

Solution Brief

PROFITAP AND SECURITY ONION SOLUTIONS

Security monitoring in high throughput environments



The Challenge

Enterprises often fail to pay close attention to what goes on before a cyber attack. Many assume that a single Network Security Monitoring (NSM) tool or the occasional test is sufficient to prevent, detect and respond to attacks which are so common today. However, just collecting and analyzing data doesn't get you there. Malicious activity often masquerades as legitimate activity. This means your organization requires continuous monitoring, with a diverse toolset.

While some of these requirements can be fulfilled by accessing network data through SPAN/mirror ports on switches in low bandwidth environments, multi-gigabit per second environments require a dedicated solution to access, manage, and analyze the traffic.

The joint solution of Security Onion and Profitap offers the most efficient end-to-end monitoring platform you can get for high-speed networks. It offers reliable access to the network and actionable data for the visibility you need to identify on anomalous events.

Security Onion provides a suite of tools, including full packet capture, network-based and host-based intrusion detection systems, and network and protocol metadata collection, combined with powerful analysis tools used to slice and dice network, endpoint, and application log data.

Profitap's innovative Network TAPs and Packet Brokers complement Security Onion's technology by capturing the network traffic (north-south & east-west) and providing all the data management required for a complete and effective security analysis in Security Onion. Using this data, security analysts can monitor networks in real-time and perform deep dive investigations, uncovering potential threats in your network.

The interface makes threat hunting easy to perform. Data sourced from your network, endpoints and applications are visualized directly in Security Onion, helping you proactively search for malicious activities. With the combination of data access and visualization, you are in complete control to implement a threat hunting gameplan tailored to your company and network environment.

Joint Solution

Visibility, performance and security. All are deeply important for the defense of your enterprise network. So what does the joint solution between Profitap and Security Onion Solutions look like in real life?

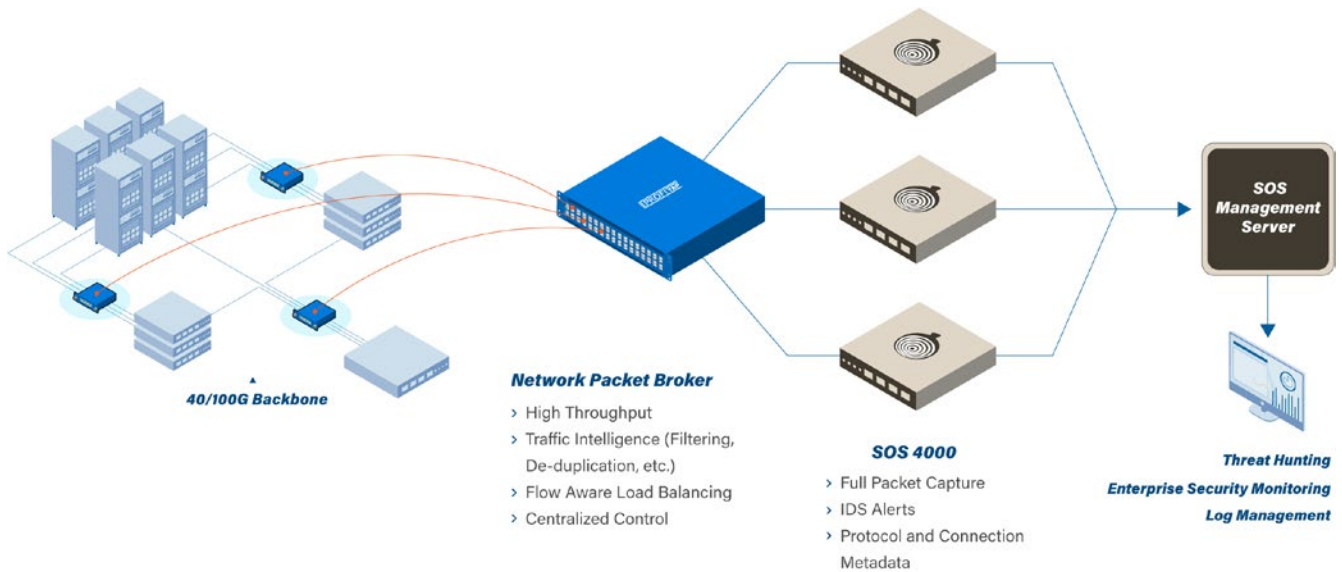
The solution can be split in two parts:

- 1.** Data access and intelligence
- 2.** Capture and analysis

Data Access and Intelligence

Reliable and accurate analysis stands or falls by the quality of the data that is captured. But you also need access in a way that does not impact the security of the network. It's important that new appliances don't add a backdoor for malicious practices on your network or, in case of a failure, cause network downtime.

