AT&T Managed Security Services

Help detect, deter and mitigate the damage of cyber attacks and business interruptions

Preserving Network Integrity, Availability and Confidentiality

Today's Internet security threats range from curious prowlers to savvy intruders, simple mischief to espionage. Without a plan to help protect your entire network and its connection points, your defense is only as strong as its weakest link. AT&T Managed Security Services adds a powerful protective layer, helping you to maintain the security of your organizations network as you access the Internet. This helps you take full advantage of the Internet as a means of enhancing your existing business relationships with your customers and suppliers.

AT&T offers a wide range of security services, availability and recovery services that provide integrated business continuity and security solutions to support your complex networking environments. We help organizations design, deploy, manage and evolve networks, systems and applications that are reliable and contain security features designed to help protect against cyber attacks and business interruptions.

AT&T security solutions start within the AT&T Global Network, and extend to customers and their applications. Security features are seen as an important component of all the AT&T product portfolios. For example, in the development of services such as AT&T Voice over IP (VoIP), Virtual Private Networks (VPNs) and Remote Access, security features are taken into consideration during the process of designing the service architecture. The AT&T network is a major component in the security model that customers are building for their businesses. Network-based security services are designed to stop security issues before they reach your organization's offices. These measures operate in tandem with the AT&T Threat Management system that scans traffic and helps AT&T security managers to identify emerging problems, see their sources and take preventative action. To help protect customer networks and services, AT&T uses "defense in depth" security architecture, with security features built into every network layer and every supporting process. The theory of "defense in depth" is based on the concept that multiple diverse security measures are intrinsically more effective than a single homogenous defense. So, if the security measures in the first network interface layer are breached, security measures placed inside the network edge at the second and third layers help prevent an attacker from being successful. This makes it more difficult for someone to penetrate a network because there are layers of security built into every system, process and piece of the network architecture. AT&T utilizes this "defense in depth" architecture with proactive management to quickly and easily determine if known threats are being directed at our network or may effect application performance and then mitigate these threats before they can affect the network or the applications running across it. This way we can help reduce the risks to our network and help protect your AT&T network connections and the information crossing it.

Benefits

- Execution
- Potential Financial Effectiveness
- Highly Reliable Wireline and Wireless Networks
- Global Resources

Features

- AT&T DDoS Defense Service provides security alerting and mitigation of DDoS attacks impacting your network
- AT&T Mobile Security extends your security controls beyond the mobile device into the AT&T network
- AT&T Firewall Services provides enforcement of policy in the cloud or at the premises with optional features to perform additional scanning
- AT&T Web Security offers a managed network solution for content filtering and web control
- AT&T Intrusion Detection/ Prevention Service helps detect and respond to malicious activities by sending you alerts specific to your network
- AT&T Security Consulting Solutions utilizes our security expertise to help safeguard your IT infrastructure

With AT&T Managed Security Services, you get the benefit of enterprise-grade security services without the associated expense and technology expertise required to support an in-house staff. We design, build and manage our services to be reliable – providing standardization, scalability and availability while you retain control. This means we provide the operations and day-to-day security infrastructure and support and you provide the policies and overall decision making on how we apply those policies.

AT&T provides both network-based and premises-based security solutions. Our network-based approach enables us to efficiently manage network security issues, redundancy, load balancing and recovery. Our security expertise is based on protecting the AT&T global network infrastructure all day, every day of the year. You benefit from that expertise, and are able to extend our capabilities to your network when you use our security solutions. AT&T also offers premises-based solutions, giving you the flexibility to house security infrastructure within your own premises.

