Gigamon

IBM Security

Joint Solution Brief

Security Intelligence from IBM Security and Gigamon for Defense Against Advanced Targeted Threats

The Challenge

To detect and defend against today's increasingly sophisticated and targeted attacks, organizations need to do more than monitor logs and network flow data; they need to apply advanced profiling and analytics to reveal the footprints of would-be attackers.

Integrated Solution

Together with the Gigamon GigaSECURE® Security Delivery Platform, IBM QRadar SIEM delivers network visibility and actionable security intelligence to identify anomalies and defend against advanced targeted threats.

Joint Solution Benefits

- Enhanced visibility and easy access to traffic from physical, virtual, and cloud networks with the GigaSECURE Security Delivery Platform
- Ability to generate NetFlow/IPFIX from any traffic flow and decrypt SSL traffic to avoid unnecessary processing.
- Automatic traffic load balancing helps optimize the performance of IBM QRadar SIEM at reduced cost
- Aggregation, filtering, and distribution of relevant traffic to IBM QRadar SIEM helps accelerate processing throughput

Introduction

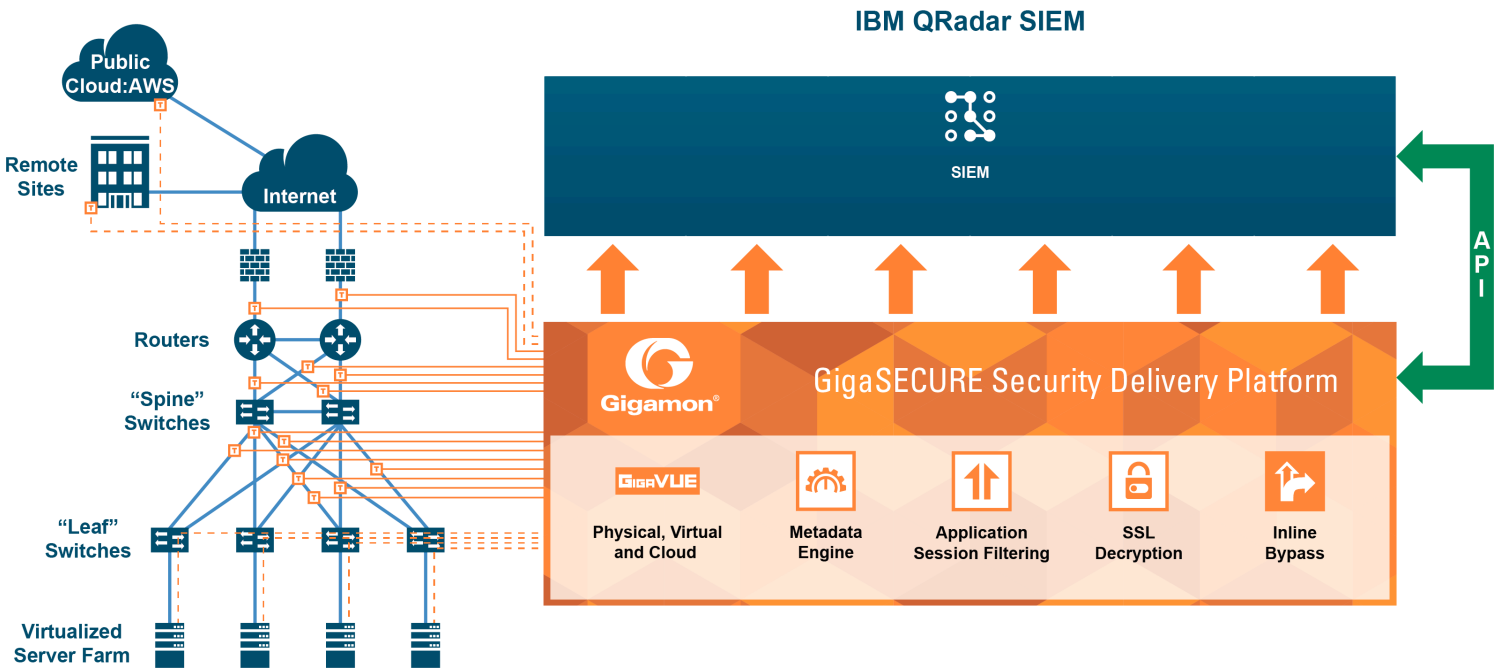
IBM QRadar SIEM consolidates log events and network flow data from thousands of devices, endpoints, and applications distributed throughout a network. It normalizes and correlates raw data to identify security offenses, and uses an advanced Sense Analytics engine to baseline normal behavior, detect anomalies, uncover advanced threats, and remove false positives.

