AT&T Synaptic Hosting℠ Service Security Overview

A Look at AT&T's Protective Measures to Enable Your Business Success

AT&T follows high security standards to help protect customers from the risks and challenges that confront businesses today. On the following pages we describe the depth and breadth of experience and dedication we provide in securing the AT&T Synaptic Hosting℠ service.

It is the policy of AT&T to protect its network, managed systems and applications from unauthorized or improper use, theft, accidental or unauthorized modification, disclosure, transfer or destruction, and to implement protective measures commensurate with their sensitivity, value and criticality. By leveraging superior resources, time-tested methodologies and proven infrastructure and management expertise, AT&T enables the initial and ongoing success of our customers' business initiatives.

AT&T Synaptic Hosting is a utility hosting package that provides a managed local area network (LAN), server and storage on a prebuilt, virtualized infrastructure delivered out of regional data center hubs around the globe. The service is backed by a single, holistic service level agreement (SLA).

Benefits to companies that use the AT&T Synaptic Hosting service include:

- Cost efficiency by right-sizing capacity to match business demands and avoiding a bloated infrastructure that goes underutilized most of the time
- Flexibility to handle traffic spikes at peak periods, such as campaigns and promotions, open enrollment, or the holiday season; to capitalize on immediate market opportunities; and to adapt quickly to acquisitions, divestitures and other business changes
- Improved application functionality and a better end-user experience
- Reduced risk because of lower investment costs, more effective technology and use of best practices for infrastructure and security

AT&T Synaptic Hosting includes the following features:

- Virtualized "pay-for-what-you-use" computing platform that supports capacity on demand. We manage the network, computing capacity, security and storage. Four service classes are designed to meet your specific recovery time objectives
- Designated account support by a Client Executive, Client Technical Lead, and Client Service Lead who proactively manage your infrastructure and application performance
- Application awareness capabilities, an optional service through which we proactively monitor and report on your application, which is available for most software
- Integrated service level agreement that covers availability and response time for the entire service, up to 99.9%
- Monitoring and management of the network, servers, operating system, Web and database layer
- Portal and reporting for access to detailed information on the service, 24x7x365

AT&T Security Methodology

Having one of the largest global IP networks and 38 Internet Data Center (IDC) locations around the world, we apply our own expertise to protect our hosting business. Every day we successfully thwart real-world threats posed to AT&T's own assets. The expertise behind our security services stems from our engineers in AT&T Labs, who have made significant contributions to the security field, as well as our experienced, highly certified security operations teams. Our security consultants continually stay abreast of current issues by participating in news groups and security forums, taking part in continuous education and resolving actual client security issues.

The AT&T Security Policy establishes the security standards for protecting AT&T computing and networking infrastructure, and AT&T Hosting & Application Services (H&AS) has an established methodology to provide end-to-end security services to all AT&T managed devices, including the AT&T Synaptic InfrastructureSM.

AT&T implements a layered security model, which provides for multi-level protection of all information, data and physical assets including data center environments. In this model, security does not depend on a single countermeasure. Rather, layers of security provide a reinforced system of countermeasures so a single point of failure does not compromise the entire system. This layered security approach protects

at&t

AT&T hosted solutions from both physical and logical security threats. It includes:

- Physical Security
- Network Security
- Intrusion Detection
- Firewall Management
- Environment Hardening
- Virtual Guest Security
- Virus and Patch Management
- Access Controls
- Data Security – Encryption of Data

Following is a summary of the key security features of the AT&T Synaptic Hosting.

Physical Security

AT&T data center facilities offer a physically secure environment 24x7 to protect from outside intrusion. Physical security procedures involve controlling, monitoring and recording physical access to facilities where client servers and other equipment reside.

AT&T provides complete physical security for AT&T locations, with a special emphasis on security of the data center and other sensitive areas. Our stringent physical security controls include:

- Access Policies and Procedures
- Multi-layer/Multi-factor Access Control Systems
- Employee Access Procedures
- Visitor Procedures
- Contractor Access Procedures
- Building Security
- Data Center Security
- Global Client Support Center Security
- Background Checks
- Monitoring Systems
- 24x7 Guards

The automated access control system controls and monitors access to AT&T data centers and our Global Client Support Centers through the use of electronic badge readers, biometric scanners and PIN keypads. The system logs access and sends alerts if entrances are left ajar. Security guards patrol the facilities and maintain a 24X7 physical presence at each data center. Access to the building, including lobby entrances, requires an electronic access badge. Access to AT&T data center locations requires an electronic access badge, biometric scans and/or a PIN number. As an additional measure, strategically located video cameras record and monitor activity.

