REPORT REPRINT

Gigamon moves up the network security stack with ICEBRG acquisition

ERIC OGREN

26 JUL 2018

The company enters the network traffic analytics market with the acquisition of ICEBRG. The network security vendor can offer cloud-based analytic and threat detection services to enterprise and managed security service provider customers. The combined capability promises to allow security operations to automatically store copies of network traffic to review for threats.

Security operations centers have come to appreciate that network traffic, header and data packet content carries information that cannot be gleaned from log files yet is critical for quickly detecting active threats. The ability to draw security inferences from traffic analysis becomes increasingly important as the SOC requires visibility into cloud and colocated datacenter environments. Gigamon products are known for filtering and cleaning up network traffic, enabling third-party security and network performance products to be more productive. With the ICEBRG acquisition, Gigamon now has cloud-based data storage, analytics, detection and threat-hunting features that allow the vendor to become a full-fledged player in the growing network traffic analytics market segment.

THE 451 TAKE

Gigamon steps up into the network traffic analytics market with this acquisition of ICEBRG. The deal is significant for two reasons. One: the NTA market shows sustaining growth potential as SOCs enhance their tactics for detecting attacks. Once a threat uses the network, its footprints are visible to NTA. Network security is now integrating with the SOC to effectively detect and respond to security threats. Two: Gigamon extends its product line up the network security stack. No longer a low-level processor of network traffic, Gigamon leverages ICEBRG technology in offering a subscription NTA service for enterprises to detect modern attack tactics and react according to their incident response practices.

Gigamon has carved out more room to grow its business by offering security and network analytic packages, expanding sales channels by enabling customized services from managed security service providers to their subscribers and having a cloud-based architecture that can be leveraged for other security products.

DEAL DETAILS

Gigamon enters the NTA market with the acquisition of ICEBRG. The network security vendor can offer cloud-based analytic and threat detection services to enterprise and managed security service provider customers. The combined capability promises to allow security operations to automatically store copies of network traffic to review for threats that expose themselves as they use the wire to probe, replicate, communicate and exfiltrate sensitive data.

ICEBRG was founded in 2014 in Seattle. The company closed a $10m series A round in 2016, bringing its total investments to roughly $12.5m. We estimate Gigamon paid $100m, or about 20x ICEBRG's annual revenue.

Momentum Cyber advised ICEBRG and Goldman Sachs advised Gigamon.

TARGET PROFILE

ICEBRG features a cloud-based data system for receiving and analyzing metadata extracted from network traffic. Crowd-sourced detection algorithms and a custom query language allow security teams to customize network security queries of the data according to its own environment and ability to remediate.

The ability to leverage customer insights to rapidly contribute detection algorithms that can then be replicated across the Gigamon base is a key feature, allowing the vendor to stay up to date with ever-changing attack tactics and techniques.

ACQUIRER PROFILE

Gigamon was acquired in 2017 for $1.6bn by the Evergreen Coast Capital private equity practice, a subsidiary of Elliott Management.

Gigamon flagship products, GigaVUE and GigaSMART, are designed to collect copies of network traffic, efficiently remove undesirable data, and forward the extracted data to upstream security products for additional processing. These features are also available in the GigaSECURE Security Delivery Platform. By filtering traffic in a manageable location in the network security stack, Gigamon enhances the performance of downstream security inspection products, reduces data management costs and increases accuracy of security assessments.

COMPETITION

The NTA market is rapidly emerging as SOC teams realize that network data is a rich source of information that threats cannot modify. It can present actual evidence of interactions between on-premises assets and cloud-based computing assets and thus present a fertile data source for analytics to detect discontinuities in behavior that can indicate threat activity.

The appeal of an NTA service is that it relieves the SOC from having to administer collecting and processing network flows, new analytic algorithms are immediately applied to network traffic as they become available, and the SOC can still write custom detection algorithms and response interfaces. Large vendors such as Cisco, FireEye and Palo Alto are adopting the cloud-based NTA approach and noticeable traction follows ExtraHop Networks and Vectra Networks. We fully expect to see SaaS offerings based on Corelight with its open source Bro technology and Awake Security, Corvil, Darktrace and SecBI also evolving their NTA products.

We view the NTA market as complementary to security information and event management systems. The network can produce prodigious amounts of data, which is not great for SIEM pricing models and there is little need for long-term data management because network data rapidly loses its detection value after 30 days (e.g., the attack has probably run its course and the sensitive data is long gone by the 30-day mark).

Many of the major SIEM vendors have clients that consume network data in support of analytics and interactive queries. IBM QRadar has its roots in network behavior anomaly detection and its ability to combine network with log data analysis. Splunk Cloud aims to relieve customers of the need to manage clusters of servers, LogRythym CloudAI is a platform for artificial intelligence and machine learning, Securonix Cloud delivers application packages dependent on network visibility and AT&T/AlienVault may bring NTA to medium-sized businesses.

ACQUIRER
Gigamon

TARGET
ICEBRG

SUBSECTOR
Security

DEAL VALUE
Undisclosed

DATE ANNOUNCED
July 24, 2018

CLOSING DATE
July 24, 2018

ADVISERS
Momentum Cyber (ICEBRG) and Goldman Sachs (Gigamon)