Intrusion Detection System (IDS): Perspective

By Gerald Arcuri and Kristen Noakes-Fry

(Published Jan. 23, 2001)

The increasing reliance on electronic commerce, the rise in the use of collaborative forecasting and planning among supply chain participants, and the growing use of self-service Web sites— in combination with increasingly complex networks—have, along with other factors, exposed network servers to unauthorized access attempts. Although most companies have in place adequate authorization measures and firewalls to stop external attacks, these measures represent only part of the security measures required to protect network and computer systems. Intrusion detection systems have become a critical component in managing the security of network and host systems.

Intrusion detection systems are one way to detect malicious hackers, and they are an important mechanism to protect critically important networking equipment and corporate data. An IDS may be a small price to pay compared to the financial (and possible public relations) damage hackers can create.

Technology basics

The need for intrusion detection

Primarily, networks have reached sophisticated levels of complexity in response to the evolving nature of the e-business processes. The driving force behind this business process evolution is that companies are being forced to open their networks to a wider audience in order to stay competitive.

This new audience includes teleworkers, trading partners, suppliers, and customers—many of which have access to sensitive internal data and unrestricted access to the enterprise's entire corporate infrastructure and the Internet. Each of these factors offers more opportunities for criminal activity or for unauthorized access attempts. The intrusion detection systems protect against both types of unauthorized access using several different methods.

International Computer Security Association (ICSA) research revealed that during 1998 a computer was attacked or broken into more than once per second. Such attacks can come from hackers that attempt to penetrate computer environments for criminal intent.

Some hackers attempt to circumvent security devices, such as firewalls that protect an intended target. Others attempt to alter critical system or data files in order to sabotage the system or steal important corporate data. Still others initiate denial of service attacks by flooding targeted segments of the Internet with a multitude of packets to prevent others from conducting business.

In addition to this criminal intent, inexperienced hackers (script-kiddies) can also pose an annoyance threat by attempting network intrusion for the thrill of it. Disgruntled employees are yet another source of potentially serious problems because they know system vulnerabilities:

- Many organizations believe that since they have firewalls or other types of security mechanisms at the boundaries of their enterprise they are protected from attacks originating from the Internet. However, that is not the case, for a variety of reasons. Firewalls are designed to allow some packets in (the authorized ones) and disallow others. The IDS complements the firewall to detect if those tunnels through the firewall are being exploited.
- Sometimes, firewalls and filtering techniques fail because of user configuration errors, hardware failure, or for a number of other causes. Intrusion detection systems can function as a second line of defense in these cases.
- Some users may install new types of software with unknown or proprietary protocols that are unknown to the firewalls. In many cases, these protocols can be detected by the intrusion detection system.
- Firewalls do a very good job of filtering incoming traffic from the Internet; however, there are ways to circumvent the firewall. For example, external users can connect to the internal

intranet via an unauthorized modem that does not pass through the firewall— with traffic that, obviously, the firewall does not see. If the threat comes from within the organization, for example from a disgruntled employee, the firewall does not recognize those threats because it monitors only traffic between the internal and external network.

An *Intrusion detection system (IDS)* monitors computer systems and network traffic and analyzes that data for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the enterprise. The main advantage of an intrusion detection system is that it provides a view of server and network activity and issues alerts notifying administrators of unauthorized or unusual activity.

Types of intrusion detection systems

Currently two primary types of intrusion detection systems are available: host-based and network-based. Some vendors market either a host-based or network-based type of product; however, the trend is to provide an integrated approach that combines both types of products into a centrally managed product that improves network resistance to intrusions and provides greater flexibility in deploying the products.

This evolving integrated approach will support an integrated event database and reporting capabilities to provide a more seamless approach to network and security management.

Host-based system

With the host-based system, the intrusion detection software resides on a server and monitors the server (and some application) logs for unauthorized access attempts and aberrant behavior patterns. The security administrator authors the host-based rules that trigger the analysis of the audit and event logs. The host-based system can then evaluate those actions such as user or login activity or user account and application activity.

The host-based systems analyze audit and event logs to look for aberrant patterns of local or remote users that may indicate unauthorized attempts to enter the system.

For example, some host-based systems may issue an alert if a sales clerk attempts to gain access to payroll data. A host-based IDS may also perform statistical analysis on information looking for patterns of unusual activity, such as multiple failed login attempts.

Despite the positive efforts of these systems, there are limitations.

For example, because the host-based systems use event logs, they do not operate in real time. And those systems that use statistical techniques to monitor abnormal patterns have the difficult task of recognizing "normal" behavior.

