Security Information Management

VENDOR/ PRODUCT	PLATFORM(S)	COST	SIM TYPE (S)			PROS	CONS	VERDICT
			Command	Contain	Control			
e-Sentinel	Sun Solaris Solaris 2.6/7/8; Windows NT 4.0 SP 6/6a	$95,000 for Starter Kit (includes the Open e-Security Platform, e-Security Administrator Workbench and 20 devices to be monitored).	✓			Has more history and rev cycles than most other SIMs. GUI in 3.1 includes neat graphics library and support for 59 customized Crystal Reports.	PERL, Tcl or other scripting experience needed to build/modify agents. Jury's still out on SNMP.	Good solution for centralizing alerts from multivendor security equipment.
ActiveEnvoy	*Console*: Windows NT 4.0; Solaris 2.6, 2.7, 2.8; Red Hat Linux *Agent*: Windows NT 4.0; Solaris 2.6, 2.7, 2.8; Redhat Linux	$4,995 for EasySecure (entrylevel NT Solution) and support for three devices.	✓			Use of XML is a plus. Excellent multivendor support. Support for role-based administration.	Eagerly awaiting SSL encryption for agent communications.	Scalable architecture and excellent cross-vendor support.
SystemWatch	Windows 98, NT 4.0 and 2000; Unix: IBM AIX 4.3 and above, Sun Solaris 2.6 and above, HPUX 11.0 and above, Linux 2.2 and above	$23,895 for Security Starter Pack (includes Enterprise Console and five Security Agents).	✓	✓		Only solution with in-house network monitoring tie-in (NerveCenter). OPSEC-compliant agents that support the Nokia platform are a plus. Advanced event-correlation features may help catch subtle attacks.	Sparse out-of-thebox device support. The ability to automate actions can be a doble-edged sword if implemented poorly by the user.	Advanced event correlation features make this product an attractive option.
Solsoft NP	*Control Server*: Sun Solaris; Network Control Point: PC-style x86 hardware	Management Station is available in Enterprise ($14,995) and Service Provider ($49,995) editions. Device modules start at $195 each.			✓	Best at supporting Cisco gear. Simplifies the development and deployment of a security policy across the enterprise.	Lags in support for the most current versions of security hardware and software. Rollback only supported on Cisco gear.	Focus on distributing unified security policies across the enterprise is a plus, but lack of updated drivers out of the box is a drawback.
NsControl	Windows NT 4.0 SP3 or higher, Windows 2000	Pricing varies depending on the customer requirements. A large enterprise may spend around $4 million to become fully deployed.			✓	Scalable architecture. Device support limited only by time it takes to create drivers. Serious about security; deployment well encrypted. Broad rollback support.	Talking to devices in their native language may require lots of engineering effort. Limited Web interface requires more reliance on PERL and Tcl scripting.	Newcomer to the field that has done a lot of things right, making the distribution of unified security policies a practical reality. However, the processes of turning policy into machine controlling code will require a dedicated effort.