DockOS

Powerful open-source network monitoring tools such as Zeek, Suricata, or SNORT®, deployed quickly and easily on any EndaceProbe.

Open source tools provide powerful insights into network traffic for security and operations; however, teams often lack the time required to set open-source software up.

DockOS is a ready-to-deploy "open source toolkit" that will get you up and running with open source tools in minutes. It is a Linux virtual machine image that is fully open source (source code is available), free-of-charge and can be extended by adding additional open source tools or custom code.

Eliminate time-consuming installation and build tasks with a pre-built VM image configured with recent versions of popular open-source network monitoring tools, and optimized for high performance on any EndaceProbe in your network. Deploying open-source network monitoring software has never been easier.

Introduction

The EndaceProbe™ Analytics Platform's unique Application Dock™ hosting capability makes it an ideal platform for deploying open-source tools or custom applications alongside commercial solutions from our Fusion Partners, giving you the flexibility to deploy what you want, where you want, when you want.

DockOS is a Virtual Machine optimized for high-performance deployment on any EndaceProbe. Using DockOS, Endace customers can deploy open-source or custom network traffic analysis applications without deploying additional hardware. Hosted applications can take advantage of the high-speed, lossless, packet capture capability of the EndaceProbe platform for accelerated performance.

Included Applications

DockOS is based on Alma Linux, configured for deployment on EndaceProbe hardware, and supplied with several commonly-used open-source tools preinstalled as part of the DockOS image:

- SNORT®: Widely used IDS application with an excellent signature detection library (www.snort.org).
- Zeek™ (formerly Bro): Open-source network monitoring tool that monitors network traffic and generates transaction logs, file content and customized output (www.zeek.org).
- Suricata™: High-performance intrusion detection (IDS) and network security monitoring (NSM) engine (www. suricata-ids.org).
- Wireshark™: The de-facto standard tool for packet inspection and analysis (www.wireshark.org). Wireshark-cli, the command-line version, is pre-installed in DockOS.

Deploying DockOS and Hosting Applications

DockOS can be deployed directly into the EndaceProbe's built-in Application Dock™ hosting environment. An Application Dock instance can be provisioned in a range of "sizes" (with different amounts of RAM, storage, and CPU) to support the resource requirements of different hosted applications.

APPLICATION DOCK

Endace Application Dock™ allows users to run a Virtual Machine (VM) hosted on EndaceProbe. Each VM has dedicated compute resources and access to packets captured by the hosting EndaceProbe. Multiple VMs can run concurrently to increase packet processing volume or to run several applications at the same time.

Application Dock has dedicated resources, separated from other EndaceProbe operations, and can use one of several deployment sizes:

- Gen 4 EndaceProbes allocate up to 24 Cores (48 vCPUs), 144 GB RAM, and 600 GB storage for hosting VMs.
- The smallest VM ("Single Dock") provides two Cores (4 vCPUs), and 12 GB RAM.
- All VMs must use a multiplier of a Single Dock VM size (i.e 1X, 2X, 4X).

BENEFITS

Fast deployment – Rapidly deploy solutions on any EndaceProbe with minimal effort.

Flexibility – Use preinstalled solutions, or deploy any compatible, open source packet processing tools or custom applications.

Data Security – On-device analysis ensures packets never leave the data center.

Performance – Get the best performance using DAG technology and load balancing.

Automated Workflow – Automated data retrieval and processing using REST API and scripts.

To ensure maximum application compatibility, DockOS provides several ways for hosted applications to access and consume real-time or historical network traffic. This network traffic is presented to the hosted application using any of the following interfaces:

- vDAG with Native API – use the native DAG API for the highest available I/O performance and the ability to perform in-place processing if desired.
- vDAG using a 3rd Party API such as libPcap or PF_RING. Applications with interfaces to libPCAP or PF_RING can be deployed in DockOS with minimal effort and still achieve high I/O performance. A DAG-enabled libpcap library is installed in DockOS by default.
- VirtIO – a para-virtualized network driver that allows applications to be deployed very easily, with very good I/O performance. Includes DPDK API support on top of PF_RING and libPcap.

Multi-threaded applications that perform best using multiple input interfaces can use OSm's Hash Load Balancing to distribute incoming traffic across many Application Dock interfaces. Each interface receives a portion of the traffic for processing.

