The use of wireless mobile devices to access an organization’s private network has become standard practice across all industries. As the number of mobile and un-tethered devices accessing network applications continues to grow, so does the security risk. At the same time, the Internet has left data resources vulnerable to a variety of potential outside threats and attacks. As a result, it has become critical to protect your information assets with a comprehensive security strategy that helps provide highly secure access while supporting your organization’s infrastructure. Mobile attacks are increasing rapidly in number and sophistication, and hackers continue to be financially motivated to steal data, identities, and intercept agency communications. These occurrences should be among the top concerns for an organization that relies on mobile devices and tablets to fulfill their mission.

AT&T has been focusing on network security for most of our history. We have been at the forefront of many developments that have become today’s network security best practices including a security governance/policy model, risk management methodologies, defense-in-depth security design, firewalls, threat management and analysis, and security event correlation. So, it’s only fitting that, to address the challenges of mobile security, AT&T is using our expertise in network security to help protect an organization’s assets through wireless access.

Mobile security solutions typically scan for security risks only at the device-level, using application controls and anti-virus/anti-malware scans. As shown in Figure 1, multi-layer and carrier grade AT&T Mobile Security goes further by adding network-based security controls to maximize your organization’s wireless security and help defend against unauthorized applications, e-mails, and disruptions in operations. Network security provides access to an organization’s Virtual Private Network or VPN, the Internet, or cloud-based services as well as additional traffic filtering and scanning. By integrating device-level security

Benefits

- Helps protect personal and sensitive information and guards against unauthorized use
- Helps maintain compliance with government and industry regulations
- Less disruption to service and operations by helping to protect data
- Better protection for your mobile assets and network from increased threats
- Centralized enforcement of unified agency security policy across wireless and wireline assets
- Multiple layers of security – at the device and in the network
- Integration with AT&T Remote Access services, AT&T VPN services, and AT&T Secure Network Gateway for more granular network security options
- Manage employee owned or agency provided devices

Features

- Data-in transit FIPS 140-2 compliance
- Administration Console
- Anti-Virus/Anti-Malware device scanning
- Prohibited Application Alert
- Secure Socket Layer (SSL)
- Network Address Translation (NAT) Firewall that hides the private IP addresses of the mobile device
- BotNet Identification
- BotNet Black List/White List
- Policy Routing
- Enhanced options for AT&T Secure Network Gateway

Figure 1. AT&T Mobile Security service and the points in which the security policy and controls are applied.
features with network-based security controls and encrypted transport, AT&T Mobile Security provides a holistic approach to mobile security. And, it’s available even if you aren’t an AT&T wireless customer.

**Make AT&T Mobile Security an Integral Part of Your Security Solutions**

AT&T Mobile Security better provides protection for mobile devices as well as the AT&T VPN that the devices are accessing and enables you to synchronize your security policies between the two. AT&T Mobile Security service is an application that is installed on the end-user’s mobile device that helps enable device-level security features and provides a highly secure connection to the AT&T virtual private gateway. The network security features and policies applicable to your organization are enabled in the AT&T virtual private gateway.

AT&T Mobile Security service also provides a web-based administrative console that gives organizations the ability to manage and control security policies across wireline and wireless assets. This service also allows you to connect to the AT&T Secure Network Gateway platform as well as other AT&T services, including remote access and AT&T VPN.

Because viruses and malware may cause unwanted billing issues and breaches of valuable user data that render mobile devices unusable, AT&T offers an array of device security capabilities and solutions to assist you in heading off security threats to your mobile users. These include:

- Anti-virus scan on devices and memory cards helping to protect mobile devices against viruses and malware while alerting the user when harmful content is detected;
- Anti-virus and anti-malware heuristic detection providing behavioral-based spyware detection; and
- Prohibited/Malicious Application Alert feature that scans a device at specified time intervals (e.g., daily, weekly) set by you and notifies users if any harmful applications are detected on their devices.