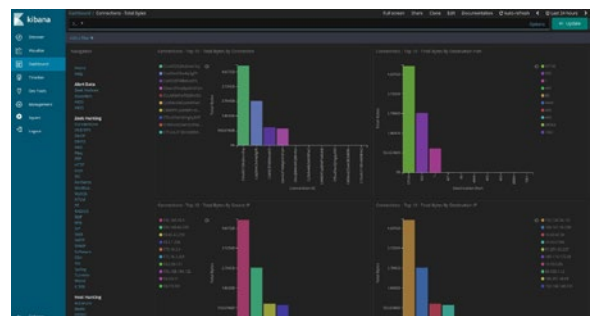
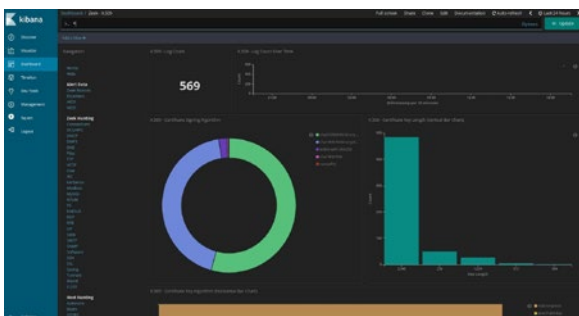
Profitap's network TAPs provide fail-safe access to the network and optimize the flow of traffic data by aggregating this into a centralized NPB. This way the Packet Broker is in an ideal position to perform advanced traffic management like deduplication and time stamping, forwarding only actionable flow data while keeping bandwidth usage to a minimum.

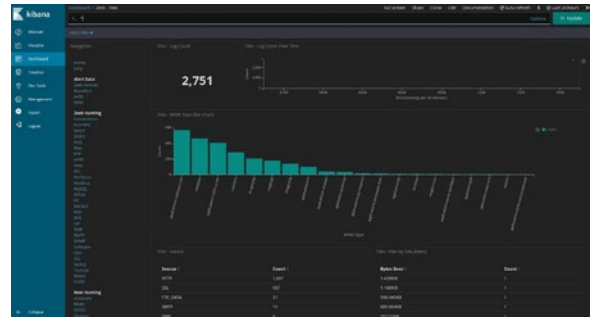
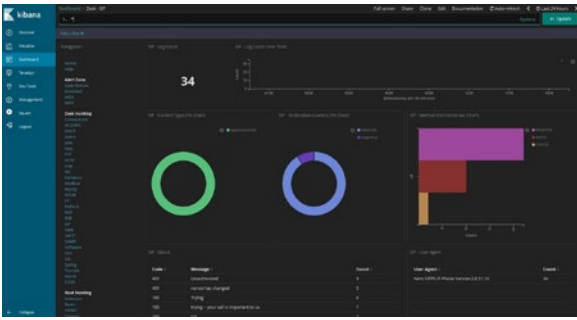


Capture and Analysis

With the help of Security Onion, you will be able to quickly analyze and pivot between all the different data types generated by Security Onion through a "single pane of glass." This includes not only NIDS/HIDS alerts, but also metadata generated by Zeek and system logs collected via syslog or another agent transport. With one click, your analysts can pivot from alerts and metadata to full packet capture for relevant details.

