Pervade Software

Full Stack Monitoring

To get a complete view of an organisations systems, comply with with governance, risk and compliance requirements and and ensure security monitoring for all threats, it is essential to have complete visibility and analysis of every layer of the OSI model. Traditionally, this has been achieved through the use of multiple systems with manual correlation and analysis to give the desired full stack view. With an ever increasing range of solutions on the market, all claiming to be a silver bullet for an organisation's monitoring and security needs, it can be difficult to create a monitoring solution that gives a truly unified approach ensuring no events fall between the cracks formed from multiple systems and ensuring the information delivered is in a format that is fit for purpose. For that reason, pervade software have developed the below comparison table to assist end users when comparing popular technologies to see how much visibility they can provide.

OSI Layer	Pervade Software	SIEM	Traffic Analysis
Application *Serves as a window for users and application processes to access services (HTTP, IRC, DNS, SNMP)*	**✓ Complete** Full visibility can be gained through custom queries of app data as well as analyzing any log format	**✓ Partial** Only available where logs are produced in a compatible format containing all relevant data. No app data compatibility	**✗ No Visibility** Active traffic data cannot provide a view of any application layer detail, traffic may indicate that applications are active but not what is being done
Presentation *Formats data to be presented to the application layer including handling encryption (SSL/TLS, SSH, IMAP, FTP, JPEG)*	**✓ Complete** Can identify successful and failed actions in this layer as well as summarizing trends and alerting anomalies	**✓ Partial** Available where logs are produced as a result of an action taken, typically this is only available where an operation was successful	**✗ No Visibility** It is possible to see increases in connections or traffic flow but there is no view of what is being communicated
Session *Maintains connections and is responsible for ports and sessions (APIs, Sockets, RPC, SQL, NFS, ASP)*	**✓ Complete** Able to identify calls and open sockets as well as scan for available ports along with known vulnerabilities	**✓ Partial** Access, Error and Event logs provide a partial view at this layer allowing for further investigation. No view of ports or vulnerabilities	**✗ No Visibility** Packets may be routed through identifiable ports, but no further details about sessions or results is possible
Transport *Ensures that messages are delivered error-free, in sequence and with no loss or duplication (TCP, UPD)*	**✓ Complete** Active traffic monitoring along with device and appliance log analysis allows full visibility	**✓ Partial** Available where devices and appliances support creation of relevant logs. Cannot analyse live traffic	**✓ Partial** Allows visibility of packet metadata but no view of packet contents or request result
Network *Controls the operations of the subnet, deciding which physical path data should take (IP, ICMP, IPSEC, IGMP)*	**✓ Complete** Active traffic monitoring along with appliance log analysis allows full visibility	**✓ Partial** Available where devices and appliances support creation of relevant logs. Cannot analyse live traffic	**✓ Partial** Allows visibility of packet metadata but no view of packet contents or request result
Data Link *Transfer of data frames from one node to another over the physical layer (Ethernet, PPP, Switches, Bridges)*	**✓ Complete** Log and Config auditing combined with customized queries allows full visibility	**✓ Partial** Can give a view of any changes and processing where an event/error log is produced. No config auditing capability	**✓ Partial** Gives limited data regarding source and destination with no view of errors or config changes
Physical *Looks at physical medium used to move raw data (Coax, Fiber, Wireless, Hubs, Repeaters)*	**✓ Partial** Through queries and correlation rules it is possible to discover the state of physical connections.	**✗ No Visibility** As no logs are produced at the physical layer, it is not possible for these to be analysed	**✗ No Visibility** A loss of traffic to an area of the network may be discoverable but this cannot be attributed to a physical cause

Castle Court, 6 Cathedral Road, Cardiff, CF11 9LJ
+44 (0)29 2064 7632 | www.pervade-software.com