Network Security

We protect our network in depth. Around the clock, highly trained security and network personnel manage packet filters at the network borders of the Synaptic Infrastructure, which stops the majority of unauthorized traffic. Because the packet filters are tightly integrated into the management framework, we can adjust them with the latest security protocols in real-time, closely monitoring and automatically updating the filters to mitigate immediate security threats. The best network security design and implementation must be continuously managed.

Network security is a process, driven by management and supported by expert skills and advanced technology. AT&T provides a world-class security posture through its consistent coverage worldwide, its depth of execution in each region and the guidance and support of the global security team, which administers and coordinates security initiatives.

Intrusion Detection

Our intrusion detection system, deployed at multiple points throughout our network, recognizes suspicious activities and immediately alerts our information assurance team. AT&T has deployed packet-based intrusion detection systems on the network perimeter of each data center and the Synaptic Infrastructure to capture all traffic going in and out of our network and identify Windows network attacks, Web attacks, probing attacks, denial of service attacks, remote procedure attacks, service exploits, FTP exploits and unauthorized network traffic.

The intrusion detection system's sensors relay their observations back to a database that aggregates and correlates the events, so that even distributed attacks are detected. The system also reassembles data streams and makes sense of hacker attack patterns that have been "chopped up" expressly to avoid recognition. The result is a very sensitive, intelligent network alarm system that, when combined with the efforts of our highly trained security engineers, gives us the ability to pinpoint security events and react immediately and purposefully.

Firewall Management

The Synaptic Infrastructure is used by multiple client companies – which may have different security requirements. For this reason, AT&T has segmented and protected each client system with a set of virtual firewalls. The Synaptic Infrastructure leverages virtualized firewalls running in a high-availability configuration.

Each client has a firewall policy rule set specific to their security needs. The firewall's purpose is to deny unauthorized entry into the individual client environment. Having firewall policies that are client-specific makes it simpler to segregate rule sets and coordinate changes;

changing one client's firewall rule will not affect that of another client. The firewall is under the management of AT&T and requires customer documented approval to authorize any changes to the policy.

Only traffic with the proper authorization, entering through the appropriate port, will be allowed past the firewall. Each client can request firewall rules to adhere to their unique specifications. The firewall is configured in a default deny mode, and AT&T opens ports to allow inbound traffic based on client instruction. The traffic may be restricted by protocol or by service port, as well as by source IP

address. The firewall can be configured in groups to allow different groups to have different rules. For example:

- Web Servers: Open port 80 (HTTP) and port 443 (HTTPS)
- Application Servers: Open application specific port. This group would only be accessible to the Web server group
- Database Servers: Only open to application server group

All three groups would permit administrative access, but only from the AT&T management network or via client remote access using VPN with two-factor authentication.

We test the security of every client delivery before go-live to verify that it meets current security requirements. AT&T security experts evaluate the firewall rules to check that they adequately meet the security needs of the client and AT&T. Each time a firewall rule is changed through the change control process, the security team reviews the firewall rule set and the proposed changes before the change is approved and executed.

Rigorous levels of firewall management help each client feel confident that the security of their solution is sufficient to their needs and in line with security best practices throughout the life of the system.

Environment Hardening

AT&T invests heavily in developing the proprietary hardening techniques implemented in the Synaptic Infrastructure. Adherence to best practices, relationships with software vendors and real-world experience are the drivers behind our operating system (OS) hardening philosophies. As each system hosted on the Synaptic Infrastructure is developed, tested and deployed, the AT&T security team is continuously involved to verify that security standards are met.

The hardening process is an ongoing pursuit for all components and systems AT&T manages in the hosting environment. To achieve the highest level of system security possible, AT&T hardens the OS as well as the applications and databases under our management at the client system level. In the unlikely event that a hacker gets through the packet filters, past the intrusion detection system and past the firewall, the hardware and software on the server are set up to detect and deflect unauthorized use.

During project implementation, the OS is set up securely. As changes are made in the environment or the security standards are updated, the system is updated to adhere to the latest, highest standards. The automated processes for virtual server builds are also updated with each applicable new security standard. Information is collected only through specified ports, and all other ports are closed.

Securing the Virtual Server

AT&T security standards dictate that the Synaptic Infrastructure utilizes hardened operating systems. Unnecessary services and features that may expose a future vulnerability are turned off.

AT&T Synaptic Infrastructure leverages the ability to create individualized security systems for each client. VLAN technologies use industry-adapted standards in protecting the virtual server environment.