Proactive Network Security

Most security services react to attacks after they have occurred and attempt to minimize and contain damage. AT&T employs a preventative approach to help identify attacks and manage intrusions proactively by:

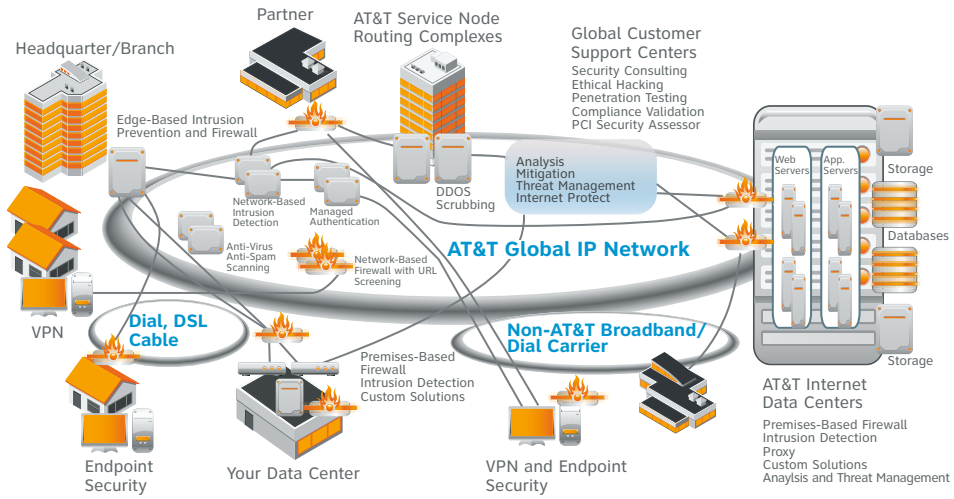
- Assessing vulnerabilities
- Proactively scanning for potential attacks
- Helping to protect against unauthorized access
- Quickly responding to and reporting suspicious activities

Key to this preventative approach is the ability to not only collect data, but also to analyze, interpret and communicate it on a near real-time basis to help respond to the incident. As the scope of cyber attacks becomes more complex and creates more pervasive damage, prevention rather than containment becomes more attractive to the bottom-line.

AT&T Managed Security Services Portfolio

The core focus of AT&T is to keep networks and applications running – and to help assure that viruses, worms and other attacks do not impact the network or affect operations. AT&T has invested in developing and applying tools to achieve world-class reliability, security features and business continuity for businesses. Each security service in the AT&T portfolio provides a different and enhanced layer of protection.

Managed Security Diagram



AT&T Internet Protect®

AT&T Internet Protect is a security alerting and notification service that offers information regarding identified potential attacks, including viruses, worms and denial of service attacks that are in the early formulation stages. This managed service culls information from the extensive AT&T IP backbone which is one of the largest in the world. It performs examination of over 19 petabytes of daily network data to help identify malicious activity from the Internet which you can use to help predict and prevent malicious traffic from infecting your network. Using the Web-based Information Security Portal, pagers and e-mail, AT&T notifies you of identified critical malicious activity and recommends immediate action. AT&T Internet Protect also delivers security information such as top vulnerabilities, recent patch releases and other security "need to-know" facts. In addition to features just mentioned, AT&T customers benefit from an additional service option within AT&T Internet Protect called Private Intranet Protect.

With the Private Intranet Protect option, the traffic on your Virtual Private Network (VPN) is analyzed for known threats that originate both internal and external to your network. These include network misuse, non-conformance to your network security policies, network traffic anomalies that are indicators of possible threats, phishing attacks and other identifiable known threats.

AT&T DDoS Defense Service

AT&T DDoS Defense Service consists of detection and mitigation service components that examine your Netflow data. When the detector identifies a DDoS attack, an alarm is sent to both an AT&T operations center and to you with notification of the detected attack. Concurrently, AT&T will also contact you directly. AT&T systems are designed to reroute traffic directed at the IP Addresses that have been identified as under attack to network scrubbing facilities within the AT&T IP Backbone, where attack traffic is dropped and valid traffic is passed to your access router. Traffic destined to your IP Addresses that are not under attack, continues to flow directly to your network. Organizations who want to better protect their network can obtain AT&T DDoS Defense Service no matter who their service provider or carrier is. You don't need to purchase network connectivity from AT&T to purchase AT&T DDoS Defense Service.

We have conveniently packaged and simplified the purchasing, contracting and billing of AT&T DDoS Defense Service, AT&T Network-Based Firewall Service, AT&T Secure E-mail Gateway Service and AT&T Web Security Service under one contract and one invoice providing an efficient and cost-effective way to meet your business security needs.