This software also incorporates IBM X-Force Threat Intelligence, which identifies, scores, and categorizes potentially malicious IP addresses, including malware hosts, spam sources, and other threats. IBM QRadar can help manage risks, and correlate system vulnerabilities with event and network data, helping to better analyze and prioritize security incidents. IBM QRadar can also detect threats by monitoring network traffic in real-time, helps manage insider threats by monitoring user behavior, and can help analysts quickly and easily perform incident forensics investigations. Additional capabilities to expand the QRadar platform even further can be obtained from the IBM Security App Exchange.

Integrated with the Gigamon GigaSECURE Security Delivery Platform, IBM QRadar SIEM can detect threats other solutions often miss in the noise of millions of events, as well as helps ensure policy and regulatory compliance and can minimize risks to mission-critical services, data, and assets.

The Gigamon and IBM Security Joint Solution

The combined GigaSECURE platform and IBM QRadar SIEM solution provides real-time visibility to the entire IT infrastructure—operating across on-premise and cloud environments and providing detailed data-access and user-activity reports—for more effective threat detection and management. Moreover, IBM QRadar SIEM with QRadar QFlow and QRadar VFlow provides Layer 7 application visibility and flow analysis required to understand and respond to advanced and targeted security threats. By reducing and prioritizing alerts, it allows security analysts to focus investigations on an actionable list of suspected, high-probability incidents. And by offering multi-tenancy and a master console, it also helps managed service providers deliver security intelligence solutions in a cost-effective manner.



Key GigaSECURE Security Delivery Platform features that augment the value of IBM Security technology include:

- **Easy access to traffic from physical, virtual and cloud networks:** The GigaSECURE platform manages and delivers all network traffic to IBM QRadar SIEM, efficiently and in the correct format. To monitor east-west data center traffic and public cloud workloads, Gigamon taps virtual traffic and accesses and incorporates it into the GigaSECURE platform for delivery to IBM QRadar SIEM. This helps ensure that traffic is monitored and analyzed together and eliminates blind spots.
- **Aggregation to minimize tool port use:** Where links have low traffic volumes, the GigaSECURE platform can aggregate these together before sending them to IBM QRadar SIEM in order to minimize the number of ports that need to be used. By tagging the traffic, the Security Delivery Platform ensures the source of traffic can be identified.
- **De-duplication:** Pervasive visibility requires tapping or copying traffic from multiple points in the network, which, in turn, means tools may see the same packet more than once. The GigaSECURE platform has a highly effective de-duplication engine that removes duplicates before sending to IBM QRadar SIEM.
- **Filtering traffic to only send relevant traffic:** The GigaSECURE platform can be configured to send only relevant traffic or sessions to IBM QRadar SIEM to help ensure that it only analyzes traffic that provides security value.
- **Load balancing to spread traffic across multiple devices:** When traffic flows are large, the GigaSECURE platform can be used to split the flow across multiple IBM QRadar SIEM devices.
- **SSL decryption:** The GigaSECURE platform's real-time SSL decryption integration increases traffic visibility for sIBM QRadar SIEM.
- **Metadata generation:** The GigaSECURE Security Delivery Platform generates and sends to IBM QRadar SIEM unsampled NetFlow/IPFIX metadata for any traffic flow as well as extended metadata records (e.g., for HTTP response codes and DNS queries) to provide highly detailed contextual analysis when looking at network events.

Learn More

For more information on IBM Security and Gigamon solutions, contact:

IBM Security
www.ibm.com

Gigamon®
www.gigamon.com

3217-02 02/17