Network Security features and functions are comprised of:

- Secure Socket Layer (SSL) protocol to access your network through a private and encrypted tunnel;
- Network Address Translation (NAT) Firewall that hides the private IP addresses of the mobile device;
- BotNet Identification that informs the user if their device has been infected as a Bot;
- BotNet White List/Black List that prevents users from going to BotNet sites;
- Root/Jailbreak detection which provides the availability to detect if a device has been rooted or “jailbroken” and prohibit the device from establishing a connection to the network;
- Policy Routing which is the ability to control user access to the Internet, cloud or your private network; and
- Enhanced options available by connecting to AT&T Secure Network Gateway, Network-Based Firewall, URL Filtering, Intrusion Prevention Service.

**AT&T Mobile Security with AT&T Managed Trusted Internet Protocol Service (MTIPS)**

AT&T has integrated AT&T Mobile Security as Feature 9 to the Managed Trusted Internet Protocol Service (MTIPS) offering under the GSA Networx Universal and Enterprise contracts. To order AT&T Mobile Security, a federal customer must first order the MTIPS basic service and add MTIPS Feature 9 to the order request. AT&T integrated AT&T Mobile Security into MTIPS so that federal customers would be able to order and receive a mobile device security service that is tied to a Trusted Internet Connection (TIC) solution. By integrating the security features of AT&T Mobile Security with those delivered via AT&T MTIPS, AT&T delivers a robust solution that will help you strengthen your security defenses.

MTIPS from AT&T is a managed TIC service that encompasses TIC portals, transport collection and distribution, customer-premises managed firewall, Security Operations Center (SOC), service management and network operations. AT&T Mobile Security Service, built on the same platform that supports the MTIPS offering, provides a breadth of security features including: Firewall, NAT, URL Filtering, and Antivirus services. Figure 2 below illustrates the new AT&T Mobile Security platform and its relationship to the existing foundation of the Network Based Security (NBS) environment.

AT&T Mobile Security, when deployed in combination with MTIPS:

- Provides a higher level of security, meeting the FISMA High requirements required by many government agencies;
- Delivers MTIPS failover/redundancy capabilities to mobile users and un-tethered endpoints; and

![Figure 2. AT&T Mobile Security Platform. The new AT&T Mobile Security platform and its relationship to the existing foundation of the Network Based Security (NBS) environment.](image-url)
• Enables agencies to stay in compliance with HSPD-12 personnel screening requirements.

AT&T has harnessed the power of our network, our strength in network security, and access to world-class processes, tools and people to develop security services that answer the need for a defense-in-depth architecture. You can count on AT&T as a reliable provider with global reach for a comprehensive range of security services that can provide integrated solutions to help support your complex networking environments.

For more information contact your AT&T Representative or visit us at www.att.com/gov/mobile.

About AT&T Government Solutions
Every day, thousands of experienced AT&T Government Solutions professionals seek to go beyond their customers’ expectations and deploy visionary solutions that serve our citizens, defend our nation and prepare for the future.

We serve as a trusted provider to the federal government, backed by a proven performance record in integrating our network expertise with IT professional services and a managed service portfolio, which includes: traditional and IP-based voice; Wi-Fi; high-speed Internet; data transport; cyber security; cloud-based services; and mobility devices, services and applications. Our broad array of advanced technologies, dynamic service management tools, and experienced staff help us to address core government needs – reduce expenses, modernize operations to increase workforce productivity, and protect information, infrastructure and people. AT&T solutions enable agencies to focus on their mission and performance goals.

Fusing our core capabilities with innovation from AT&T Labs, we are driven to meet today’s demanding agency requirements, while establishing a path to emerging technologies. Underpinning every solution we build and deliver are the global resources and assets of AT&T, one of the world’s largest communications services providers, connecting people, infrastructure and information with speed, security and reliability.

To learn more about our full array of products and services, contact your AT&T Agency representative at: 1.800.862.0926 or www.corp.att.com/gov/rep/mobility.

AT&T Government Solutions
3033 Chain Bridge Road
Oakton, VA 22185-0001
www.att.com/gov