AT&T Mobile Security
Mobile security solutions typically scan for security risks at the device level only. However, in order to maximize your wireless security and help defend against unauthorized applications, e-mails, and disruptions in business activities, AT&T Mobile Security service provides the capability to extend your security controls beyond the device and into the AT&T network. Device security includes the use of application controls and anti-virus/anti-malware scans. 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 and is mobile carrier agnostic. It's a security service that lets you extend, help protect, and synchronize your security policies even if you're not using AT&T wireless services.

AT&T Firewall Security
AT&T Firewall services help protect organizations infrastructures with various network security functions. These fully-managed solutions are configured to match your specific requirements with flexibility to select the right level of protection. Network-Based firewall, Premises-Based firewall and Web Application firewall services are available. Day-to-day management and maintenance, expert support and proactive 24x7 security monitoring are provided.

AT&T Network-Based Firewall Service
By placing firewall functionality into the AT&T network infrastructure, AT&T Network-Based Firewall service inspects inbound and outbound traffic and is designed to take action according to your predefined security policies. You can also select your company's required bandwidth allocation for Internet access globally through the firewall. The service is available world-wide with firewall configurations ranging from simple outbound only security policy to extensive bi-directional policy with optional features, such as Web filtering, malware scanning, intrusion detection and prevention, Application Control, Data Loss Prevention as well as support to protect multiple, independent network segments. Reports summarizing events and utilization as well as policy self-management capabilities are available through the AT&T BusinessDirect® portal.

We have conveniently packaged and simplified the purchasing, contracting and billing of AT&T Network-Based Firewall Service, AT&T Secure E-mail Gateway Service, AT&T Web Security Service and AT&T DDoS Defense Service under one contract and one invoice providing an efficient and cost-effective way to meet your business security needs.

AT&T Premises-Based Firewall Service
AT&T Premises-Based Firewall Service utilizes industry-leading firewall platforms from Cisco, Checkpoint, Fortinet, Palo Alto Networks, and Juniper. They protect your network perimeter from the hazards resulting from connecting the Internet with your private network. AT&T Premises-Based solutions scale from small, home office environments to large globally distributed organization networks. The standard powerful firewall capability is complimented with the ability to add optional features including high availability, support for complex security policy, VPN, DMZ/extranet support and the Next Generation capabilities of Intrusion Prevention Service, Anti-Virus filtering, Anti-Spam protection, Zero Day Malware Detection, and URL content filtering.

AT&T Web Application Firewall Service
AT&T Web Application Firewall service is a fully managed security service that combines Web Application Firewall technology with expert management and 24x7 security monitoring to help protect web applications and their underlying systems. Web Application Firewall helps customers meet Payment Card Industry 6.6 regulatory requirements. Web Application Firewalls are deployed in front of the application servers as a transparent Layer 2 bridge at the customer premises or in a Hosted environment. It provides protection without interrupting legitimate traffic to web applications.

AT&T Intrusion Detection/Prevention Services
Using around-the-clock network surveillance, AT&T Intrusion Detection/Prevention Service is designed to monitor unauthorized attempts to access your business networks and provides you with the tools to help you implement your internal network defense. Similar to a security camera on a physical property, this service monitors network traffic by employing intrusion detection sensing components at various points at the perimeter and within your network. The sensing components monitor data packet header and payload information to help detect known malicious activity by comparing the traffic to a continually-updated database of over 1,000 existing attack signatures. When a pattern of misuse is detected, the system is designed to respond quickly and automatically according to your predefined policies. AT&T Intrusion Prevention can help detect, contain and neutralize known threats that can attack any IP enabled endpoint on your network.

Additionally, a Host-Based intrusion detection/prevention option is available within the AT&T Intrusion Detection/Prevention Service. This option consists of security software installed on customer servers or hosts which monitors the networking subsystem or operating systems to determine if new Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) services are started, or if existing services have stopped.

AT&T Web Security Service
AT&T Web Security service helps create a protected and productive Internet environment for your organization. The service is designed to keep malware off your network and allow you to control the use of the Web by employing Web Filtering, Web Malware Scanning and Roaming User Support to protect users who are not on the corporate network.

