Ovum
TMT intelligence | informa

Gigamon offers a "next-generation" network packet broker for security

Publication Date: 06 Jul 2018 | Product code: INT003-000194

Rik Turner

Ovum view

Summary

Network packet broker (NPB) vendor Gigamon is doubling down on security. It is positioning its network visibility devices as traffic monitors that see activity in any network (on-premises, virtual, or in the public cloud) and forward it to the appropriate security tools for further investigation. It has been adding functionality to enhance its NPBs' suitability for use in security, all of which has led it to proclaim its "next-generation" status.

Gigamon started life in network and application monitoring

Gigamon was founded in 2004 as a developer of NPB technology, operating originally as Gigamon Systems LLC. The company went public on the NYSE in June 2013 and, after four years as a listed company, went private again in December 2017. It was acquired for $1.6bn by Evergreen Coast Capital, the private equity arm of Elliott Management Corporation.

Paul Hooper has been Gigamon's CEO since December 2012. He joined the company the previous year as its VP of Marketing, having previously held executive positions at Extreme Networks. The company's CTO is Shehzad Merchant, who joined in that capacity in 2013, having previously been CTO at Extreme Networks.

Gigamon has pivoted to focus on security

Having built a business providing technology for network and application performance management (NPM and APM) for over a decade, Gigamon moved toward the security sector in 2015. This has involved endowing its GigaVUE visibility appliances (such as NPBs) with additional features and functions specifically for this new remit. These include:

- Decryption of SSL-encrypted traffic so that it can be inspected, then re-encrypted for its onward journey, if deemed legitimate. This feature was initially delivered as an out-of-band capability in 2016, and was enhanced to inline capability in February 2017. In December 2017 the company added another physical module, extending the inline capability with support for 100Gbps networks, and the actual decryption activity was offloaded to specialist Cavium hardware.
- The ability to forward metadata (about network traffic seen by the NPBs) to a security incident and event management (SIEM) platform. GigaVUE can export the information in NetFlow, IPFIX, ArcSight's Common Event Format (CEF), and IBM QRadar's Log Event Extended Format (LEEF). Data can be forwarded to all the leading SIEM solutions (Splunk, QRadar, and ArcSight), as well as the Phantom orchestration and automation tool, which is now part of Splunk. Integrations for Splunk, Phantom, and QRadar are now available.
- Application session filtering, which now spans everything from the handshake to the end of the session, taking the analytical capability beyond the packets.
- Metadata engines that incorporate the response codes for HTTP traffic and the cryptographic algorithms for HTTPS.

- APIs that enable Gigamon to offer apps in the app stores and marketplaces of Splunk, QRadar, and Phantom, so that customers can see data from the NPBs on those other platforms.

Incorporating the new functionality with the GigaVUE technology has resulted in Gigamon's GigaSECURE Security Delivery Platform. The company describes it as a "next-generation" NPB that enables companies to scale security tools, prevent tool sprawl, and contain costs.

Inline bypass enables more efficient security routing

The "next-generation" NPB claims are underpinned by the so-called "inline bypass" model. This is a network design where the typical concatenation of security tools, such as an intrusion prevention system (IPS), a web application firewall (WAF), and advanced threat protection (ATP), with the traffic proceeding serially through them all, is replaced with one where a Gigamon visibility node becomes a hub, connected to each of the security devices individually.

Traffic is sent first to that hub, which centralizes the network traffic analysis function and "trombones" out to the disparate tools with only the relevant parts. In a hub-and-spoke topology with a Gigamon device in the center, for instance, non-web and video traffic need not go through a WAF, while email traffic should go through both the IPS and ATP.

This approach enables traffic to be routed more efficiently than the serial chaining of the security tools. It also makes it possible for companies to maximize the capabilities of their existing security tools prior to expanding their capacity to handle increasing traffic volumes.

Why Gigamon should be on your radar for security

With the threat landscape in continual evolution, and the inevitability of security incidents and breaches, the ability to inspect network packets (including the encrypted traffic) is a major requirement if companies are to detect when attackers and malware are in their infrastructures. This capability offered by Gigamon, when added to its ability to promote more efficient use of existing security tools via the inline bypass architecture, makes it a compelling option for any security-focused network monitoring project.

Appendix

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum’s consulting team may be able to help you. For more information about Ovum’s consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum
TMT intelligence | informa

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo