HOLONET SECURITY

Frequently Asked Questions

Pre-Sales

HoloNet Security, Inc.
1294 Kifer Road
Sunnyvale, CA 94086, USA

www.holonetsecurity.com

Published in the United States.

00-01001-A-05/16

Frequently Asked Questions - Pre-Sales

How can OnFire help to uncover the unknown in my network?
OnFire leverages a patent pending Network Hologram to transcend the limits of contemporary network security solutions to uncover activity in your network which is invisible to firewalls, SIEM's, and DLP solutions. By uncovering the hidden relationship between users and their devices, applications, and data, OnFire provides unmatched visibility, bringing a new transparency across all data that traverses the network from Layers 2 through Layer 8.

How is OnFire different from other network visibility or analytics tools such as Splunk and Lancope?
OnFire is the first product in the market to bring the real-time network technology and big data analytics together to connect users with their devices, applications and data in full-mesh, presenting complete top-down visibility for an enterprise network from layer 8 to layer 2 in real-time. While all existing tools are focusing on network or application visibility in silos, OnFire provides a complete Network Hologram, focusing on the relationships among the four key security vectors - users, devices, applications, and data in such a way that every piece of data moved or application accessed has clear ownership, visible in real-time.

Will my users require any training or notice any changes to their network experience?
No. The changes should be completely transparent to your end users. No agents or other end user interaction is required.

How long does it take to setup OnFire in my network?
Your deployment can be up, running, and identifying interesting information in minutes. OnFire has two subsystems:

- **HoloVision** for analytics and customer portal, running in the Amzaon Web Services (AWS) cloud
- **HoloFlow** for traffic processing, running on-premise or in cloud. It can be setup easily with existing network gateways such as firewalls or switches through simple configuration modifications on the gateways.

How does OnFire deal with BYOD devices which are not on my domain or under my corporations control?
OnFire does not require any agents to be installed on your end systems. Any device connecting to the network, whether corporate or not, can be supported.

To inspect SSL traffic from BYOD devices, the client must have a CA certificate from your organization installed into its system/browser. This is easily done with MDM solutions or can be done with a few quick steps. Even without the CA certificate, OnFire can still fully inspect HTTP traffic for BYOD devices and gain insights into SSL traffic based on heuristics.

My organization is challenged with visibility into who is within the network, utilizing which devices, and generating what data, at any given time. How can OnFire help me get this under control?
This is a problem statement facing virtually every organization with an internet connection. Unlike legacy applications which required extensive coordination between an application team, server team, network infrastructure team, and end

user IT to provision, new applications can be spun up by your end users with nothing more than an email address. They require no administrator privileges, installed software, or training. Worst yet, these applications may be capable of processing your most valuable asset, your intellectual property.

OnFire solves this critical challenge by providing the corporate security team with a complete top-down visibility in full-mesh among four critical security vectors - users, devices, applications, and data in such a way that every piece of data movement and every application accessed through the network will be identified and linked to a specific owner in real-time. With OnFire, forensic investigations could be reduced from weeks or months to minutes.

Most security and visibility solutions often generate a lot of noise with activity and alerts. How does OnFire provide actionable intelligence?

Because OnFire generates its own logs through the processing of selected traffic in HoloFlow, the metadata is purposely collected to be relevant to the visibility. This is in contrast to the high-noise metadata used by SIEM products, generated from anywhere and any devices. The high-quality, smart metadata ensures that OnFire's analytics are extremely accurate.

Through the patent-pending Network Hologram technology, OnFire uncovers the hidden relationship between users and their devices, applications, and data. This linkage among the four security vectors enable much more precise profiling and create a solid baseline for all the behavior analytics built on top.

OnFire employs the power of the cloud to enhance your network's security posture with cloud-grade scalability and availability, eliminating the limitations of on-premise solutions.

My organization has strict data privacy requirements. How can OnFire support my deployment scenario?

- OnFire offers several deployment options. One option is to deploy HoloFlow on-premise which enables all network traffic to remain on premise. In this deployment scenario, no files or raw data is exposed outside.
- OnFire offers the ability to whitelist/blacklist which applications to inspect. This enables you to avoid processing traffic for certain applications, or to only process traffic for specified applications.
- OnFire also has the ability to operate in TAP mode, where only unencrypted traffic is processed.

How can OnFire help me in the event that a data breach or violation of my acceptable use policy occurs?

OnFire identifies the full-meshed relationships among users, devices, applications, and files in real-time. You can find "who did it" for "what happened" instantaneously without spending weeks or months of effort to connect the dots.

OnFire profiles the base behaviors for all security vectors to identify suspicious behavior in your network in nearly real-time so you can react more quickly to prevent malicious activity which may be escalating from breach to exfiltration.

Does OnFire require any agents or configuration on my end systems?

No agents are required. The only element that is required on your end system is a CA certificate from your organization to be able to inspect SSL.

What OS types are supported by HoloVision?

HoloVision provides analytics and customer portal for administrators to access the OnFire dashboard. Virtually any end-

point that is network enabled and has a web browser is supported.

Can OnFire help me comply with regulations like HIPPA, PCI, and SOX?
Yes. OnFire's content scan engine scans all files transferred through the network for sensitive data - such as social security, credit card number, and customized keywords - to help you identify, in real-time, any potential compliance violations. OnFire's integrated reporting and audit features help provide you with the necessary visibility and controls. While there is no single product that can holistically meet all requirements, OnFire provides a top-down overview of all network activities as a layered component of your overall compliance ecosystem.

What are some questions OnFire can answer that would supply me with early indicators of data breaches and enhance my current security posture and investment?

- Who has accessed what data, with what apps, and what devices?
- What anomalous or suspicious behaviors is happening on my network? Who is contributing to them and how are they different from baseline activity?
- Who is transferring my sensitive and customer data, from what devices, and to where?
- What are the risk-prone unknowns in my network?
- For any specific moment, who has accessed what data, with what apps, and from what devices?