We have conveniently packaged and simplified the purchasing, contracting and billing of AT&T Network-Based Firewall Service, AT&T Secure E-mail Gateway Service, AT&T Web Security Service and AT&T DDoS Defense Service under one contract and one invoice providing an efficient and cost-effective way to meet your business security needs.

Additionally, AT&T Cloud Web Security Service is designed to provide comprehensive Web security including near real-time protection against viruses and malware, protection against compromised/hacked web sites and granular control of Web applications. In addition to near real-time content security, AT&T Cloud WSS includes Negative Day Defense, which can help secure your organization from attacks that have not yet occurred. Best of all, AT&T Cloud Web Security requires no on-premises equipment which eliminates the

need to install, house and maintain physical hardware. IT staff, who would have been tasked to manage on-premises solutions, can now be better utilized to secure enterprise and employee assets.

AT&T Secure E-Mail Gateway Service
AT&T Secure E-Mail Gateway is a security as a service solution that offers protection against inbound e-mail-borne threats such as malicious web links and attachments, and targeted phishing in addition to blocking traditional spam and viruses. Just as important as preventing inbound attacks, Secure E-mail Gateway also provides the powerful features you need to support your email DLP policies through policy based outbound filtering and encryption. To help meet your e-mail storage management, record retention and legal and regulatory compliance needs the SEG Archiving service supports archiving of unlimited amounts of data with flexible retention periods from 30 days up to 10 years.

We have conveniently packaged and simplified the purchasing, contracting and billing of AT&T Network-Based Firewall Service, AT&T Secure E-mail Gateway Service, AT&T Web Security Service and AT&T DDoS Defense Service under one contract and one invoice providing an efficient and cost-effective way to meet your business security needs.

AT&T Endpoint Security
AT&T Endpoint Security service is a fully managed solution to help protect both end users and company's internal systems from external hazards posed by doing business on the Internet. The service is designed to enforce compliance with customer-defined policies for firewall, anti-virus and software compliance at remote end points. The service also provides centralized management tools for control of remote end points and a path for customer to gain control over the applications operating on these end points.

The service consists of central policy servers and AT&T Global Network software clients. The software clients receive security policy information from the servers located at AT&T Internet Data Center. The software clients interact with the policy server to receive policy updates and to perform policy enforcement. Your security policies will be populated into a central policy server by your administrator, and then distributed to your users from the AT&T managed policy server. The service also includes a number of reports such as user activity, connection history and event logs as well as provides enforcement of anti-virus updates and software patches.

AT&T Encryption Services
AT&T Encryption Services is a service that simplifies e-mail and data encryption by automating the management and use of digital credentials. You can quickly and efficiently digitally sign and encrypt messages or files using existing desktop, mobile and web interfaces. Multiple methods of message delivery and receipt help ensure that encrypted data reaches the intended audience.

Whether it is employees exchanging confidential information with associates or the delivery of confidential statements to customers, AT&T Encryption Services provides a comprehensive suite of encryption solutions to help protect data in motion and at rest.

AT&T Token Authentication Service
Organizations need to know who is gaining access to network applications to help avoid unauthorized access and disclosure of sensitive information. This risk of exposing proprietary and sensitive information is magnified as the number of remote users accessing the network increases. AT&T Token Authentication service is a network access protection method that uses an enhanced security feature, called two-factor authentication, which requires a user to provide two unique factors to gain access to a private network: something they know (a password or PIN) and something they possess (an authenticator). This method makes it more difficult for a hacker to gain access to authentication credentials than a password since the authenticator's token code changes randomly every sixty seconds and must be combined with a secret PIN selected by the user accessing the network.

AT&T Security Analysis and Consulting Solutions

AT&T Security Event and Threat Analysis Service
AT&T Security Event and Threat Analysis service is a virtual Security Operation Center that utilizes expertise AT&T has developed in security analysis and operations to correlate information from multiple devices and device types, on premises and embedded in the AT&T network. Based on information gathered, AT&T provides notification of prioritized events based on their risk to your company and the ability to mitigate them. Critical event notifications person-to-person and less critical event notifications get delivered via e-mail and through a customized security portal.

