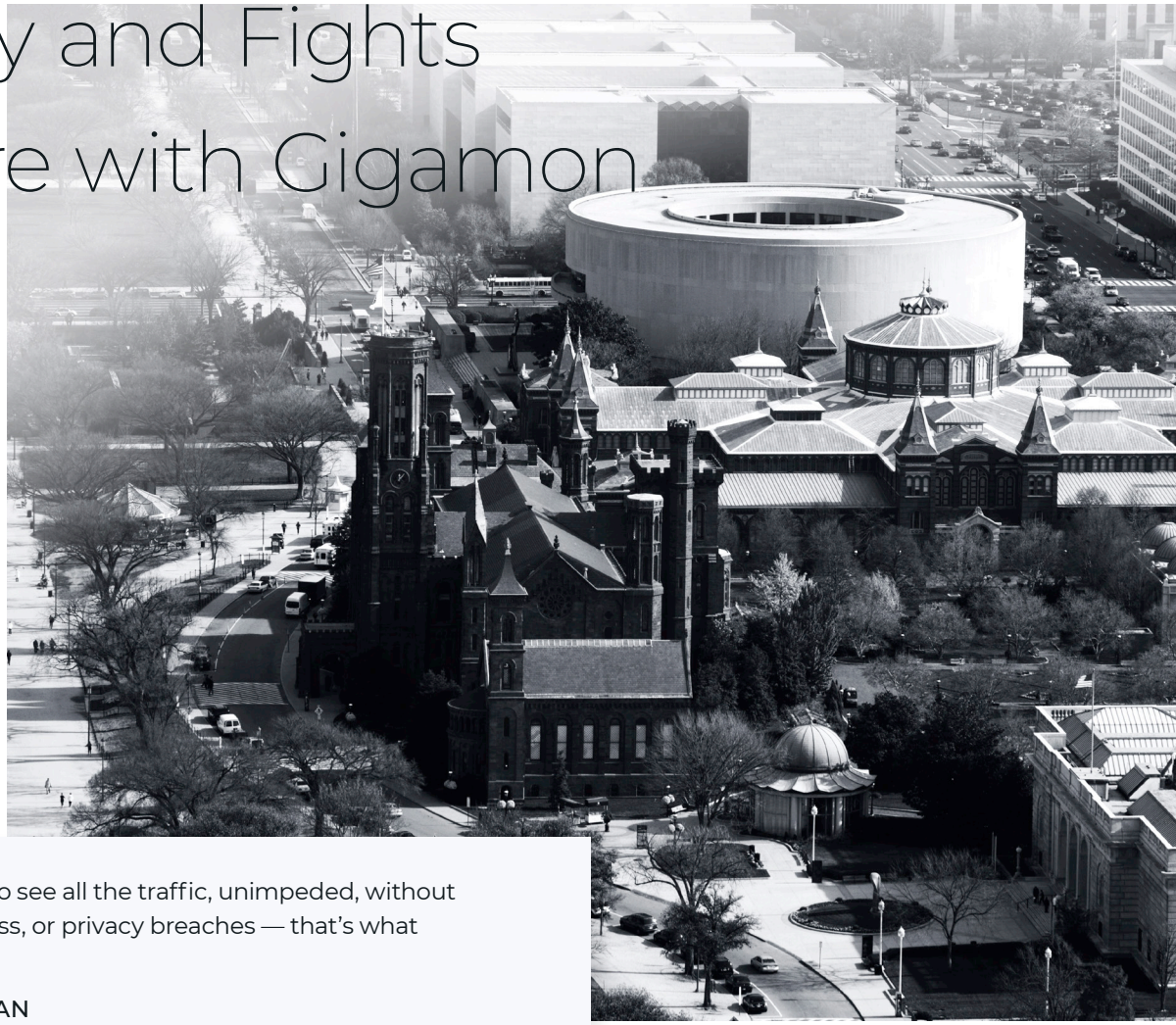
The Smithsonian Institution Improves Visibility and Fights Malware with Gigamon



> When you want to see all the traffic, unimpeded, without any risk of data loss, or privacy breaches — that's what Gigamon offers."

