Gigamon Acquires ICEBRG to Extend the Power of Network Traffic Analytics

Abstract

Gigamon has been known for years as a market leader in the network packet broker space, conquering the challenge of getting the right data to the right network and security tools. Over the last few years, Gigamon extended into the security space, which paved the way for their acquisition of ICEBRG. With ICEBRG, Gigamon has expanded its capabilities to help organizations use data better by delivering next-generation security analytics with all of the captured data. Now, in addition to giving network tools the visibility to increase network and application performance and giving security tools access to the traffic they need to process and act upon, Gigamon delivers further insights to combat threats.

With the ICEBRG acquisition and integration, Gigamon can capture network traffic metadata into a central platform that offers an API, a user-friendly query language, and built-in advanced security applications, transforming itself from a leading-edge network traffic company into a leading-edge cybersecurity company. Gigamon's vision is to transform not only the way it handles data, but the way cybersecurity teams operate by providing a rich, open-access network traffic analytics platform upon which multiple security applications can be deployed, whether such apps are developed by Gigamon, a customer, or a third-party partner.

Event

In its first acquisition, Gigamon selected ICEBRG, a network security startup founded in 2014 in Seattle, WA by former Microsoft and DoD experts. The ICEBRG platform is a scalable, cloud-based data repository designed to receive data from physical or virtual sensors. The sensors receive optimized network traffic from the Gigamon next-generation network packet broker (NGNPB) known as the GigaSECURE security delivery platform. The virtual sensors can also be deployed in a cloud environment.

What ICEBRG Brings to the Table

ICEBRG provides significant synergies with the Gigamon NGNPB solution and for its customers. First, it is a data collection and enrichment platform. It can store rich metadata based on the data Gigamon collects, enrich it, and make it available for any API-compatible tool. The platform provides incident response and forensics capabilities with fully documented API, which enables other tools and developers to access the enriched data and analytics for other tools like security automation, orchestration, and ticketing. Second, ICEBRG is an analytics platform designed to be a force multiplier for security operations teams. ICEBRG makes use of network data as the root of truth. The platform maintains a plethora of data, and makes the security analyst's job easier and faster by providing an easy-to-use GUI to organize the information as individual and related incidents across a consolidated set of capabilities. It also allows drilldown into event details and pivoting between data points to identify related cases. By providing enrichment and analysis, personnel of any skill level can get value from the capability and provide value to the organization.

The platform uses government-grade encryption for both data in transit and at rest. All provisioning is fully managed for data acquisition, storage, and analysis, and the platform optimizes bandwidth for sending the data to the cloud-based analysis engine in the platform. The platform additionally optimizes bandwidth utilization for data sent to cloud.

ICEBRG supports ingestion of full PCAP data on demand. It also integrates with the major open-source and for-purchase threat intelligence platforms to correlate internal activities with externally-observed threats. Once threats are identified, the platform categorizes them by severity and confidence level based on the volume, types, and age of the available data.

Gigamon vs. its Competitors

The solution seamlessly integrates with the current Gigamon data acquisition architecture and provides an easy-to-deploy virtual appliance to broaden capture and facilitate cloud environment analytics. The combination of data enrichment and analytics increases the value proposition of the Gigamon solution and simultaneously decreases the value of the competing solutions. When considering their options, prospects now have the option of upgrading from a standalone NGNPB solution to one with cloud data storage, analytics, and forensics features. The backend infrastructure for security analytics is maintained by ICEBRG, which enables customers to spend more time on securing their enterprise instead of building and managing extensive and complex security infrastructure.

Adding Value to Customers and Prospects

Within the ICEBRG platform, anonymized metadata is shared to increase the detection accuracy for all customers. External, crowd-sourced metadata is correlated with internal telemetry and threat feed intelligence for further enrichment and analysis, reducing what was already an extremely low false positive rate. Using its analysis engines, the platform merges multiple related but seemingly individual events into a single case to further reduce alert fatigue.

Rich real-time and historical searches across hundreds of terabytes of network data is very fast, with most searches having a sub-second response time. The search interface and results are delivered through an easy-to-use GUI, so even junior analysts can perform advanced functions. Security teams can pull numerous reports to communicate with peers and senior management about the status of incidents and provide legal teams with the data necessary to support law enforcement and other trial-related activities.

Whether an organization is a current Gigamon customer, trying to get more out of their existing NGNPB solution, or investigating an NGNPB, companies at every stage can benefit from the acquisition and integration of Gigamon and ICEBRG.

- ✓ **Customers with no analytics:** The combined strength and visibility makes this a no-brainer
- ✓ **Customers with analytics**: The benefit of a consolidated platform is most likely lower than the cost of maintaining and integrating separate security tools, but users can perform a trial to see which is better or more cost-effective.
- ✓ **Organizations in need of packet brokering and analytics:** ICEBRG is the only package to offer enterprise-class analytics in a single platform. When used in combination with GigaSECURE, customers experience data delivery and analysis in a centralized repository for security and operations data at a much lower cost than other operations and analytics tools.
- ✓ **Organizations in need of packet brokering only**: Try Gigamon GigaSECURE and see its value in that capacity. Evaluate its ability to deliver enriched data to existing security tools, then use a trial to try the integrated analytics that ICEBRG offers.

Creating Opportunities for Technology and Channel Partners

The ICEBRG platform is architected to maintain petabytes of data securely. This, combined with the API, role-based access controls, and full database management style controls, creates a fantastic opportunity for unbiased technology integration. No potential partners have been left out.[1] Data can feed other security applications, reporting engines, and ticketing workflow to fully support use within an MSSP, divisional, or business unit security groups with full information isolation.

The three main impediments to operations success are tools, data, and political silos. Each makes it difficult to get the visibility needed to be successful. With ICEBRG, Gigamon centralizes data and creates an open pathway for many tools. The new Gigamon platform breaks down two of the three silos, providing data storage and analytics capabilities that are open for integration with other tools. For channel partners, this facilitates increased sales because data is available to a wider variety of tools.

[1] Due to technology differences, some customization for data mappings may be required.

EMA Perspective

The acquisition is a great move for Gigamon, its customers, and those who identified the need for NGNPB and/or a security analytics solution. The synergies from the acquisition are strong and create a significant challenge for NGNPB competitors, and supply an excellent opportunity for technology and channel partners.

In a time when the number of security tools deployed ranges from six for the average small to medium business and as many as twenty-three for an enterprise, the need for centralized data, API integrations, and automation and advanced analytics has never been higher.

For channel partners expanding into managed services, this creates a consolidated platform to upsell in both solutions and services. The generally accepted rate of sale is two dollars in service opportunities for every dollar of product sales. For channel partners ready to move into services, this is part of the perfect storm.

1. For the previous four years, security budgets increased at an annual rate of nine to eleven percent year over year.
2. Low staff and skill availability are driving more companies to managed services.
3. The ICEBRG platform supports managed security services delivery.

3757.080618