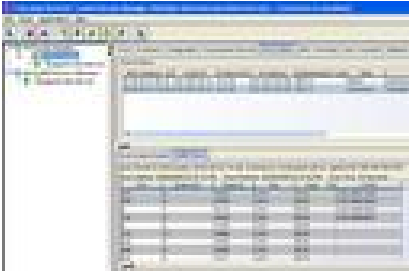




EXCLUSIVE: Enterasys Sentinel 1.0



Rating: ★★★★★

Price: £15,116 for 500 nodes exc. VAT, £25,532 for 2000 nodes exc VAT

Company: Enterasys Networks

Review Date: Oct 06

Verdict: A pile of management consoles to handle but Enterasys Sentinel is relatively simple to implement, offers strong end point vulnerability scanning and its agent-less architecture makes for easy deployment in enterprise networks.

End point security is a big buzzword in the enterprise but historically there have been few solutions on the market that allow administrators to implement these controls.

The concept is quite simple as devices such as workstations, laptops and PDAs are interrogated to determine what security threats they pose and their level of network access is determined by these findings. Another issue is deployment as the majority of current solutions require an agent installed locally on each system.

Enterasys' Sentinel (ES) takes a different tack as it doesn't require any local software installed on user's systems. In a nutshell ES provides the services for end point assessment and authorisation. It functions as a proxy RADIUS server where it intercepts the authentication process, queries the end point and determines its level of network access based on what is running on it and whether it satisfies certain criteria.

The smart part of ES is that it uses access policies and depending on the actions contained within will dynamically configure network switch functions such as VLANs, CoS and filtering allowing it to control traffic at the Layer 2, 3 and 4 levels.

The downside is that ES is currently aimed at Enterasys-centric networks although policies are supported by all of its mid-range and enterprise level switches. Policies are entirely port based so, for example, a rule that forbids FTP traffic is applied to a specific switch port and all those users that are physically connected to that port. In Enterasys' world users would be connected to an edge switch to their own dedicated port and policies would be applied to each port and not to the uplink. Note that the next release of ES later this year will support switches that are RFC3580 compliant for creating dynamic VLANs.

ES requires a number of components to function and uses a trusted access gateway (TAG) which is supplied by Enterasys as a standard Intel-based 1U rack appliance. Enterasys advised us it will also be releasing an expansion module for its Matrix DFE switch family that incorporates the TAG. The core software component required by ES is the NetSight Console which is used to manage and monitor the network on a day-to-day basis.

The appliance itself is configured from Enterasys' trusted access manager (TAM) software which is installed as a plug-in to NetSight. Policies are looked after by the NetSight Policy Manager (NPM) which is also a plug-in.

The vulnerability scanning is carried out by the open-source Nessus - a highly respected security audit tool. As Nessus is open-source it must be supplied by the customer and if they want it on an appliance then they must also supply that as well. Enterasys cannot provide these components but advised us that it will assist in its installation. Despite Nessus' pedigree

some enterprises may not want open-source software on their networks but Enterasys has this covered as ES also supports the LockDown Networks Enforcer appliance.

There are a lot of components here but installation is actually fairly straightforward. The TAG appliance merely requires the IP address of the Nessus server which is entered during the software installation phase. The TAM is installed on the NetSight Console server and requires a RADIUS server to function. It can use an existing one or the TAG appliance can provide these services. Essentially, any existing security schema is left undisturbed.

ES TAM uses the concept of security domains which contain individual or multiple physical network switches.

Creating a security domain starts by naming it and selecting a NetSight authorization group that is allowed to modify the security domain. Custom configurations determine how authentication is applied and include proxy RADIUS and local authentication of MAC addresses. You then decide which policy is to be applied if the client system passes the scan and another policy to apply if the scan fails to finish or the Nessus systems goes offline. You determine how often you want end systems to be scanned and what policy should be applied if they fail the scan. You can even apply a different policy whilst a system is waiting to be scanned or in the process of being scanned. Configuration can be made even easy as Enterasys provide a bunch of generic templates.

The end point scan is carried out by the Nessus server as and when instructed by the ES security domain parameters. The Nessus server is easily configured from its own management utility or via a standard browser. You can pick and choose from a range of plug-ins which are regularly updated via automatic downloads. Nessus is virtually an industry standard for end point scanning and it shows as it provides a huge range of options.

You can scan for the latest Windows vulnerabilities and installed patches, the type and version of operating systems, running applications such as P2P, active services, anti-virus signature file versions - the list is almost endless. Once Nessus has completed the scan it passes the results back to the relevant security domain which then analyses them and applies an appropriate policy. If a client doesn't pass the Nessus scan then TAM will apply a policy that can block all access to network resources except remediation services such as a web server that provides information on fixing the problem.

From the TAM console you can see all end systems and view the status of each one along with details on any scans they may have failed. You can drill down to each event and view Nessus' comments and its suggestions for remedial actions. TAM also provides basic reporting facilities consisting of pie or bar charts showing all scanned, accepted, rejected and quarantined systems. Historical data can be queried over a time period although it's all fairly basic with no options to export data into other file formats. Alerting features are more sophisticated as TAM integrates with the NetSight Console and uses its Alarms Manager.

During testing we found ES worked well although it can be confusing having to deal with four separate management interfaces as you have consoles for NetSight Console, NetSight Policy Manager, ES TAM and the Nessus server. However, in practice we found they all worked very well together and the fact that ES is agent-less means reduced administration overheads and easier deployment.

Reviewed by Dave Mitchell

Specifications

Windows XP; Windows 2000; Windows Server 2003; Solaris 2.8 & 2.9. Clients: Windows; Linux; Solaris; MacOS, FreeBSD.

Nessus Vulnerability Scanner to be supplied by end user - supports Linux, FreeBSD, Solaris and Windows. Minimum hardware requirements for Nessus: 733MHz Pentium III or G4 processor, 256MB of memory - 1GB recommended.