Idappcom and Endace

Detect and remediate the most challenging cyber threats across your network.

Idappcom and Endace solutions combine for scalable threat detection, accelerated response to security events and reduced threat exposure.

Idappcom's Distributed Rules Manager (DRM) is a rules-management platform that streamlines and automates rule management across large deployments of Intrusion Detection or Prevention Systems (IDS/IPS). Using rule deployment policies, customers can automatically deploy the appropriate rules to the right locations, reduce false positives and ensure accurate detection of the very latest exploits.

Combining access to multiple SNORT®, and SNORT-format, rule databases with editing, testing and provisioning capability, DRM enables rapid alert assessment and vulnerability remediation to help maintain maximum network and data protection.

EndaceProbe™ Network Analytics Platforms capture, index and store network traffic with 100% accuracy, regardless of network speeds, loads or traffic types. The EndaceProbe's built-in hosting environment, Application Dock™, extends security and performance monitoring by allowing Idappcom-managed SNORT instances to be hosted on the open EndaceProbe platform. Hosted SNORT instances can analyze recorded traffic in real-time at full line-rate, or analyze recorded, packet-level Network History for back-in-time investigation.

Streamlining Security Investigations

The Network History recorded by EndaceProbes is integrated with Idappcom's DRM using the Pivot-To Vision™ function of the EndaceProbe's powerful API.

Pivot-To-Vision lets security analysts pivot from DRM threat alerts directly to EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze the related, packet-level Network History. Using the IP address and time range of the trigger, Pivot-To-Vision focuses the analyst directly on pre-filtered incident data. EndaceVision lets analysts extract, dissect and review the relevant traffic from the terabytes of Network History recorded by EndaceProbes on the network. It enables analysis to microsecond level with views filtered by Application, IP, Protocol, Top Talkers and many other parameters, allowing rapid insights and accurate conclusions.

Being able to get directly to the related packets lets security analysts quickly and conclusively establish the root cause of issues and respond appropriately, dramatically reducing the time to investigate and resolve critical incidents.

PRODUCTS

- **Idappcom Distributed Rules Manager**
- **Idappcom Managed SNORT IDS**
- **EndaceProbe with Application Dock**

BENEFITS

- Detect threats across your network, anywhere you deploy an EndaceProbe
- Easily manage IDS policy and rulesets from multiple sources across your distributed network
- Respond to and remediate incidents quickly and efficiently with streamlined investigation workflows.
- Rapid, conclusive and actionable investigations with drill down to packet level detail.
- Catch zero day exploits by replaying network history through updated rulesets.
- Reduced threat exposure through greater analyst productivity and faster incident investigation.
- Definitive evidence trail with an accurate record of all relevant packets.
- Increased awareness and remediation of False Positive Alerts

Scaling IDS Deployment with DRM and Application Dock

Idappcom-managed SNORT deployments can be hosted on the EndaceProbe in Application Dock. Every packet captured and recorded by the EndaceProbe can also be simultaneously streamed to these hosted, Idappcom-managed SNORT instance in real-time.

Security Operations teams can dynamically deploy managed SNORT

anywhere on the network that they have EndaceProbes deployed, allowing them to increase their detection footprint on demand with no additional hardware installs.

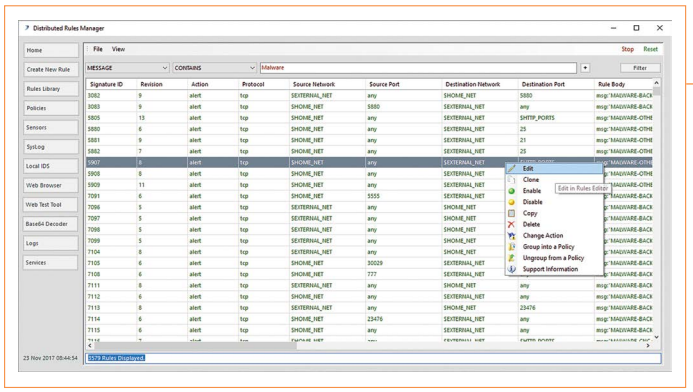
EndaceProbes are designed to ensure system resources used for capture and recording are separated from the resources used by hosted applications. This means capture performance is never impacted by hosted applications and vice-versa, guaranteeing 100% accurate recording even when Idappcom-managed SNORT instances are processing heavy traffic loads.

Conclusion

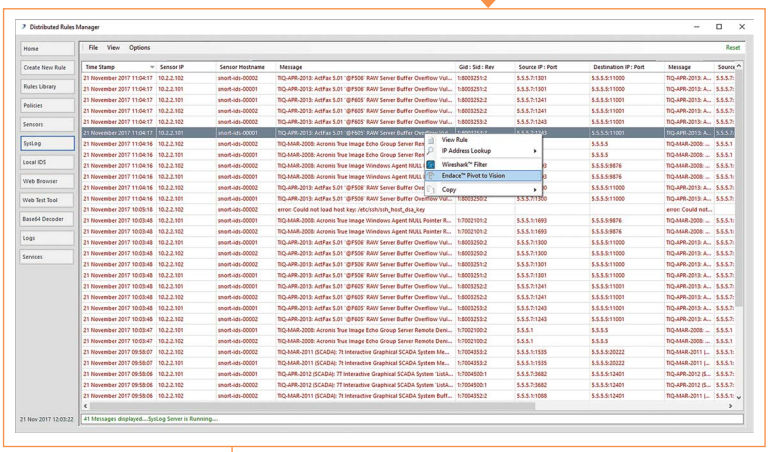
Using Idappcom DRM and integrating Network History into Idappcom-managed SNORT instances delivers comprehensive security detection and deep contextual insight that accelerates the investigation of, and response to, security issues.

And, by deploying Idappcom-managed SNORT instances to EndaceProbes in Application Dock, security teams can extend their reach easily, leveraging existing EndaceProbe hardware deployments to extend security monitoring and network recording capability.

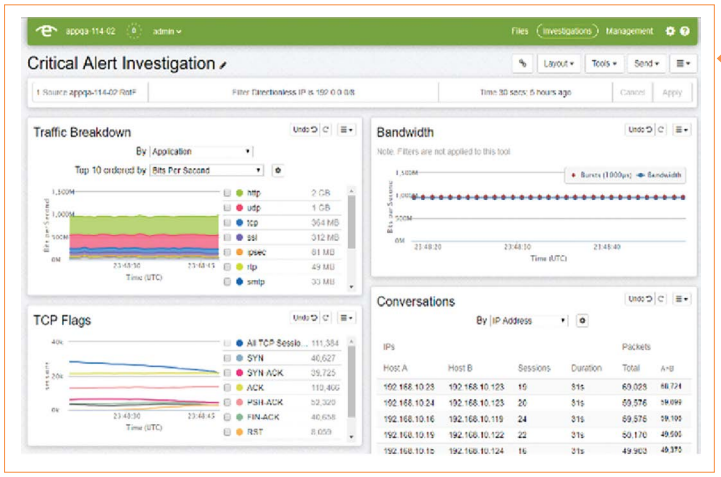
The combined Endace and Idappcom solution provides improved security posture, reduces threat exposure and accelerates incident response with definitive evidence.



Idappcom DRM manages Rules across multiple SNORT deployments running on EndaceProbes



From DRM alerts, operators can pivot directly to EndaceVision to analyze related packet history



EndaceVision and EndacePackets let analysts dissect traffic and draw accurate conclusions

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

For further information, email: info@endace.com