Because of this difficulty, these systems have the challenge of minimizing false positives, or false alarms, while simultaneously effectively trapping intruders. Thus, this type of statistical analysis is currently more common on host-based systems because of the local nature of the activity.

The biggest negatives of host-based systems are:

1. If a host is put on the network without the IDS agent, the host is unprotected
2. If the host has anyone besides security folks who have admin privileges, very often the IDS agent will be disabled if it appears to get in the way of production software.

Network-based system

The network-based type of IDS resides as an agent on LAN servers in the form of a sensor. It filters and analyzes network packets in real time and compares them against a database of known "attack signatures" or patterns. The attack signatures are known methods that intruders have employed in the past to penetrate a network.

Typically four techniques are used to recognize attack signatures:

- Pattern or byte-code matching
- Threshold crossing
- Correlation of lesser events
- Statistical anomaly detection

If the packet contents match an attack signature, the IDS takes appropriate countermeasure steps as enabled by the network security administrator. These countermeasures can take the form

of a wide range of responses. They can include notifications through Simple Network Management Protocol (SNMP) traps or issuance of alerts to an administrator's pager, e-mail or phone.

Responses can also take the form of the creation of a log or the recording of a network session; or the most aggressive type of response can include connection termination, automatic reconfiguration of the firewall to block the source IP of the offending packets, or the execution of a specific program.

This signature type of analysis (as opposed to the statistical analysis approach discussed below) has the advantage of producing a low rate of false positive alarms, but is limited by the difficulty recognizing new types of attacks not in its repertoire of attack signatures. Therefore, these types of systems must be updated to remain current.

In order to offer a more granular approach to unauthorized detection, some network-based intrusion detection systems can also monitor command structures and analyze protocol-specific information. Others can analyze requests for sensitive information or repeated attempts to circumvent security features and take appropriate action if the activities fall outside of predefined thresholds. However, this type of analysis can pose problems and raise the number of false alarms because defining thresholds for a wide range of activities can be difficult and time consuming.

A Network-based IDS can work with encrypted networks and generate so much data that it can be very expensive to analyze all the data.

Table 1

Strengths and Weaknesses of Host-Based and Network-Based Intrusion Detection Systems

Host-Based Systems	Network-Based Systems
Strengths	
Monitor both incoming and outgoing traffic on a specific host system.	Operates in real time and employs unobtrusive passive monitoring techniques.
Not impacted by network encryption because the files have been unencrypted before entering the log file. This is in contrast to network-based systems, which encounter encrypted payloads. Encrypted network files are unencrypted for entry into the log.	Minimal system resource usage.
Provides better application layer protection than a network-based IDS because it can monitor failed login and application execution attempts.	Typically platform independent because it resides on the network; most are relatively easy to deploy.
Functions well in network-based encrypted environments because by the time the host-based system sees incoming network traffic it has been decrypted.	Because it reads packet headers, which a host-based IDS does not, it detects attacks that host-based systems do not.
Functions well in switched environments because they can be located on as many hosts as required.	Detect problems before they reach the targeted system.
Weaknesses	
Requires up-to-date and installed attack signatures, which can be expensive to update and distribute.	Requires up-to-date and installed attack signatures, which can be expensive to update and distribute.
Does not operate in real time.	Has a tendency to generate false positive alerts about attacks when using statistical analysis techniques.
Only protects a specific computer system.	Many are not integrated into enterprise network management systems, requiring two monitoring stations.
Can put stress on local resources, such as disk storage and memory.	It may not be able to know with certainty that an attack was successful, unless it has information on the system being attacked.
Provides no protection for the network traffic, which means it	If the attacker is logged into the computer

does not read the packet headers that the network-based IDS monitors.	being attacked, no information of the attack would travel the network, and the attack would be unrecognized by the network-based IDS.
Can only recognize attacks on systems running their software agents.	Difficulty handling traffic more than 65 Mbps.