MARTIN BECKMAN
Director of Information Technology Engineering and Plans at the Smithsonian Institution

CHALLENGES

The Smithsonian Institution needed a way to passively monitor network traffic, feeding a myriad of tools, all without slowing down traffic or opening up an avenue of attack.

SOLUTION

Two Gigamon® GigaVUE-HC2 nodes

CUSTOMER BENEFITS

+ Gain reliable access to data
+ Prevent tools from being overwhelmed with traffic
+ Successfully troubleshoot network data
+ Maximize network visibility and performance monitoring

The Smithsonian Institution is a unique American treasure, comprising 19 museums and the National Zoo in Washington, D.C. With 6,300 employees, it's a large size by most standards, though relatively small in the world of other very large organizations also within the U.S. Federal government. In addition to all the threats common to Federal agencies, like malware attacks, the Smithsonian must also deal with fairly unique requirements. For instance, unlike most organizations within the government, the Smithsonian runs a payment infrastructure on its own network so that it can accept credit cards at snack bars and gift shops.

For Martin Beckman, Director of Information Technology Engineering and Plans, total visibility into the Smithsonian's network is absolutely key to smooth operations. Having cut his teeth at the FBI and the Pentagon, he brought the gospel of visibility to the Smithsonian. He rattles off the list of things network operations needs to know: "Why do things not work? Why do things break? What port is this crazy application on? What you don't know is what's going to destroy your network and your IT infrastructure."

Beckman had used the Gigamon Visibility and Analytics Fabric™ at his previous Federal assignments, and had come to respect that value Gigamon delivered. "For a corporate or large government operation where you're tracking all the traffic and dumping it into one spot, Gigamon does the work of five people," he says. He became an evangelist for Gigamon once he arrived at the Smithsonian.

SOLUTION

The Smithsonian Institution deploys two GigaVUE®-HC2 nodes, with NetFlow accompanying them. The GigaVUE-HC2s are tapped into the traffic north and south of the primary firewalls.

"A TAP takes a port from my box, and also leaves you pushing around on the backbone of the network," explains Beckman. "I like to use Gigamon nodes in pairs: tap the fiber, watch the traffic and put a pair of switches behind it. Then put all your appliances on the switch."

The appliances passively monitor all that traffic, using a variety of tools that Beckman and his staff are comfortable with. "Most people don't understand that Gigamon is not the device that does the analysis," he says. "It's the device that lets you attach all those devices, and passively grab that traffic. Gigamon doesn't provide the solution; it provides the means of making the solution work."

DO YOU SEE WHAT WE SEE?

With the Gigamon Visibility and Analytics Fabric deployed, Beckman says he has the visibility he needs to meet a number of threats:

+ **Malware:** "People don't watch what's going on inside their network," he says. "If you have malware on an end-user device, it can actually set up a two-way stream — a stream from a trusted host into the datacenter, and that trusted host, which is now compromised, back through a VPN through the firewall."
+ **Attacks on payment infrastructure:** "If somebody tries to maintain a session with one of your PCI-compliant servers that collects credit card information, you know what certain traffic looks like and what it doesn't look like," he explains. "Anything that's outside the boundaries is what you capture."
+ **Ransomware:** As part of the federal government, the Smithsonian Institution is a malware target — and Beckman has eyes on that too. "A SIP Trunk is an elegant way to hack, and we're seeing it now: ransomware being brought in over VoIP sessions via SIP," he says. "You can pick that up just watching the traffic go by."

And it's particularly important that Gigamon can monitor all this traffic passively. "Otherwise, you wreck latency and bandwidth, and the box itself that's tracking becomes a target for a hacker," Beckman says.

AFTER THE RETURN, PLANS FOR THE FUTURE

At the moment, the Gigamon Visibility and Analytics Fabric is helping keep the Smithsonian network afloat as its staff works almost entirely from home during the coronavirus pandemic. But once he's back in the office, Beckman has some ideas on where he wants to go.

"Before COVID hit, we were about to look at going into the East-West traffic, which is difficult due to the topology, and we wanted to get the additional deduping licenses and a license for SSL/TLS Decryption," he says. "Now we're working remotely and I can't set that up — working on a datacenter from home is like scuba diving down in the Titanic — but it's on the horizon."

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 80 percent of the Fortune 100. 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