Scaling Application Performance with Multi-Hosting

Some applications have limits on the number of threads or CPUs they can effectively utilize to process incoming traffic, which in turn limits performance. Multiple DockOS instances can be deployed on a single EndaceProbe to overcome any processing limitations an application may have.

Multiply the performance of hosted applications by hosting multiple instances on a single EndaceProbe to boost throughput. For example, run two or three SNORT instances and load-balance network traffic across them to double or triple the processing throughput.

Hosting Custom or Open Source Applications

In addition to the preinstalled open-source tools in DockOS, the open DockOS environment allows other 3rd party or open-source monitoring tools to be deployed, including:

- Data Leakage Protection (DLP)
- Application Performance Monitoring (APM) tools
- Network Monitoring tools (such as Argus)
- Security Monitoring and Analytics tools
- NetFlow or metadata generation tools
- Custom developed network analytics tools
- Tools for analysis of captured network traffic

Hosting custom applications is simply a matter of installing an Alma Linux compatible version of that application in DockOS and configuring it to use one of the supported network interfaces.

Capture performance depends on the network interface used by the hosted application. Using the native DAG API, which bypasses the kernel and allows in-place processing, provides the best possible performance.

Using kernel processed vNIC also provides good performance. Other supported Kernel bypass APIs (DPDK and PF_RING) deliver high performance while using active polling and higher CPU usage.

Example Use Cases

There are many different use-cases that customers can, and do, use DockOS for. Here are a few of them:

Exporting Zeek Logs to SIM/SIEM

Zeek, preinstalled on DockOS, is a versatile and high-performance IDS software. Zeek can analyze incoming network traffic at high speeds and generate rich metadata which can be exported in real-time to a SIM/SIEMs or data-lakes. Zeek metadata combined with a SIEM provides a highly detailed view of the network and enables the security team to investigate detected anomalies quickly and accurately.

Continuous Intrusion Detection

Selecting and deploying an open-source IDS can be complicated and time-consuming. DockOS comes with three of the most popular open-source intrusion detection packages: SNORT, Zeek, and Suricata. Each can be deployed quickly to directly capture packet data from the host EndaceProbe and process it at high speeds using the proprietary vDAG interface. Alerts can be exported to your chosen SIM/SIEM, data-lake or SOAR tools.

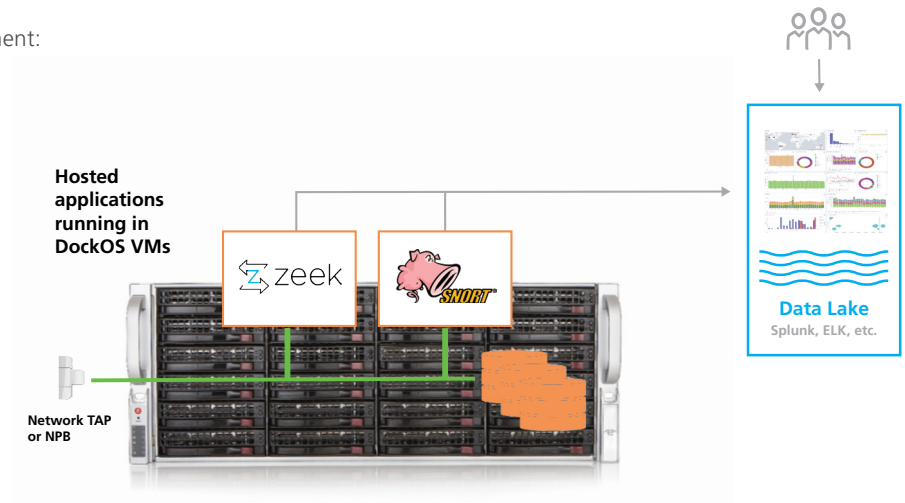
Conclusion

DockOS simplifies the deployment of open-source and proprietary network processing applications, eliminating network changes and the need to purchase new equipment. DockOS achieves uncompromising high performance using Endace's unique DAG technology and dedicated compute and memory resources. IT, SecOps and NetOps teams save time and money by rapidly deploying VMs instead of making expensive hardware changes to the data center.

DockOS is made available free-of-charge for customers, but is not covered by support. All source code is available.

How it Works

Here's an example deployment:



For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com