Complimentary products

In addition to intrusion-detection systems, there are a number of complementary products that organizations should be aware of and consider as their networks become more complex and as their need for security protection grows. The following security products and technologies can be used in conjunction with intrusion detection systems:

- *Firewalls* are deployed in nearly all organizations today and are typically one of the first security mechanisms deployed to protect the perimeter of the network. Typically firewalls protect computers from external attacks, but increasingly companies are deploying firewalls to compartmentalize internal departments, for example, separating R&D from the rest of the organization or segregating accounting and the rest of the organization. In addition, many companies are also now deploying Internet firewalls to monitor access from the Internet and control the services that are allowed.
- *Antivirus software*, like firewalls, is one of the first security measures deployed by enterprises. Antivirus software has done an excellent job of protecting corporate networks against known and traditional viruses. However, today most antivirus software vendors are evolving toward file content review and protection in order to protect networks against malicious code arriving through the Internet, or mail or Web servers.
- *Vulnerability assessment tools* are derivatives of intrusion detection systems. But unlike an IDS, which scans for attempts at unauthorized system use, vulnerability assessment tools scan for security holes or flaws that may lead to potential problems. They allow consistent auditing and diagnosis of system configuration settings that may contribute to security problems.
- *Virtual Private Networks (VPNs)* are increasing in popularity as an inexpensive alternative to leased lines or frame relay services and as a method of exchanging information securely over the Internet. Based on the IPSec protocol, VPNs provide authentication and encryption mechanisms to ensure the security of data traversing a public network. As Internet traffic and e-commerce increase in usage, and as mobile PCs are used to connect to the enterprise network, VPNs will become increasingly more prevalent.
- *Public Key Infrastructure (PKI)* is a technology that provides strong authentication for organizations conducting secure transaction-processing applications. It includes the issuance of digital certificates, which verify the identity of the person involved in the transaction, and the use of a dual-key (one private and one public) system to ensure security. PKI is still in its infancy, but will likely increase in usage with Windows 2000, which has an integrated PKI that enables the secure exchange of information across the Internet, extranets, and intranets.

Technology analysis

IDS is not a panacea

Despite the positive impact it can have on an enterprise, no IDS is foolproof and certainly should not be the only security measure an organization should employ. Several cautions should be considered when intrusion detection systems are deployed:

- *Strong identification and authentication is still required.* An IDS uses very good signature analysis mechanisms to detect intrusions or potential misuse; however, organizations must still ensure that they have strong identification and authentication mechanisms in place. These can include passwords, smart cards, challenge/response tokens, or biometric devices.
- *Intrusion Detection Systems are not a solution to all security concerns.* They perform an excellent job of ensuring that intruder attempts are monitored and reported; however, these

systems represent only one important link in a comprehensive corporate security solution designed to protect critical corporate computing and networking assets. In addition, companies must employ a process of employee education, system testing, and development of and adherence to a good security policy in order to minimize (but not eliminate) the risk of intrusions.

- *Firewalls are not enough.* Many organizations believe that since they employ a firewall they have enough security protection. However, intrusion detection systems are good complements to firewalls. Although firewalls provide good protection against intrusions from external sources, like the Internet, organizations should realize that not all access to their enterprise infrastructure occurs through the firewall, particularly with impatient employees who may establish an unauthorized modem connection to the internal intranet.
  Similarly, organizations must understand also that not all intrusions occur outside of the firewall. For example, some employees may accidentally or maliciously try to access files or systems with authorization. This activity might be caught by the host-based rules, but not by the network-based monitoring, so the firewall would never be part of the defense mechanism for this type of employee activity. Since these attempts do not pass through the firewall, they would be undetected without an IDS.
- An *IDS is not a substitute for a good security policy.* As with other security and monitoring products, an IDS functions as one element of a corporate security policy. Successful intrusion detection requires that policy must be followed to ensure that the IDS—among other elements of a security program—is followed and intrusions and vulnerabilities, virus outbreaks, etc., are handled according to corporate guidelines.
- *Detecting unknown threats is still difficult.* Despite the talk about the use of statistical analysis and artificial intelligence, IDS still cannot protect systems proactively against new forms of attack. Anomaly detection is employed to alert administrators about unusual activity, but this type of technique has the problem of a high number of false alarms, which can be expensive for organizations to manage with respect to staff time wasted chasing false leads.
- *Human intervention is still required.* While the IDS can identify that an intrusion has occurred or is in process, and it may be able to provide the intruder's IP address, the security administrator or network manager must then investigate the attack, determine how it occurred, and correct the problem. Human intervention is also required to recognize false alarms and override possible system lock out for those occasions. This need for human intervention should drive many organizations to look at the IDS as a service and to consider outsourcing IDS monitoring.

