

## Endace Operating Systems

### ENDACE OPERATING SYSTEM FOR MONITORING (OSM)

Endace's OSm (operating system for monitoring) is a Linux-based operating system optimised specifically for EndaceProbes. It's an open, flexible software environment that delivers 100% accurate captured network traffic to any application you require. It enables:

- Multiple monitoring applications to run simultaneously on a single EndaceProbe without compromising performance
- Every application to have access to the EndaceProbe's single, authoritative and 100% accurate source of captured and time-stamped network traffic
- Applications to take advantage of OSm's inter-application messaging, alerting and data exchange – amplifying the power of each application
- Captured traffic to be routed to any applications or storage systems anywhere on the network
- Generation of 100% accurate Netflow (v5) on a 1:1 or sampled basis for consumption on or off the EndaceProbe.

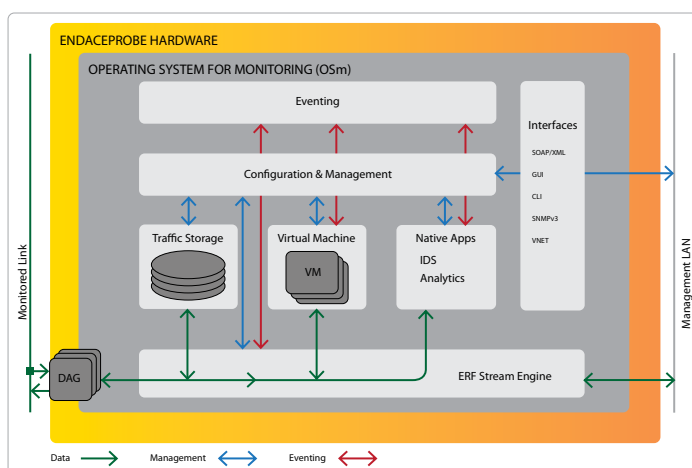
In addition, OSm provides a full management interface that allows a 'fabric' of EndaceProbes to be easily deployed and managed using the Endace Management Server (EMS).

### DEPLOYING THIRD-PARTY APPLICATIONS

To guarantee application performance, monitoring solution vendors have traditionally opted for dedicated single function appliances. In theory this is fine; however, in practice it results in multiple appliances consuming valuable data centre resources. Additionally, each appliance uses its own dedicated packet capture interface, which introduces a new set of issues as the accuracy of capture interfaces can vary wildly – particularly under load.

To provide organisations with a single authoritative platform capable of supporting a range of different monitoring applications Endace OSm provides the ability to host multiple

Virtual Machines into OSm. This allows organisations to run multiple applications simultaneously, confident in the knowledge that every application is being fed from a single, highly accurate, data source. OSm has been extensively optimised and tested to ensure there is minimal performance impact on the performance of applications running in the VMs.



The illustration shows a high-level overview of the OSm architecture. It illustrates how:

- The DAG card interfaces to the monitored link which captures traffic and feeds it to the ERFstream engine
- The ERFstream engine moves the packet data around the system like a bus, with virtualised applications using the ERFstream engine to filter live traffic and extract packets from the traffic stored on disk
- An EndaceProbe can run multiple Virtual Machines as well as native applications such as Endace Analytics
- A configuration and management layer talks to Endace Management Server (EMS)
- The Eventing layer allows applications to share 'events' between them, which amplifies the value of the applications. For example, a threat detection application could feed alerts to a forensics or lawful intercept tool.



## APPLICATIONS

OSm's Virtual Machine capability enables organisations to run a range of different applications – custom, commercial or open source. Applications that run in VMs interface to a standard network interface card (NIC) via libpcap – the industry standard application interface – making it compatible with a wide range of applications. Currently applications based on Linux are supported, with support for Windows-based applications coming later in the year. OSm currently supports up to six VMs on a single EndaceProbe.

VMs are suitable for running a broad range of applications including:

- Network monitoring applications
- Application and performance monitoring tools
- Feed and trade latency monitoring applications such as SeaNet or Correlix
- VoIP and video Quality of Service (QoS) monitoring applications
- Deep Packet Inspection security engines such as SNORT and Suricata
- DLP engines.

## VIRTUALISED APPLICATION PERFORMANCE

Historically running applications in VM's has resulted in a significant impact on application performance and made the technology unsuitable for use in very high performance environments. As a result of extensive tuning and testing, the VM overhead in OSm has been reduced to the point where multiple applications can happily co-exist on a single EndaceProbe with negligible performance degradation.

In real-world tests, SNORT (as an example of a processor-intensive application that runs in a VM) shows just a 6% degradation in performance when compared to the same application running natively.

## ROUTING

Part of OSm's uniqueness results from its flexible traffic routing. OSm has been designed to enable captured traffic to be routed to any application that needs it, whether in real time or post-capture, whether on the EndaceProbe itself or remotely. OSm supports a range of different interfaces, including SOAP/XML that make it easy to get the packets where you need them as efficiently as possible.

## EVENTING

Eventing enables applications to share information without requiring extensive application integration. It is based on a proprietary, lightweight, secure protocol that enables applications to emit and receive events. A full interface specification is available. Eventing rules can be configured and managed either through a CLI or GUI interface.

As an example, security events triggered by SNORT or Suricata can be passed directly into an analytics application (e.g. Endace Analytics) that enables the application to grab the packets of interest from the traffic storage disk and present them to the user for interrogation without requiring user intervention. This can dramatically speed the mean-time-to-resolution (MTTR) for network events.

## BUSINESS BENEFITS

By deploying a fabric of EndaceProbes across a network and leveraging the power of Endace's OSm organisations can derive significant benefits.

From a **resource** perspective, separating the hardware layer from the application layer and consolidating multiple software applications onto a single purpose built hardware platform makes sound business sense. This strategy saves valuable data centre resources and improves the effectiveness of operations teams as they can manage more applications more efficiently.



From a **flexibility** perspective, consolidating applications onto a single platform and leveraging a single source of highly accurate data also makes good sense. By leveraging the openness of OSm organisations avoid becoming inextricably tied to a single application vendor and can move easily between vendors without requiring a hardware refresh. OSm's flexibility and openness enables organisations to choose best-of-breed applications from their chosen application vendors and consolidate all those applications on a common, high-performance, 100% reliable packet-capture hardware fabric.

From a **performance and accuracy** perspective, fuelling all applications from the same data means that results from different applications can be compared and contrasted with the confidence that the underlying source data is accurate. By leveraging the power of the eventing interface it's possible to create new value from existing applications and derive further operational efficiencies through reductions in MTTR.

EndaceProbes running OSm represent a strategic investment. By investing in OSm at your next application refresh you can ensure that any future application refreshes need only involve upgrading software. And new applications can be easily deployed on top of your existing infrastructure.

For more information on Endace products visit: [endace.com](https://endace.com)  
For enquiries email: [enquiries@endace.com](mailto:enquiries@endace.com)