AT&T Security Device Management
AT&T Security Device Management is an integral part of the AT&T Security Analysis and Consulting Solutions providing monitoring and management of security hardware and software you own located

AT&T Security Services Advantage

Proven Execution
- Deployment of updates based upon security and industry events
- Proof of Service through Service Level Agreements
- Visible performance through reporting
- Supported by the "TRUSTED" AT&T infrastructure Financial Effectiveness
- Minimized capital and asset expenditures
- Operational efficiencies through AT&T skilled professionals
- Innovation from AT&T Labs Highly Reliable Network
- Network availability guarantees of up to 99.999%
- MPLS-based services available to more than 180 countries representing 99 percent of the world's economy.
- 38 State-of-the-art Internet Data Centers
- AT&T Global Network carries 56.2 petabytes of data on the average business day

Global Resources
- Approximately 2000 security experts and support professionals
- 6 Network Operations Centers
- 8 Global Customer Support Centers

on your premises or the implementation of complex and customer security solutions. AT&T Security Device Management service lets you take advantage of the AT&T Security Network Operations Centers (S/NOC) expertise to monitor and manage your security hardware, manage your security infrastructure, or migrate to a custom security architecture designed to meet your specific requirements.

AT&T Security Consulting

AT&T provides a unique and world-class portfolio of compliance and related security services. Our experience, expertise and commitment to open standards have established us as a strategic and trusted advisor. AT&T Security Consulting provides solutions that allow you to operate your security operations more efficiently. We work as a trusted team to provide knowledge based services. Our consultants have industry and security expertise that can be utilized to complete short and long term engagements. Experts are focused in six areas: Security Strategy, PCI Solutions, Governance Risk and Compliance Solutions, Secure Infrastructure Solutions, Threat and Vulnerability Management and Application Security.

AT&T Security Consulting services provide a proactive, comprehensive approach to security and compliance across all your organizations operations. Our security consultants have accreditation in the latest security certifications and expertise across all aspects of security and provide solid methodologies for validating and streamlining regulatory compliance.

AT&T Secure Network Gateway

AT&T Secure Network Gateway provides an integrated, turnkey security solution on a single pricing schedule with multiple service and term discounts on one convenient contract and bill. The services available under AT&T Secure Network Gateway service are AT&T Network-Based Firewall Service, AT&T Secure E-mail Gateway Service, AT&T Web Security Service and AT&T DDoS Defense Service.

AT&T Threat Management and Analysis Service

Cyber threats have become a boardroom agenda with the potential to bring down an organization's network, create compliance issues, damage bottom lines, and impact brand reputation. Additionally, disparate security technologies create 'security silos,' increasing cost and complexity of security management, and making it almost impossible to uniformly monitor security threats across IT environments. AT&T Threat Management and Analysis Service will help address these challenges with a highly secure network infrastructure an optimal blend of security consulting, on-premises and next-generation cloud security capabilities, including AT&T Network-Based Firewall Service, AT&T Intrusion Detection/Prevention Services, AT&T Secure-E-Mail Gateway Service and AT&T Distributed Denial of Service (DDoS) Defense Service protection, and security monitoring, analytics and emergency response services.

Trust Your Security to AT&T

AT&T has a long legacy of developing security services which answer the need to address a defense in depth architecture, from the information level to the network level. You can count on AT&T as being a trusted provider with true global reach that has a comprehensive range of security, availability and recovery services that can provide your business with integrated business continuity solutions and help support your complex networking requirements.

Security by Design

AT&T is committed to enhancing the security services and features by continuing to develop security innovations and management techniques to create additional security services for enterprises. In the following paragraphs, we describe what techniques AT&T has been using to add security features both within its networks and within the services it provides.

Processes

All AT&T Services follow AT&T Service Realization Process that includes a focus on security considerations in every step of service development and network deployment. For each new service or feature that is being developed, the AT&T Security Team works closely with product management, systems architects, engineers, developers and testers to add security features into the service.

