AT&T Managed Intrusion Detection/Managed Intrusion Prevention Services

The Need for Real-Time Security Management

As IP networking and e-business continue to expand, the need for protecting networks against malicious intruders and unauthorized activities becomes even more critical to businesses. The spiraling threats of cyber attacks and increased vulnerabilities are resulting in rising costs, causing network security spending to outpace overall IT expenditures. AT&T Managed Intrusion Detection/Prevention Service (MIDPS) is designed to detect and respond quickly to these types of malicious activities. AT&T MIDPS provides the same type of protection for networks as a security camera does for physical property. The intrusion detection/prevention sensing components placed at various points in your network act as “security cameras” for your network traffic. The sensing components monitor data packet headers and payload information to detect possible malicious activities and respond swiftly with actions based on your pre-defined security posture. A Host-Based intrusion detection/prevention option is available within the Managed Intrusion Detection/Prevention portfolio. This option consists of security software installed on customer servers or hosts as commonly referred to. These servers are generally located at AT&T Data Centers. The intrusion detection/prevention security software monitors the networking subsystem on operating systems to determine if new Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) services are started, or if existing services have stopped.

Managed Intrusion Detection Service

Benefits
- Utilize AT&T technical expertise and world-class customer service and support
- Focus on core business functions by saving time, money and effort to design, monitor and upgrade network security
- Help detect malicious activities and respond quickly
- Provide another defensive layer of security for your network
- Enforce Threat and Policy Violation Detection and Containment to help contain threats that may not be detected
- Meet corporate and business objectives – help reduce costs help maintain business continuity
- Compliance With Federal Regulations – to Sarbanes Oxley, HIPPA, GLBA and SAS 70 rules
- Easy Deployment without signatures or desktop software agents

Features
- Customized AT&T MIDPS Security Posture (Relaxed, Moderate, Strong)
- Dynamic Access Control List (ACL) creation in the screening router to shun attacks
- Out-of-band management with state-of-art security features
- Support of multiple manufacture models and bandwidth
- Internet Provider Agnostic
- AT&T Security Network Operations Center – monitoring and technical support
- Critical Event Notification
- Real-time online interactive reporting
Maximum In-Depth Protection

AT&T Intrusion Detection/Prevention Service is a fully managed, comprehensive, IP network attack recognition and response solution for network security. There is a premises-based hardware/software solution option with AT&T providing the hardware/software components and continuous support through the AT&T Security Network Operations Center.

The Host-Based intrusion detection/prevention option includes monitoring of files for permission change, size and ownership alteration. Monitoring system resources exceeding configuration thresholds, defending against system core compromise and log file attacks are all part of the in-depth protection.

This fully-managed service also includes maintenance procedures, installation and day-to-day management. In addition, hardware/software maintenance and required upgrades are performed continuously. You have direct input on how the security posture is implemented for each installation.

Sophisticated and Effective Network Security

AT&T Managed Intrusion Detection/Prevention Service monitors network traffic for potential misuse from internal and external sources via an unaddressed monitor port on a switch. The insertion of this switch does not affect IP traffic performance. Upon recognizing a pattern of misuse, such as suspicious or unauthorized activity, the system automatically and quickly responds according to your predefined policies to send an alert and take immediate action.

Intrusion Detection Sensors (IDS) located at your site use a signature-based approach to perform real-time intrusion detection or prevention if configured at the network level. This involves the capture and real-time analysis of IP packets “signatures” by performing both context and content monitoring.

- Context monitoring entails the examination of the IP packet header data
- Content monitoring evaluates the assembly and examines the data content of a single or series of IP packets

The system then evaluates each digital signature against a known database of over 1,000 existing attack signatures. The signature database is continually updated as computer security organizations develop new signatures. You may designate multiple custom signatures per sensor in order to monitor and respond to specific security related criteria.

To effectively monitor and manage hundreds of signatures, the system also has the ability to “remember” what has happened and compare this with past and current sessions. Some attack signatures contain a string of packets, and in order to identify those attack signatures, the system must “remember” the order and type of packets and headers that have passed the sensor.

Intrusion Prevention Mode

When configured in intrusion prevention mode, the AT&T Intrusion Detection/Prevention Service uses a combination of detection mechanisms to increase the speed and accuracy of detecting suspicious activities. For example, the service performs the following functions to identify malicious traffic:

- Monitors who a sender is communicating with and how often
- Tracks traffic to unused IP addresses and uses deception technology to help slow and block attacks
- Identifies packets that violate protocol standards and conducts reconnaissance
- Identifies machines that perform DNS lookup; only mail servers should perform this function
- Looks for “cyber offenders” performing “low and slow” scanning techniques
- Looks for spoofing, where the initiator changes the appearance of a packet’s source, and can result in a Distributed Denial of Service attack
- Helps prevent unauthorized traffic on IP Telephony network segments, DoS and spoofing

Proven security expertise along with the AT&T global portfolio of managed security services can give you some of the most powerful weapons available today in the battle against cyber-security attacks.

For more information about AT&T Managed Security Services, visit us at www.att.com/security, call us at 877 954-7771 or email us at mss@att.com.