Business use

Currently intrusion detection systems are used primarily by security-aware firms, such as banks, financial services companies, and other organizations with high-availability networks. However, a number of market and technology factors are driving the interest and growth in intrusion detection systems:

- As intrusion detection technology matures, more organizations will be drawn towards the benefits it offers. Some of the larger IDS vendors are moving toward incorporating intrusion detection management with enterprise network and system management systems. As this trend evolves, the management of the intrusion detection process with managing the entire health of the network will reside on a single console.
- The increasing complexity of networks and the accompanying huge investment in networking equipment and personnel will become a strong incentive to encourage corporate executives to invest in intrusion detection systems. The loss that an intruder can inflict on a network and a corporation's critically important data can be staggering relative to the price of an IDS.
- As electronic commerce continues to grow, and as more companies open up their networks and files to trading partners, suppliers, and customers, the use of host-based intrusion detection systems will rise across all industries and companies of all sizes in order to offer increased protection against unauthorized activity.

?? As enterprises complete deployment of other security basics, such as security procedures and policies and the implementation of antivirus software and firewall functions, more companies will recognize that intrusion detection is an excellent complement to these security measures.
?? As intrusion detection management improves, more companies will recognize the benefit of the systems and find them easier to use. This will occur even for companies that do not require the IDS management integrated with a corporate network management system.
?? Options for outsourcing intrusion detection services will entice some organizations to move toward this security measure. The growth in intrusion detection services, combined with the paucity of skilled technicians with IDS experience, will drive the growth for services.

Benefits and risks

Benefits

Additional levels of protection

An IDS can provide additional layers of protection in the enterprise. Because intrusion detection systems monitor the operations of other security devices including firewalls, some routers, and other internal files used by other security devices, they can provide an added level of security if those devices fail.
Some companies also use an IDS to scan for compliance with company network usage policy and, as part of that process, to analyze suspicious activity.

Easy to sell to upper management

IDS is growing in importance. As more companies experience external attacks and employee abuse of connectivity privileges and as more companies willingly open their network to trading partners, intrusion detection systems will become increasingly important as a device to protect corporate information and networks. As a result, the business value of an IDS will become easier to sell to upper management.

Supports policy development

An IDS can help develop security policies. Since many vendors provide intrusion detection systems as part of a full suite of security protection, a company without a fully developed policy can employ the guidelines included with many intrusion detection systems.

Risks

IDS cannot do the job alone

IDS can provide a false sense of security. Some organizations may believe that an IDS can detect all attack patterns and, thus, it is the only security measure required. An IDS should be deployed as one element of an integrated, enterprise-wide security program.

An IDS cannot replace a security policy and planning

A risk with many security technologies is the tendency of many companies to act as though the security product can compensate for the lack of a security policy. As mentioned earlier, IDS technology, like other security technology, serves to implement policy. In addition, poor planning can effect the financial position of a business adversely (because of costs incurred resulting from intrusions) and place an increased burden on the technical staff (who will have to deal with the likely occurrence of security problems).

The IDS market is fairly new

The IDS market is so new that— other than among companies and industries that are traditionally early adopters of security technology— the need for this technology is not generally recognized. However, as networks increase in complexity, and as more intrusions are successful and wreak financial havoc, the interest in the IDS will grow.

Standards

Since intrusion detection is an emerging and growing technology, the standards efforts on its behalf are also in the development stage:

- The Internet Engineering Task Force (IETF) Intrusion Detection Working Group (IDWG) and Common Intrusion Detection Framework (CIDF) are tackling standards issues that encompass all aspects of intrusion detection—communication protocols between sensors, signature representation, etc. Internet draft versions of the *Intrusion Detection Exchange Format Requirements and Data Model*, the *Intrusion Alert Protocol,* and the *Intrusion Detection Message Exchange Format XML* have been completed. However, requests for comments (RFC) have not yet been issued.
- Standards important for an IDS are included in the Common Vulnerabilites and Exposures (CVE) sponsored by Mitre Corp. A database of standardized names for vulnerabilities and other information security exposures, CVE provides standardized terminology to provide a baseline for evaluating the coverage of security tools. A number of IDS products are currently under evaluation for inclusion in the CDE list of products that conform to the naming standard. Some members of the CVE Editorial Board also participate in the IDWG and CIDF.

