Other Security Management Software

The enterprise security management/security information management market is populated by a hybrid mix of solutions offering similar features and functions. Here are 10 examples of what's available.

VENDOR/PRODUCT	ESM/SIM TYPE			COMMENT
	Command	Contain	Control	
Spectrum Aprisma	✓			Similar to e-Sentinel and ActiveEnvoy products: centrally correlates syslog entries from third-party security tools and performs "root-cause"and "fault-isolation" analysis to prioritize alerts
bv-Control BindView	✓		✓	BindView offers 10 bv-Control software suites for a wide range of platforms and applications (e.g., bv-Control for Windows 2000 and Active Directory, bv-Control for Unix). Suites offer enterprise-wide assessment of vulnerabilities while helping ensure consistency and accuracy of network configuration policies
FireWall-1 Check Point Software			✓	Check Point FireWall-1 uses a centralized management server to integrate multiple enforcement points, centralizing changes and reporting. FireWall-1's Log Viewer provides dynamic tracking, monitoring and accounting information for all connections logged by FireWall-1 enforcement points.
eTrust Suites Computer Associates	✓		✓	CA offers several complementary security management suites in its eTrust line of solutions, including suites for policy compliance, single sign-on and log auditing. eTrust Admin helps users manage users and resources across enterprise security systems and directories, including NT, Unix, NDS, CA-ACF2, CA-Top Secret, RACF, Lotus Notes and Exchange.
Consul/eAudit Consul Risk Management	✓			Collects security logs from different platforms and archives them on a centralized server. Event-based audits are performed automatically, delivering exceptions and attentions depending on security policies.
NeuSecure GuardedNet	✓			New "command"-type SIM tool that centrally collects and correlates security event logs from distributed third-party devices. Calculates threat levels of a given chain of correlated security events and provides users with ranked list of attack severity for each host.
Network Security Manager 3.3 Intellitactics	✓			A "command"-type SIM solution that collects security data from firewalls, IDSes, virus detectors, activity logs, routers, switches and servers. Looks for patterns of suspicious activity, identifies both internal and external threats, and analyzes the security implications of those threats.
Netcool Firewall Micromuse	✓	✓		For Check Point and Cisco gear, Netcool provides firewall log capture and viewing, intrusion detection (including recognition of all session-level attacks), and attack responses, such as sending an e-mail or pager alarm or closing down an attacker's connection.
Global Management System (GMS) SonicWALL			✓	Security policy management tool provides centralized administration of remote SonicWALL security appliances while also managing VPNs and other security applications, such as network AV, content filtering, vulnerability assessment and authentication.
Enterprise Security Manager 5.5 Symantec			✓	Released in November, version 5.5 of the former Axent ESM suite helps administrators automate the distribution and management of security policies on remote applications. Performs more than 2,000 security and vulnerability checks across multiple platforms, including Windows NT/2000/XP, Solaris, HP-UX, AIX, Red Hat, NetWare, OpenVMS and AS/400.