



Joint Solution Brief

Unlock Powerful Insights with ExtraHop and GigaSECURE Security Delivery Platform

The Challenge

IT networks are more complex, network speeds are accelerating, and the variety of monitoring tools are growing. IT Operations teams must manage and secure an ever-growing portfolio of applications that no longer run only in a dedicated infrastructure, but may run in private, hybrid, and public clouds. A new approach is required—one that will empower IT organizations with real-time visibility to manage the performance, availability, and security of these applications.

Integrated Solution

By deeply examining the network streams and transactions that traverse the asynchronously routed network, the joint solution from Gigamon and ExtraHop enables IT organizations to apply machine learning and advanced analytics to their wire data.

Joint Solution Benefits

- Broad and deep visibility across physical, virtual and cloud network traffic flows to gain full application (L2-L7) visibility
- Automatic traffic load distribution and aggregation functionality optimizes traffic
- De-duplicate traffic gathered from multiple collection points and distribute east-west traffic
- Get increased visibility into traffic flows without performance degradation
- Generate metadata (NetFlow/IPFIX) from any traffic flow to avoid unnecessary processing
- Go from raw network data to insights using machine learning and advanced analytics

Introduction

IT complexity and scale is quickly outstripping the capabilities of traditional network and application monitoring tools. Network speeds are accelerating, not only in total traffic but also in the breadth and diversity of traffic. The number and variety of monitoring tools is also growing. Securing the network and keeping customer data safe is as important as providing a good customer experience. IT Operations teams must manage an ever-growing portfolio of applications that no longer run only in a dedicated infrastructure, but may run in private, hybrid, and public clouds. A new approach is required—one that will empower IT organizations with real-time visibility to manage the performance, availability, and security of these applications. Together, Gigamon and ExtraHop offer the visibility and analytics enterprises need to improve performance, security, and the user experience.

The Gigamon and ExtraHop Joint Solution

ExtraHop is the leader in real-time network analytics. The ExtraHop platform applies advanced analytics and machine learning to all digital transactions, delivering timely and accurate insight that makes data-driven IT and security a reality.

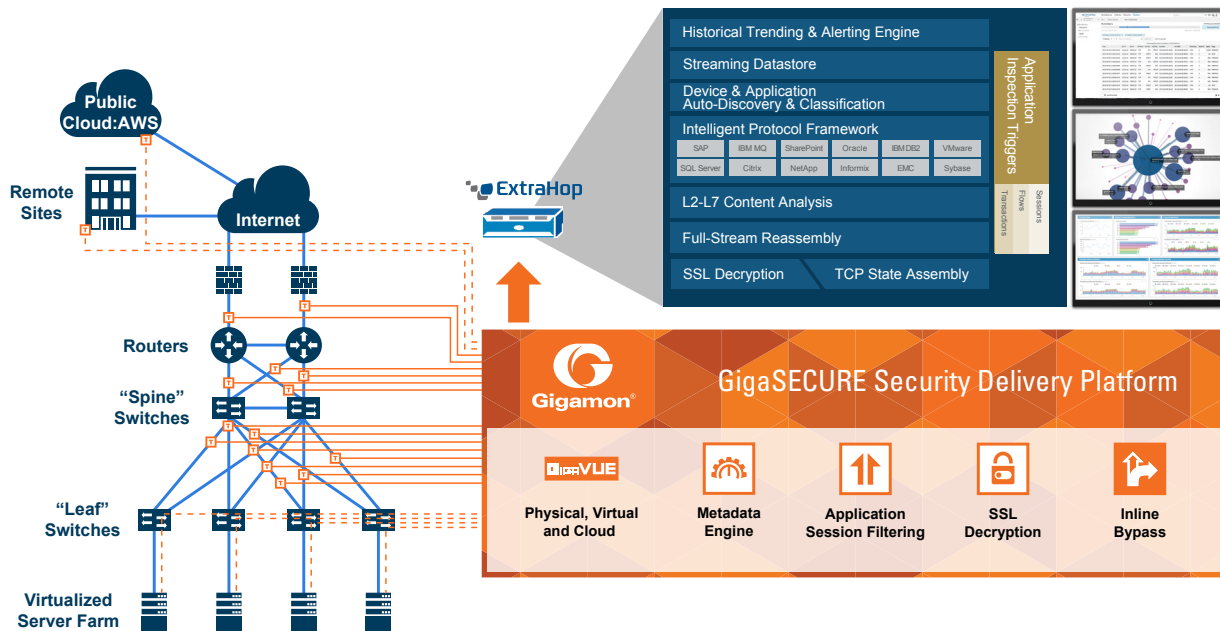
Fed by the Gigamon solution's ability to acquire network traffic from across on-premises and cloud environments, ExtraHop fully reassembles the network packets into server/client conversations, producing a real-time data source that is called "wire data."

Key features of the ExtraHop platform:

In-depth visibility – Know what's happening across your hyper-dynamic enterprise. ExtraHop works on-premises, in the public cloud, and in hybrid environments so that you have complete visibility into every interaction in every environment.

Speed to response – Accelerate incident response and service restoration with the industry's fastest workflow, backed by real-time analysis and machine learning.

Adaptable security – The security threat landscape is constantly changing. Meet threats where they are happening: on the network. ExtraHop fills the visibility gap in your dynamic environment so that you can understand what's normal and detect what's not.



Hybrid Deployment Model

Key GigaSECURE Security Delivery Platform features that augment the value of the ExtraHop platform include:

Easy access to traffic from physical, virtual and cloud networks – The GigaSECURE platform manages and delivers network traffic—in the format required—to ExtraHop. To monitor east-west data center traffic, and public cloud workloads, Gigamon taps virtual traffic and access and incorporates it into the GigaSECURE platform for delivery to ExtraHop for comprehensive security, monitoring, and management.

Filtering traffic to only send relevant traffic – The GigaSECURE platform can be configured to send only relevant traffic or sessions to ExtraHop so that it only analyzes traffic that provides value.

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. To avoid unnecessary packet processing overhead on ExtraHop, the GigaSECURE platform has a highly effective de-duplication engine that removes duplicates before they consume resources and helps balance monitoring coverage.

Load balancing to spread traffic across multiple devices – When traffic flows are larger than a single tool can handle, the GigaSECURE platform can split the flow across multiple ExtraHop devices and can also be incrementally grown by adding new devices to those already connected.

Aggregation to minimize tool port use – Where links have low traffic volumes, the GigaSECURE platform can aggregate these together before sending them to ExtraHop to minimize the number of ports needed. By tagging the traffic, the GigaSECURE platform helps enable the identification of the traffic source.

SSL decryption – Real-time SSL decryption integration increases traffic visibility for ExtraHop, broadening its scope for analysis.

Masking for security – The GigaSECURE platform is able to mask sensitive data (e.g., credit card numbers in e-commerce and patient identification in healthcare) within packets before sending them to ExtraHop where operators or other unintended recipients may see them.

NetFlow Generation – If desired, processing intensive tasks can be offloaded from ExtraHop by using the GigaSECURE platform’s functionality for generating unsampled, enhanced metadata in NetFlow or IPFIX format from any selected traffic stream.

Learn More

For more information on ExtraHop and Gigamon solutions, contact:

