CASE STUDY

Federal Agency Turns to SAIC for Cybersecurity Resiliency

AT A GLANCE

Challenge

SAIC's client, a large U.S. federal agency, required a reliable inline security tool architecture.

Gigamon Solution

- Two GigaVUE-HC2 Series visibility nodes providing:
- Inline bypass to remove tools as single points of failure
- Traffic capture, filtering
- Automatic load balancing across security tools

Customer Benefits

- Force all traffic through the security stack
- Continuous network uptime in the event of an inline security tool failure
- Avoided using SPAN ports for traffic capture, reducing complexity while optimizing tool performance
- Streamlined network operations, auditing and maintenance

Challenges

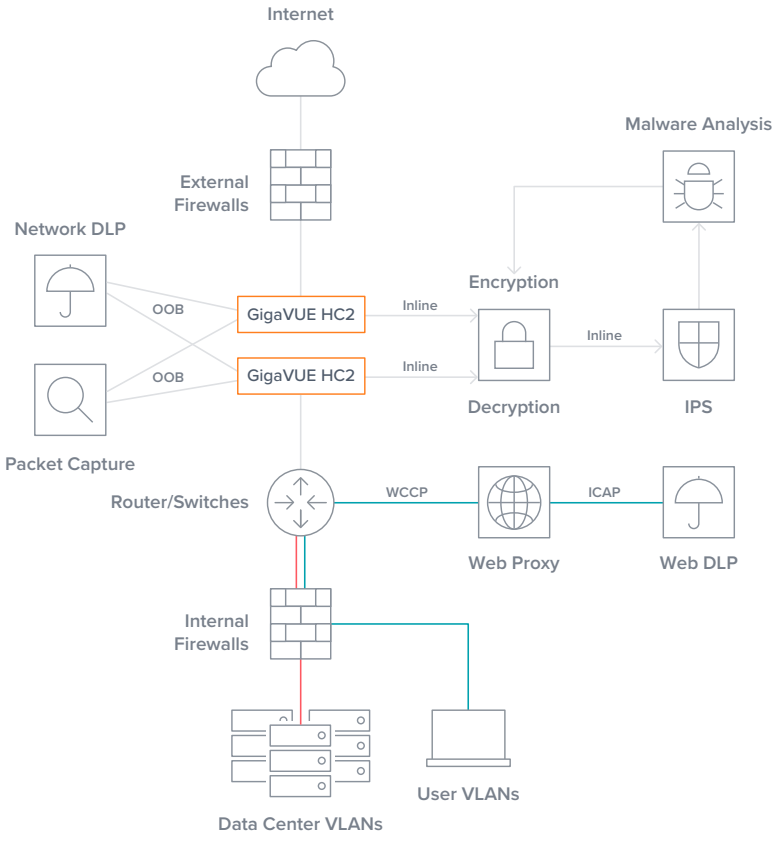
A large U.S. federal agency brought in SAIC (Science Applications International Corporation) to assess — and revamp — the agency's aged network security infrastructure.

"The network was lacking many security capabilities. The agency's security posture was heavily relying on VLANs, signature-based Intrusion Detection Systems (IDS), and traditional firewalls that had reached end-of-life. The infrastructure design made it difficult to introduce new security tools such as data loss prevention (DLP) or an advanced intrusion prevention system (IPS)," says Chris R., Security Engineer at SAIC.

Reliability Objections to Inline Security Architectures

The team's initial thought was to connect new security tools using a mirror or SPAN (switch port analyzer) ports off network switches. "SPAN ports can drop packets, making them unreliable to capture everything that is happening — and you cannot enable blocking on the security tools since they are just passively monitoring or receiving copies of the live packets," says Chris R.

Switching to an inline security architecture would help immensely and force all production traffic through the security tools, the SAIC team thought. But they needed a way to answer the agency's performance and reliability concerns about inline architectures. Luckily, a Gigamon demonstration gave the team the knowledge and confidence they needed to push forward with a network packet broker.



Solution

The SAIC team completely overhauled the agency's security infrastructure by redesigning it with two inline GigaVUE-HC2 visibility nodes with Inline Bypass capabilities. The nodes sit between the perimeter firewall and the internal firewall, sending all traffic through a modernized security stack that decrypts and inspects packets before it can pass into or out of the network.

Easy, Efficient Operations

Features in the Gigamon Visibility and Analytics Fabric such as Flow Mapping® improved the network's overall speed by automatically filtering out traffic that didn't merit decryption or inspection by the security stack.

The Gigamon solution also helped reduce the infrastructure's complexity, leading to more straightforward operation for the agency. "The new architecture makes it very easy to explain to people how everything is set up," says Chris R. "And we do not have taps hanging off ports that are not managed by our team, which would have complicated things quite a bit. Also, from a troubleshooting standpoint, it is now quick and easy to identify where an issue may be occurring."

"Adding new tools to the network is a snap. When testing proof-of-concept (PoC) products, we can easily insert the tool off Gigamon either inline or out-of-band depending on our client's requirements and the tool's purpose. Upgrading or changing the infrastructure is easier now, too. Gigamon allows us to singlehandedly manage the security toolchain ourselves without involving other teams, and without affecting production traffic," says Chris R.

Resilient Fail-Over

The two GigaVUE-HC2 appliances afforded an extra level of redundancy in case one should fail. A feature called Gigamon Resilient Inline Protection (GRIP) let the SAIC team place the second GigaVUE-HC2 inline with the first.

GRIP allows the two units to switch in or out on the fly dynamically. In the unlikely event that the first unit suddenly fails, the other node can seamlessly step in to shoulder the full load. Testing showed the fail-over process to be unnoticeable to users or operators.

"We've automated as much as we can," says Chris R. "If something were to happen at 2 a.m. with Gigamon, the GRIP configuration seamlessly allows the secondary unit to become the primary. If a tool hanging off the HC2 stops responding, the HC2 will automatically bypass it and take it out of the load-balanced traffic path where applicable. The logs are forwarded to the Security Information and Event Management (SIEM) to inform the administrators of the issue and an email notification is sent out from the system. And to users, it's completely transparent."

From Old-Fashioned to Cutting Edge

Thanks to intensive planning, careful implementation and solid technology and support from Gigamon, the SAIC team managed to bring the federal agency's outdated infrastructure up to modern standards while addressing the agency's prior misgivings about inline tool configurations. The project has been a great success from the agency's point of view, so now the SAIC team can put another checkmark in the win column.

About Gigamon

Gigamon is the first company to deliver unified network visibility and analytics on all data-in-transit, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation. In short, we enable you to run fast, stay secure and innovate. Gigamon has been awarded over 75 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations, including 10 of the top 10 federal agencies. Headquartered in Silicon Valley, Gigamon operates globally. For the full story on how Gigamon can help you, please visit www.gigamon.com.

Gigamon®

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