NETWORK IDS FEATURES

	Cisco Secure IDS 2.5	Computer Associates eTrust	CyberSafe Centrax 2.4	Enterasys Dragon 4.2	Intrusion.com SecureNet Pro 3.2	ISS BlackICE Sentry 2.5	ISS RealSecure 5.5	NFR Security Network Intrusion Detection	Snort 1.7	Symantec NetProwler 3.5
Platform	Appliance	Windows NT/2000	Windows NT/2000	Appliance, BSD, Linux, Solaris	Appliance, Linux	Windows NT/2000	Solaris, Windows NT/2000	Appliance	BSD, Linux, Solaris, Windows NT	Windows NT/2000
Held up on the Bruisernet	Y	N	N	Y	Y	Y	Y	Y (on final revision)	Y	N
NIDS/HIDS agents	Y/N	Y/N	Y/Y	Y/Y	Y/N	Y/N	Y/Y	Y/N	Y/N	Y/Y
Integrated HIDS/NIDS management platform	N/A	N/A	Y	Y	N/A	N/A	Y	N/A	N/A	Y
Integrates with file integrity checkers	N	N	Y	Y	N	N	Y	N	N	N
SNMP traps for integration into management platform	N	N	Y	Y	Y	Y	Y	Y	N	Y
Back-end database API	N	N	Y	Y	Y	Y	N	Y	Y (MySQL)	N
Management platform (console)	Windows NT/2000	Windows NT/2000	Windows NT/2000	Unix	Linux	Web	Windows NT/2000	Windows NT/2000	CLI	Windows NT/2000
Remote sensor management	CLI/CSPM	Windows NT/2000	Windows NT/2000	CLI/Web	GUI	Windows NT/2000, Web	GUI	Console	CLI	Windows NT/2000
Stealth mode (unbound sniffing NIC)	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Frag reassembly	Y	N	N	Y	Y	Y	Y	Y	Y	N
TCP stream reassembly	Y	N	N	Y	Y	Y	Y	Y	Y	N
Automatic signature update capabilites	N	Y	Y	Y	N	N	Y	Y	Y (if scripted)	Y
CVE cross-references	N	N	Y	Y	N	Y	N	N	Y (if Whitehats)	Y
Open signature rule sets	N	N	N	Y	N	N	N	Y	Y	N
Customizable signatures	Y	Y	N	Y	Y	N	Y	Y	Y	Y
Update frequency	Quarterly and mailing list alerts	As needed	Quarterly and as needed	Weekly	Monthly	As needed	Quarterly and mailing list alerts	As needed	Daily releases	N/A
Rule tuning (turn on/off specific signatures)	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Alerting mechanisms	SMTP, SNMP HP OpenView, CSPM	E-mail, phone, fax, OPSEC, CA Unicenter	Kill connection	SMTP, paging, SNMP, syslog, script	E-mail, SNMP	E-mail, pager, SNMP, script	E-mail, OPSEC, TCP Kill, SNMP, blocking, log to database, alert to Lucent firewall, paging, custom	E-mail, pager, SNMP, script	None built in	E-mail, pager, SNMP, script
Encrypted transmissions upstream	Optional (IPsec)	Y	Y	Y	Y	Y	Y	Y	N/A	Y
Offending packet logging	Y	N	N	Y	Y	Y	N	N	Y	Y
Standardized packet capturing	Y	N	N	Y	N	Y	N	N	Y	N
Classification system	Low/medium/high	Low/medium/high	Low/medium/high	Suspicious/probe/attacks/failures/compromise/virus	Low/medium/high	Info/suspicious/serious/very serious/critical	Low/medium/high	Info/warning/attack/error	None	Low/medium/high
24x7 support	Y	Y	Y	Y	Y	Y	Y	Y	N	N/A
Price	4210: $8,000 (appliance); 4230: $19,000 (appliance); Catalyst 6000: $14,995	Software: $3,000-$25,000	Sensor: $960 (software); Console: $3,000 (software)	Server: $8,500 (software),$15,000 (appliance); Sensor, $7,500 (software), $20,000 (appliance)	$8,495 (appliance)	Sentry full-duplex: $8,329 (software); ICEcap: $2,900 (software)	Sensor: $8,995 (software); Console: free (software)	$12,500 (appliance)	Open source (free)	$2,995 (sensor and console)

Y = YES N = NO