Selection guidelines

Selection guidelines for intrusion detection systems involve both business- and technology-related issues. The following factors should be considered and questions answered as part of the selection process for intrusion detection systems:

- Before IDS specifications are defined and the types of IDS evaluated, the deployment of an IDS must be endorsed at the executive level.
- If an IDS is supported at the executive management level, policy must be established on how to handle intrusions. Typically this policy becomes part of a larger, corporate-wide incident-response guideline.
- Organizations should realize that the deployment of an IDS will require not only system and personnel resources before and during implementation time, but resources will also be required to deal with intrusions during operation. This will require not only networking and system management resources, but also possible legal resources.
- For systems that need attack signature updates, corporations should inquire how and how often the vendor updates the signatures. Some companies may prefer a push technology to encourage system updates; however, none is currently available. This will likely mirror the process endorsed by the antivirus vendors, as the IDS market matures.
- A variety of automated response mechanisms are available, such as system or port shut down, administrator notification, diversion to decoy system, etc. Organizations should ensure that the responses offered complement their security policies.
- Companies should also inquire if the IDS can work in conjunction with network management activity, and if network device management is planned in conjunction with security monitoring.
- The option of working with a vendor that can provide IDS as a managed service should be evaluated alongside the "build your own" approach.

Technology leaders

Several vendors are emerging as market leaders for network-based and host-based intrusion detection systems. Some, like Cisco and Computer Associates, are large, well-financed organizations with established products and huge marketing budgets; others such as Internet Security Systems and Axent (acquired by Symantec in July 2000) are smaller, but have excellent name recognition in the security market place.

And some like Network Associates and Computer Associates have broad portfolios of security products that can include not only intrusion detection, but also firewall, antivirus software, VPN, vulnerability assessment, and risk and security management, to name a few.

Table 2

Vendors That Provide Host-Based and Network-Based Intrusion Detection Systems

Host-Based Products	Network-Based Products
Axent Technologies' Intruder Alert *(1)*	Axent Technologies' Net Prowler *(1)*
CyberSafe's Centrax (through an affiliation with Tripwire Inc.)	Cisco Secure Intrusion Detection System (formerly NetRanger)
Internet Security Systems RealSecure *(2)*	CyberSafe's Centrax
Intrusion.com (formerly ODS Networks) Secure Enterprise (formerly CMDS)	Computer Associates eTrust Intrusion Detection (formerly SessionWall-3)
Intrusion.com's Kane Security Monitor *(3)*	Internet Security Systems RealSecure *(2)*
Tripwire, Inc. Tripwire 2.2.1	Network Associates' CyberCop
	Intrusion.com's Kane Border Patrol *(3)*
ClickNet	Network Flight Recorder's NFR Intrusion Detection Appliance
(1) Axent introduced the integration of Net Prowler and Intruder Alert in mid-2000 with the Prowler IDS Series.	
(2) Intrusion.com became the exclusive license of RSA Security's Kane Security products in September 1999 for North America and Western Europe.	
(3) Internet Security System's RealSecure integrates both host-based and network-based intrusion detection functions.	

Axent

Axent's Intruder Alert is the leader in the *host-based* intrusion detection market, but Axent has integrated that product with its NetProwler network-based IDS to create its new Prowler IDS Series. Intruder Alert monitors all critical systems for abnormal patterns of use and responds to prevent further intrusion; NetProwler provides dynamic network intrusion detection.

It employs a Stateful Dynamic Signature Inspection processor that monitors known and new security flaws, but also protects corporate applications through an attack definition wizard. A new enhancement to the Prowler IDS Series is Axent's administrative console that lets administrators drag and drop specific security policies and attack signatures into predefined systems groups within certain business functions, such as e-commerce transactions or Intranet servers. *Note: Axent was acquired by Symantec on 27 July 2000. It will be several months before the transaction is complete, and the status of Intruder Alert within the new product catalog is clear.*

Internet Security Systems

Internet Security Systems (ISS) is the leader in the *network-based* IDS market with its RealSecure system, which is one component of ISS's family of SAFEsuite security solutions, which also includes security assessment and management capabilities.

ISS is one of the few vendors in the market that has successfully integrated its network-based and host-based intrusion detection system with its RealSecure version 3.0 introduced in January 1999. The software uses two classes of integrated detection components: Detectors, which enforce security policy, and Managers, which configure the detectors and perform management functions.

Cisco

Cisco's Secure Intrusion Detection System, formerly called NetRanger, is also a serious contender in the network-based IDS market. Other Cisco security products include firewalls, encryption and authentication devices.

Cisco Secure IDS incorporates two components: Sensors and Director. The Sensors, high-speed, real-time-based network appliances, analyze the content of network packets to determine if they are authorized. The Director, a software-based management system, centrally monitors the

sensor activities in all network segments to enable the network manager to locate the attack, qualify it, and respond.

Computer Associates International

Computer Associates' SessionWall intrusion detection system is now part of its eTrust initiative, which is designed to extend security to the electronic business environment. The eTrust product line consists of a series of integrated products including antivirus software, encryption, VPNs, firewalls, and certificate validation.