Domain Separation

A network that is comprised of one or more systems and one or more networks, all with a common function, constitutes a domain. Each domain must have a set of rules for communication within the domain and another set of rules in order to communicate outside the domain. This separation is achieved by using the principles of domain separation for systems and networks within a company. Domain separation allows communications between two domains to occur in a controlled manner, through only a few communication points and under scrutiny based on type of traffic, source, destination and volume of traffic. These few communication points are usually called security gateways, or choke points and the rules applied at each are called choke filtering. Domain separation helps ensure that communications between domains are allowed only as authorized, going through designated gateways, which are designed to help detect suspicious activity and block it if necessary. If one domain is compromised in a security incident, domain separation helps protect the other domains from compromise and helps contain the incident.

AT&T employs the principle of domain separation within its corporate intranet as well as on its various service networks and between the operational networks and network management infrastructures. Network management domains are separated from the operational networks themselves. The AT&T Points of Presence (Central Offices) are built with multiple security zones. Each zone has different requirements for security needs and is segmented to help prevent the traffic from leaking between zones. Various complementary mechanisms are deployed to maintain segmentation. "Hardening" Infrastructure Elements Network infrastructure security includes both host-based and network-based security elements. The foundation of infrastructure security is a server. "Hardening" of the server means locking down (restricting use of) open server communication ports. All servers are "hardened" based on vendor, industry and internal recommendations and industry best practices. Host-based agents (i.e., software used to monitor activity on a server or PC) monitor the servers looking for unauthorized changes in software and configurations. In addition to hardening the network elements, AT&T deploys a number of measures to help protect against denial of service attacks within the AT&T network, and at the service (application) level. AT&T has deployed state-of-the-art security mechanisms to help protect its Global IP Network and IP Services against Denial of Service (DoS) and other

network-based attacks while monitoring IP traffic for new identified attacks such as new worms and viruses. All of these systems are in place and are monitored 24x7 by experienced security personnel.

Services on the AT&T Global Network

The AT&T Global Network has evolved to a single, global, Multi-Protocol Label Switching (MPLS) enabled backbone over an intelligent optical core network. MPLS, a leading edge technology that is driving convergence in the network, is the key technological component underpinning this network evolution which provides flexibility and quality of service beyond those found on a private network. MPLS adds reliability and performance capabilities, enabling applications to scale as business needs change. AT&T is regarded as one of the MPLS industry leaders based on its early and continuing work with this technology, and continues to pioneer its use by offering a suite of virtual private networks (VPNs) that enable MPLS. AT&T services such as Network-Based Firewall and Network-Based Remote Access are designed to take advantage of the MPLS technology. The combined force of MPLS in conjunction with the AT&T multilayered security approach helps ensure that your organization can utilize a network that is flexible and scalable for future applications.

Separate Services Over IP Infrastructure

Voice over IP (VoIP) poses particular security challenges to carriers due to the protocol design itself. With VoIP both the signaling as well as the actual voice messages are carried in-band across the network, thus making signaling vulnerable to the same security risks as other Internet traffic. Recognizing these challenges, AT&T has designed a separate "Services over IP" architecture to carry application traffic such as VoIP. AT&T Services over IP infrastructure integrates with the AT&T public MPLS IP network and has been designed with multiple layers of defense, consistent with the AT&T "Defense in Depth" principles. The design principle is consistent with the general architecture used in protecting organization assets from the Internet, and includes multiple security domains, each with its own security requirements. To further enhance the security of these communications, AT&T has defined boundaries regarding what device can communicate with what device, thus providing additional control.

An additional challenge with VoIP is that a separate Session Initiation Protocol (SIP) establishes the communication channel while the call data (voice) is initiated. Specifically, SIP servers are responsible for creating, modifying and terminating sessions with one or more participants, however most of them do not include firewall functionality as part of their basic configuration. In order to help security of our services over IP infrastructure, AT&T has designed so called border elements, or intermediary gateways. The border element acts as an intermediary between domains providing an additional layer of security for AT&T SIP based service.

For more information, call 877.542.8666, or visit us at www.att.com/network-security.

04/28/14 AB-1133-09