These troubleshooting tools sound alarms, plug holes and protect your network

Company name	Product name	Operating requirements	Primary function	Notification/management software interface	Automated responses to detected attack	Price
Gilian Technologies Inc. Chantilly, Va. 703-279-3672 **www.gilian.com**	**G-Server**	Hardware appliance; supports all Web servers compliant with HTTP 0.9/1.0/1.1 and HTTPS	Prevents Web site hacking and protects applications and networks from outside compromise	Can trigger SNMP traps, sends e-mail and pager messages and executes user-customized scripts that interact with their specific emergency procedures	Replaces hacked or fraudulent data so administrators can focus on forensic measures and other damage control	$39,900 per G-Server, $19,950 per G-Server Fail-Over System
Keynote Systems Inc. San Mateo, Calif. 650-403–2400 **www.keynote.com**	**Keynote monitoring services (includes Keynote Web Site Perspective and Keynote Transaction Perspective)**	N/A—subscription service	Outsourced, subscription services that measure Web site and application performance from multiple points on the Internet, providing insight into what your end users are experiencing; can be used to detect, alert, and diagnose and react to performance problems and availability of Web applications	Delivers alerts via e-mail (SMTP), pager and SMS message; also has SNMP interface for integrating external alerts with existing management frameworks and third-party monitoring applications; integration certified with CA Unicenter, IBM Tivoli and MicroMuse Netcool	N/A	Web Site Perspective $395 up per month per URL; Transaction Perspective $1,295 up per month per transaction
	Keynote Private Agents	N/A	Features measurement agents that can be configured to measure application performance anywhere on the Internet, intranet or extranet—including Web sites hosted on private networks and behind corporate firewalls for triage and diagnosis of performance problems	Delivers alerts via e-mail (SMTP), pager and SMS message; also has SNMP interface for integrating external alerts with existing management frameworks and third-party monitoring applications; integration certified with CA Unicenter, IBM Tivoli and MicroMuse Netcool	N/A	$3,500 up per month
	Keynote Red Alert	N/A	Mission-critical Web site monitoring service that can monitor the availability of virtually any TCP-enabled Internet device of your site every five minutes	Delivers alerts via e-mail (SMTP), pager and SMS message; has SNMP interface for integrating external alerts with existing management frameworks and third-party monitoring apps; integration certified with CA Unicenter, IBM Tivoli and MicroMuse Netcool; Keynote Red Alert delivers alerts when any IP-enabled device is 100 percent unavailable.	N/A	$50 up per month
	Keynote Test Perspective	N/A	Self-service solution lets you run diagnostic tests and load tests on demand; lets customers quantify operational capacity, ensuring they have room for critical applications during sudden traffic spikes	N/A	N/A	$2,500 up per month
	Keynote LoadPro	N/A	Load testing lets you dynamically test your applications, avoid over- or under-provisioning and determine the cost of not providing 100 percent availability	N/A	N/A	$6,000 up
NFR Security Inc. Rockville, Md. 800-234-8419 **www.nfr.com**	**NFR Network Intrusion Detection System**	Administration interface: Windows 2000, NT, XP; Central management server: Sun Solaris 7 or 8, Red Hat Linux 7.3; NID Sensor (hardware and software appliance with OS and sensor software embedded)	Monitors networks in real time, raises alerts when attacks or misuse are detected and actively responds when configured to do so	Sends system and alert messages directly to user console; uses NFR's Administrative Interface to process alerts, query the events database and configure sensors; can also interface NFR data using Tivoli, HP and ArcSight ESM	Sends e-mail, sets SNMP traps and triggers notifications to external programs	$7,500-$19,900
Symantec Corp. Cupertino, Calif. 408-517-8000 **www.symantec.com**	**Symantec Host Intrusion Detection System (formerly Symantec Intruder Alert)**	Agent machine: Win 2000 with SP2; console: Microsoft Internet Explorer 5.5 or higher	Delivers automated policy enforcement and incident response to servers, applications and data	Uses e-mail alerts, pager alerts and SNMP traps for broadcasting alerts from the Symantec Enterprise Security Architecture (SESA) Manager; local logging can forward alert notifications to the OS Event Log on the SESA Manager; notifications include e-mail, pager and on-screen alerts	Notifies administrators with an alarm and take countermeasures according to pre-established security policies; monitors events from standard system audit logs and monitors changes to the system registry	$975 up for single-server license
	Symantec ManHunt Multi-gigabit-speed network intrusion detection system	Host: Sun 64-bit Solaris 8 or Solaris 8 Intel Edition with full distribution; dedicated Sparc or Intel hardware; administration console: Win98, NT 4.0, 2000; Solaris 2.6, 7, 8	Performs detection, analysis and response to both known and novel threats, including intrusions, internal attacks and denial of service	Alerts are logged in the ManHunt database, viewed via the administration console; allows for notification via e-mail and SNMP traps, lets users send alerts via any custom preferred scripts or mechanisms	Policy-based responses can contain and control an attack and initiate actions required for incident response; provides logging and analysis capabilities to drill to captured packets and keystrokes for forensic details	$12,005 up
	Symantec ManTrap: Advanced decoy-based intrusion detection system	Host: Solaris 7 and 8 (Intel or Sparc) administration console: Win98, NT 4.0, 2000; Solaris 7 or 8 (Intel or Sparc)	Supplements security measures such as firewalls and intrusion detection systems with advanced decoy technology and early warning sensors; detects threats and enables attack diversion and confinement by becoming the target of the attack	Provides configurable and flexible alerting for situations such as networking events and processes that have been started on the decoy server; issues alerts via SNMP, SMTP, SMS Messages to cell phones, and alerts to the Symantec ManHunt Network Intrusion Detection System	Policy-based responses can contain and control attacks and initiate actions required for incident response; feeds data into Symantec ManHunt for correlated attack analysis; includes an e-mail generation program that creates simulated e-mail traffic	$7,350 up
Visionael Corp. Palo Alto, Calif. 650-470-8920 **www.visionael.com**	**Visionael NRM**	NT, Win 2000, XP, Solaris, HP-UX, Linux	Supports discovery, documentation, design, and configuration and change management in large enterprise networks; creates a central repository for all logical and physical network data and tracks the status of each network element in real time	Real-time alarms issued through integration with SNMP fault management systems including Remedy Action Request System and Clarify Trouble Ticketing	Discovery, collection, and validation and reconciliation of network topology and detailed physical network devices	$105,000 up