



Joint Solution Brief

Holographic Visibility for Real-Time Breach Detection with HoloNet Security and Gigamon

The Challenge

A digital transformation driven by mobility and cloud computing has created a new threat landscape. Now, with traditional corporate network boundaries dissolved and without real-time detection tools, data breaches have become an inevitability.

Integrated Solution

Integrated with the Gigamon® GigaSECURE® Security Platform, OnFire from HoloNet Security provides a first-ever network hologram that can deliver full-spectrum “stateful” visibility—connecting users, devices, applications, and data—across corporate networks.

Joint Solution Benefits

- Visibility from network to users, devices, applications, and business data
- Easy access to traffic from physical, virtual, and public cloud networks using the Gigamon GigaSECURE Security Platform
- SSL decryption from the GigaSECURE platform avoids unnecessary processing by the OnFire solution while helping to ensure visibility into encrypted sessions
- Aggregation, filtering, and distribution of relevant traffic to OnFire accelerates processing throughput

Introduction

Organizations cannot protect against what they cannot see. And unfortunately, today, there’s much they can’t see across their corporate networks.

Let’s consider, for example, a network user, along with any data, applications, or devices—regardless of type or quantity—belonging to that user. The more users an organization adds to its network, the more blurred the relationship between these elements becomes. By extension, uncovering who is using what application, from which device, and to create or access what data also often becomes a management nightmare. The ability for organizations to detect and remediate data breaches in real time becomes increasingly difficult, if not impossible.

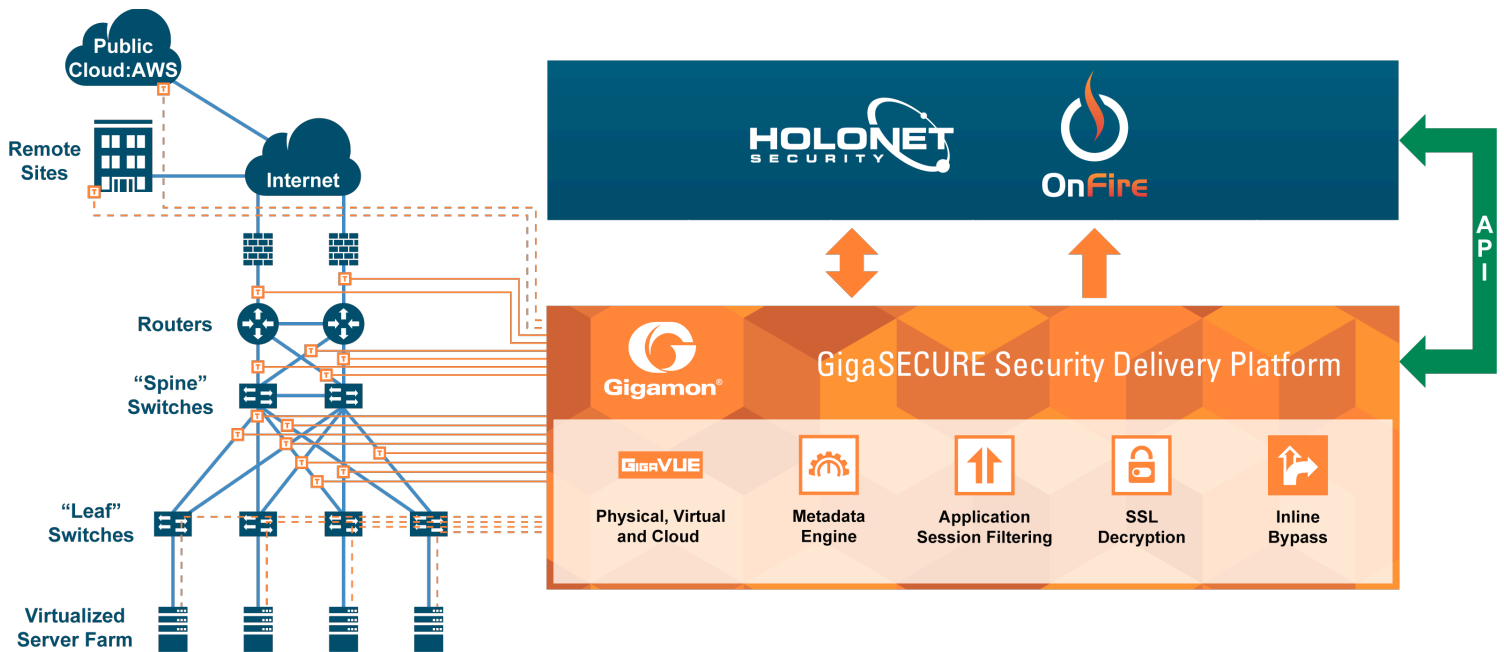
HoloNet Security wants to help untangle the chaos. With its OnFire solution, the company provides a new kind of transparency and insurance policy that extends across all data layers for any organization and delivers:

- Real-time data breach detection for sensitive business data
- Hastened post-incident investigation
- Fewer false positives than network-based anomaly detection solutions

The Gigamon and OnFire Joint Solution

OnFire offers real-time visibility and anomaly detection for sensitive business data-in-motion by integrating the best of user and entity behavior analytics (UEBA), cloud access security broker (CASB), and data loss prevention (DLP)—all through a patent-pending machine learning technology. As an extension of any firewall, the solution creates a network hologram that auto-discovers, identifies, and dynamically constructs multidimensional relationships across four key dimensions: users, devices, applications, and data. OnFire can show which users are using what devices and applications such that company data has clear ownership as to its movements; as well as automatically detect abnormal movements of business data in real time.

Integrated with the Gigamon GigaSECURE Security Delivery Platform, the OnFire technology makes hidden and complex relationships visible and helps enable organizations to protect their networks against the exposure of sensitive data. Moreover, OnFire gains resilience thanks to the GigaSECURE platform’s inline bypass functionality, which can sense tool availability and take action in the event of failure.



Key Gigamon solution features that augment the value of HoloNet Security technology deployments include:

Easy access to traffic from physical, virtual, and public cloud networks: The Gigamon GigaSECURE Security Platform manages and delivers all network traffic to the OnFire solution, efficiently and in the correct format. To monitor east-west data center traffic and public cloud workloads, Gigamon taps virtual traffic and incorporates it into the GigaSECURE platform for delivery to OnFire on the physical network. This can eliminate blind spots and help ensure that all traffic is monitored and analyzed together.

SSL decryption: Real-time SSL decryption integration increases traffic visibility for the OnFire solution.

Traffic filtering: The Gigamon GigaSECURE Security Delivery Platform sends specific traffic or sessions (e.g., HTTP, HTTPs, email) to OnFire so that the solution does not become overloaded with irrelevant traffic that would only be dropped at a later point.

Inline bypass for resilience: The GigaSECURE platform's inline bypass functionality provides physical bypass traffic protection in the event of power loss and logical bypass traffic protection in the event of an inline tool failure.

Aggregation to minimize tool port use: GigaSECURE Security Delivery Platform can aggregate links with low traffic volumes before sending them to OnFire in order to minimize the number of ports required. And by tagging the traffic, the GigaSECURE platform helps ensure that the traffic source can be identified.

Learn More

For more information on the HoloNet Security and Gigamon solutions, contact:

