simplifies operations of the Cequence Application Security Platform.

Joint Solution Benefits

- Delivers all network traffic — including east-west data center traffic and private and public cloud workloads — to tools so all traffic can be monitored and analyzed together
- Detects automated attack patterns without cumbersome JavaScript instrumentation or mobile SDK integration requirements
- Protects web and mobile applications and their associated APIs by enabling you to block, deceive or isolate malicious traffic
- Sends relevant traffic — or relevant sessions — to the connected tools, so Cequence ASP doesn't become overloaded with irrelevant traffic
- Splits overly-large traffic volumes across multiple tools, while keeping sessions together

Introduction

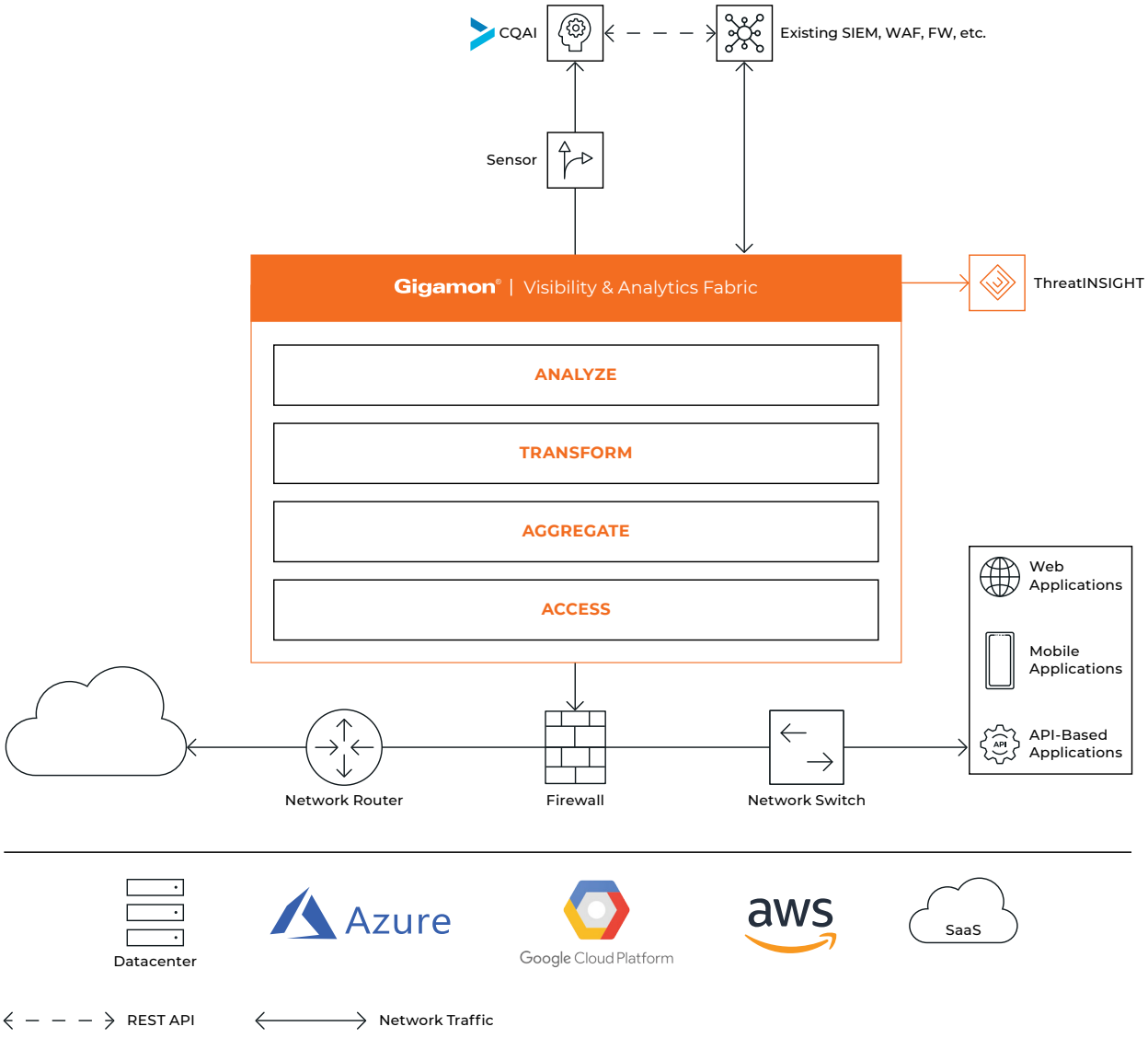
Stolen credentials, attack toolkits, and compromised infrastructure have made it easy for bad actors to launch account takeovers and business logic abuse against your public facing applications. Often times, bad actors will discover and launch their attacks directly against your exposed APIs, bypassing the web form or mobile application completely. These attacks are syntactically correct, and not easily stopped by WAFs or other network security appliances, leading to fraud, business interruption, or loss of sensitive data.

The Cequence Application Security Platform is designed to protect your web and mobile applications along with their associated APIs from automated attacks, application business logic abuse and vulnerability exploits.

The Gigamon-Cequence ASP Joint Solution

Key Gigamon Visibility and Analytics Fabric (VAF) features that enhance the Cequence ASP include:

- **Easy access to traffic from physical and virtual networks:** The VAF manages and delivers all network traffic — including east-west data center traffic and private and public cloud workloads — to tools so all traffic can be monitored and analyzed together, reducing blind spots, increasing the likelihood of spotting suspicious behavior and removing the need to learn a new set of tooling for virtual environments.
- **Load balancing to spread traffic across multiple devices:** When traffic volumes are larger than a single tool can cope with, the VAF can split the traffic across multiple tools, while ensuring sessions are kept together. Additionally, tool numbers can be incrementally grown by adding new devices to those already connected.
- **Traffic filtering:** The VAF can be configured to only send relevant traffic — or relevant sessions — to the connected tools, so Cequence ASP tools don't become overloaded with irrelevant traffic.
- **Aggregation to maximize tool use:** The VAF can aggregate traffic from multiple network links together before sending them to one or more Cequence ASP tool instances to maximize tool utilization. By tagging the traffic, the VAF ensures the source of traffic can be identified.
- **Aggregation to manage LAG and asymmetric routing:** Most security devices require that all the packets in a session be inspected by the same device since incomplete sessions risk being blocked. The VAF provides an intelligent and efficient way to help ensure packets from the same session are forwarded to the same tool enabling effective inspection in any architecture.
- **SSL/TLS decryption:** The VAF is used to decrypt TLS encrypted traffic (including TLS 1.3) for inspection by security tools and any other devices that need to inspect the payload.
- **Masking for data security/compliance:** The VAF can mask sensitive, private, or confidential data within packets before they're sent to other tools, where they could be seen by unauthorized people.



For more information on Gigamon and Cequence visit: www.gigamon.com and www.cequence.ai.

Gigamon®
Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com