The eTrust Intrusion Detection monitors both internal and Internet network traffic and detects intrusions and service denial of attacks, detects suspicious and malicious Java and ActiveX applets, and also detects viruses in the network. Based on the results of the monitoring, it can provide real time or subsequent responses based on the corporate security policy.

Intrusion.com (formerly ODS Networks)

Through a series of acquisitions, Intrusion.com (formerly ODS Networks) has expanded its security portfolio to include Kane and SecureNet Pro security software for intrusion detection and vulnerability assessment and the SecureCom security platform that provides Internet security appliances. Kane Secure Enterprise (formerly called CMDS [Computer Misuse Detection System]) is a host-based IDS for Windows NT, Solaris, CheckPoint Firewall-1 and Cisco routers.

It uses a signature-based expert system and statistical profiling to detect intrusions and automatically processes event logs for security and policy infractions. Kane Border Patrol monitors firewalls and routers for signs of packet flooding, protocol and distributed denial of service attacks at the Internet connection.

SecureNet Pro, acquired from MimeStar in July 2000, is a network-based IDS that complements the company's host-based Kane Secure Enterprise product. SecureNet Pro functions as a stand-alone network-based system; but Intrusion.com plans to integrate it with the Kane Secure Enterprise product.

Newer enhanced offerings and a view of what's to come

Many vendors have been taking steps to extend the functions of intrusion detection systems. These extensions include integration of network- and host-based systems, links to enterprise network management systems, and support for a broader variety of intrusion types. Descriptions of some of these enhancements follow:

- Some vendors have begun offering integrated network- and host-based systems. Some of the vendors/products employing this strategy include Internet Security Systems (ISS) with RealSecure; Axent with its Prowler IDS Series; Network Associates with its CyberCop Monitor; and CyberSafe's Centrax (through a partnership with Tripwire Inc.)
  Axent and Cisco, among others, have begun integrating their intrusion detection functions into a firewall. The intrusion detection software activates filters if the software detects an intrusion; however, this process is still in its infancy.
- Recourse Technologies has developed products to extend the capabilities of traditional intrusion detection systems. ManTrap employs a decoy environment to trap intruders and track their activity for possible criminal prosecution. To protect systems, ManTrap resides in a demilitarized zone (DMZ) and works with the firewall to redirect suspicious traffic to the trap. (Note: A DMZ is a series of computers that use routers and gateways to protect them from both trusted network and the untrusted networks.) ManHunt, available in late 2000, identifies an attack and begins determining the source of the attack and provides that information to other networks, such as a network service provider. Network Associates' CyberCop Sting also provides a decoy environment which employs an advanced analysis tool to collect and employ the source and techniques of an intruder attack.
- Some IDS vendors are also linking their software with enterprise network management systems so that organizations have a single view of the network that also incorporates results from intrusion detection. With this approach, intrusion detection systems can activate a response across a range of network equipment when an intruder is identified. For example,

Axent's Intruder Alert can be tied to Tivoli, HP OpenView or BMC Software system management capabilities; ISS RealSecure provides plug-ins to HP OpenView and Tivoli.

?? Computer Associates' eTrust Intrusion Detection System monitors a wide range of intrusion types. These include service denial attacks, mobile code (Active X and Java applets), attacks on known cracks in application and operating system code, application and operating system password hacking, and message content hacks.

?? CyberSafe's Centrax has begun offering a new type of network protection called network node intrusion detection, which runs on each server and workstation, to ensure that network-based attacks are detected regardless of network load, encryption or hardware switches.

Insight

IDS products can monitor host-based system log files and real-time network events so that network managers or security administrators have a view of events occurring on the network. An IDS can add a different dimension to the security infrastructure because it can monitor intrusion attempts from both inside and outside the company, as well as detecting anomalous behavior patterns that could reflect malicious intent. However, no security technology is capable of handling every threat.

Despite the importance of an IDS, it cannot be used alone, but must be part of a larger corporate security program that includes—in addition to antivirus software and firewalls—vulnerability assessment tools, VPNs, and possible PKI. The tools, then, must be surrounded by a common sense well-articulated corporate security policy that is enforced across the enterprise fairly.

As this technology matures, and as the IETF finalizes the IDS interoperability standard, demand for the product will grow. Its importance will be recognized outside of the early adopter market segments, such as banks and financial services companies, and will likely become as ubiquitous as firewalls.