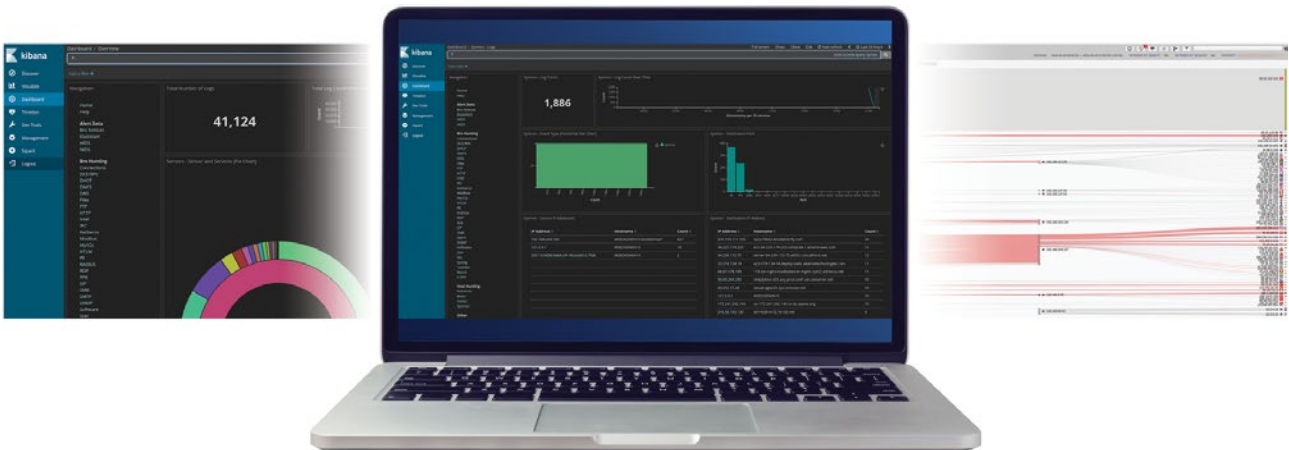
The joint solution allows network analysts to effectively and quickly identify malicious activity in very high volume networks.





Main Benefits

1. Fail-safe and real-time access to high performance networks with Network TAPs.
2. Centralized management and traffic intelligence. Leverage advanced features such as deduplication, packet slicing, flow aware load balancing, advanced filtering and time stamping from a single GUI.
3. Keep bandwidth usage low. Only actionable flow data is forwarded to the Security Onion sensor with Profitap Network Packet Brokers.
4. Easily identify network security breaches and suspicious behavior through traditional detection and response as well as threat hunting.



Company Information



Profitap develops and manufactures a complete range of innovative Network TAPs, Network Packet Brokers and Field Service Troubleshooters for security, forensics, deep packet capture and network performance monitoring sectors. All their network monitoring tools are highly performant and user-friendly, providing complete visibility and access to your network, 24/7. With a non-intrusive and fail-safe design, Profitap network analysis and traffic acquisition solutions send all the data to your security appliances so that your team can easily prevent and analyze cyberthreats.



We are the builders of Security Onion, a free Linux distribution for threat hunting, enterprise security monitoring, and log management. It includes Suricata, Zeek, Wazuh, the Elastic Stack, and many other security tools. Security Onion Solutions offers hardware appliances, support, and professional services centered around the Security Onion platform, and is the only provider of official Security Onion training.

Follow us on Twitter [@securityonion](https://twitter.com/securityonion)
or on the web at <https://securityonionsolutions.com>

**BRINGING CLARITY
INTO YOUR NETWORKS.
ANYTIME,
ANYWHERE.**



Profitap develops and manufactures hardware and software solutions that help you get complete access and visibility into your network. These network visibility solutions are designed with the security, forensics, deep packet capture and network & application performance monitoring sectors in mind.

Profitap network solutions help eliminate network downtime, add security to existing and new networks all over the world, assist in lawful interception applications and reduce network complexity. All of Profitap's network monitoring tools are highly performant, secure and user-friendly, and provide complete visibility and access to your network, 24/7.

As we are experts in our field, we have developed our products to set new standards in an industry where the definition of excellence is constantly being challenged.


With more than 1,000 clients from 55 countries, Profitap has become a must-have solution or many important businesses, many of which are among Fortune 500 companies.

**PROFITAP HQ B.V.
HIGH TECH CAMPUS 9
5656 AE EINDHOVEN
THE NETHERLANDS**

sales@Profitap.com
www.Profitap.com

 Profitap

 @Profitap

 Profitap-international