Sophisticated Needs
Due to the increased volume of Internet related computer threats, companies are in greater need of detection tools and solutions that will help them protect against malware penetration and business interruptions.

As a result, many companies rely on off-the-shelf intrusion detection software solutions to protect their private networks from Internet threats. However, such solutions can be generic and offer features rarely used by the customer. Also, in addition to paying for rarely used features, these solutions can drive increased cost through maintenance and support needs. This is particularly true for growing companies.

As your business grows, you should consider a more robust and up-to-date solution for your VPN to help avoid potential business interruptions from malicious attacks while avoiding unnecessary increased costs.

Protection Just for You
Private Intranet Protect, an option of AT&T Internet Protect service, is a fully managed Internet security service designed to analyze traffic on your VPN to detect intrusions, cyber attacks, and other potentially threatening identified anomalies. Not only does Private Intranet Protect offer you alerting and notification of outside threats, it also identifies and analyzes threats within your AT&T Enhanced Virtual Private Network or AT&T Virtual Private Network using Managed Router Services.

Potential Benefits
- Provides detailed security traffic analysis
- Enables pro-active security analysis within and outside the private network
- Network-Based service — Requires no additional hardware or software

Features
- Threat Analysis
- Custom Policy Creation
- Reporting
- Convenient Private Portal

Private Intranet Protect Architecture Overview
By analyzing your VPN traffic, this service detects the following threats below before they have a chance to damage your network:

• Worms/scanning
• Zero day events (attacks that exploit software vulnerabilities that are too new to be well-publicized)
• Dark address space activity
• Denial of service attacks
• Protocol misuse
• Global security threats
• Phishing attacks

Private Intranet Protect analyzes your complete private network traffic, and in combination with AT&T Internet Protect, is designed to monitor and analyze traffic both within your network and on the AT&T backbone.

Private Intranet Protect also offers prevention tips to help you take appropriate steps to protect your enterprise. Through the Private Intranet web portal, you have access to detailed traffic analysis views and security information about your private network.

What are the Components?
Private Intranet Protect does not require any additional bandwidth or premises equipment purchase and is comprised of the following components:

• Collectors that collect un-sampled NetFlow data from routers, compress it, and send the data to the Controller
• Controllers that analyze compressed NetFlow data that they receive from one or more Collectors. The Controller is designed to detect known patterns of anomalies in the data and generate alerts
• The Portal that shows current and past status events that occurred on your VPN

How Does it Work?
Private Intranet Protect collects unsampled NetFlow data from your routers and uses heuristics and statistical models to help predict and profile security threats and malicious activity. That means the service reviews conversations in your network to help detect anomalies. The service compares your VPN traffic against a baseline for normal behavior. If abnormal traffic patterns occur repeatedly and AT&T determines it suspicious, you’ll receive an alert via email or text message with the threat’s severity level. Your network team can then determine the course of action.

The service features are as follows:

• Convenient Private Portal – The portal provides you with essential information such as the highest priority vulnerabilities and recent patch releases
• Customizable Features – You can create custom policies to help detect specific network security events or monitor specific network activity
• Threat Analysis – AT&T gathers Internet traffic from the AT&T IP backbone, one of the largest in the world, and searches to identify anomalies as either known attacks or as threats that require immediate action. We then provide this information to you via Active Threat Feed, a service that delivers threat information directly to your security teams. Because of our advance intelligence gathering, you get expert advice on what to do and how to do it quickly
• Reporting – The Private Intranet Protect portal stores one year of historic NetFlow data from your network. You can also request detailed reports for any period in the previous year. These reports detail the activities and policy violations that occurred during the reporting period. You can request these reports in PDF, email or XML format

Let AT&T help you protect your network against malicious attacks and the losses associated with network security breaches by implementing Private Internet Protect, an option of AT&T Internet Protect.

For more information contact an AT&T Representative or visit us at www.att.com/network-security, or call 877.542.8666.