



Endace Security Manager: Simple command and control for open-source security systems



Endace Security Manager (or ESM) provides a powerful foundation for effective network security. As part of the Endace Application Suite, which is delivered natively on all Endace Systems, ESM leverages the power of open-source SNORT® to create a comprehensive network-wide threat-detection solution suited for the most complex and heavy-duty network environments.

ESM works seamlessly and elegantly within a packet capture fabric deployment, providing the highest levels of threat visibility and addressing numerous compliance requirements including PCI and FISMA.

The power of ESM lies in its ability to deliver industry-leading 100% packet capture and inspection capability. ESM enables both security professionals and security operations centre teams to easily manage large-scale, SNORT-based security deployments, safe in the knowledge that every single packet is being captured, analysed and recorded.

ESM comprises three components — the ESM Server, Agent and Dashboard — and provides:

- A rich interface dashboard for viewing and managing alerts, including trigger packets and threat information
- A graphical interface for rule and policy management
- The ability to:
 - Deploy, manage and blend commercial third-party, community-developed and custom rule sets
 - Write regular expressions against captured traffic to identify anything from HR violations to specific network usage patterns

- Full drill-down to packet level for forensic investigation
- Full reporting and audit trails
- Tight integration with Endace Analytics to improve threat analysis and alert resolution.

Although optimised to work with EndaceProbes™, ESM is deployable on any compatible hardware platform.

IDS SENSOR NETWORK MONITORING

With ESM you can monitor the heartbeat of all of your sensors from a central location. By centralising the management of all of your sensors, your ability to monitor, manage and control your network is greatly enhanced. It provides you with the power to see all across your entire sensor network.

EVENT MANAGEMENT

ESM lets you view security events in real time right across your sensor network. You can drill down into the event detail for fast, accurate decision making. Couple ESM with the sophisticated Endace Analytics tools, or leverage open-source tools such as Wireshark, and your ability to reduce mean-time-to-resolution (MTTR) is greatly improved.

RULES MANAGEMENT

You can use ESM to manage a blend of rule sets from commercial vendors (VRT), open-source communities (Emerging Threats) and custom rules that you have defined yourself. No other engine provides the level of flexibility and control offered by ESM.



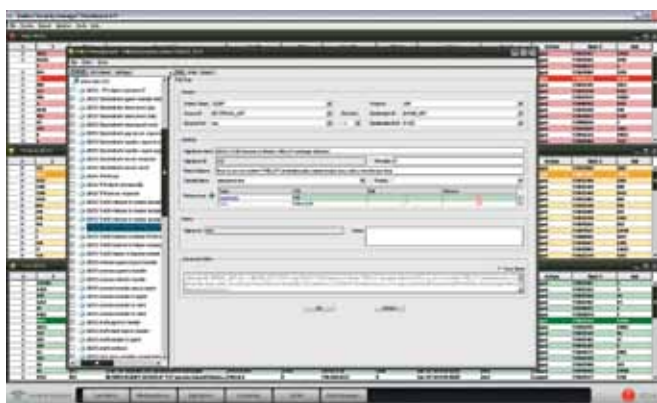
IDS NETWORK MONITORING

ESM provides centralised monitoring of your IDS EndaceProbes. An ESM Agent is deployed natively on each EndaceProbe and feeds alert information up to the ESM Server deployed on the same hardware as the platform's Endace Management Server. The ESM Server functions as the aggregation point for all alerts, and users connect to the server through the ESM application loaded onto local hosts.



MANAGING EVENTS

With ESM you can view events in real time across your entire sensor network. You can also drill down into the event detail allowing fast accurate decision-making, or improve your MTRR by using ESM with either Endace Analytics tools or open-source tools such as Wireshark.



MANAGING RULES

ESM provides a simple, centralised management console for managing and deploying rule sets from a range of different sources.

Our customers typically use ESM to deploy and manage a blend of rule sources, including Open Source (Emerging Threats), Commercial (VRT) and custom rules.



COMPATIBLE HARDWARE

While the ESM Server is optimised to run on EndaceProbe architecture, it can also run on any Linux-based server platform. Minimum system requirements include:

- 4GB of RAM
- 1TB of storage
2GHz processor

The dashboard can run on any modern laptop or PC running Windows or Linux.

For more information on Endace products visit: endace.com
For enquiries email: enquiries@endace.com