The AT&T Synaptic Infrastructure is architected so that data contained within a client's virtual server cannot be intercepted/seen/accessed by non-authorized systems or other clients deployed on the Synaptic Infrastructure. Different virtual servers (guests) running on the same physical machine are isolated from each other at the hypervisor.

The hypervisor is software that abstracts resources into multiple virtual machines, forming a robust foundation for the AT&T Synaptic Hosting service and creating a strong security separation between virtual servers. The hypervisor also includes the firewall between the physical server and the virtual server (guest) interface. All packets must pass through this layer, so virtual "neighbors" have no access to each other and are treated as if they are on separate physical hosts.

Each virtual server (guest) is secured while still enabling the flexible configuration that customers demand. AT&T retains full root access to the guest OS. Clients can have administrative control to add resources and manage content and applications. AT&T implements the following measures to secure a client guest:

- Two-factor password-based authentication is required to access the guests
- A privileged escalation mechanism is in place, with logging on a per-user basis
- AT&T Synaptic Hosting customers have no access to raw disk devices, and best practices are used for process management of Synaptic Hosting disk space. Our processes wipe every block of storage used by the customer and ensure that one customer's data is never exposed to another

Regarding packet sniffing by other tenants, the Synaptic Infrastructure is designed to prevent a virtual server from receiving traffic that is intended for a different virtual server on the Synaptic Infrastructure. The hypervisor layer of the Synaptic Infrastructure will not deliver any traffic to a virtual server that is not addressed to it. As a standard practice, we recommend that customers encrypt sensitive traffic. AT&T Synaptic Hosting service offers site-to-site VPN and dedicated private connectivity options to secure data in transit to the Synaptic Infrastructure.

Virus and Patch Management

AT&T constantly monitors virus information centers to track development of security threats. AT&T also aggressively employs a program to proactively discover security problems; monitor credible sources of vulnerability information, including subscription services, CERT® Advisories, vendor security patches, Internet news groups, Internet mailing lists, network security conferences and hacker websites; and assess recommended and specialized corrective actions to achieve security goals.

For many companies, managing vulnerabilities, especially applying patches and fixes, is a major challenge. For AT&T, vulnerability management is a core competency and a key advantage of utilizing the Synaptic Infrastructure for purposes of standardization.

We manage patches and fixes for thousands of production devices, comprising products from more than eight different hardware vendors and twenty software vendors. We have a proven, fast methodology for quickly rolling out critical patches to our clients. We watch the patch lists and filter through them, finding those that are important to implement on each client system. We rigorously test all patches before implementing them to reduce the possibility of adverse effects on the Synaptic Infrastructure, and then we apply them to all affected client servers quickly and efficiently.

Additionally, AT&T employs an ITIL-based process that identifies, evaluates and applies security-related hot fixes and configuration changes. Security-related hot fixes are evaluated for their applicability to our environment and to the unique configurations of our clients. We do not apply patches across the board on all servers unless warranted

by the nature of the vulnerability being patched. The security team meets weekly to review all alerts and threats and to establish corrective action. AT&T classifies threats as follows:

- High Risk (Critical). Any vulnerability that can easily be exploited on an identified system. This would include exploits that are publicly available, systems exposed to the Internet or systems where no special system knowledge is required
- Medium Risk. Any vulnerability that can be exploited on an identified system. This system has internal and external connections, requires some system knowledge and is moderately difficult to exploit
- Low Risk. Any vulnerability that cannot be easily exploited on an identified system. This would include exploits that require local OS level access, extensive knowledge of the system, minimal network access or a high degree of difficulty exploiting the vulnerability

AT&T will provide security patching to the Synaptic Infrastructure, operating systems, database and applications via AT&T's established patch processes. When a member of the security team discovers or is notified of a new vulnerability, the issue is immediately analyzed to determine the risk it poses to the Synaptic Infrastructure. The alert is then distributed to members of the security team to discuss the necessary actions to remediate the problem.

AT&T provides all system administration for virtual servers on the Synaptic Infrastructure. AT&T will manage the application of all upgrades and patches to the operating system. Patches and upgrades to the AT&T Synaptic Infrastructure are applied at AT&T's discretion and are communicated to the client before any implementation. Client-requested upgrades and patches can be addressed on an individual basis.

Access Controls

AT&T provides access controls as part of the standard infrastructure. All customers who require OS-level access into their AT&T Synaptic Infrastructure guest are provided with secure ID tokens for two-factor authentication. Token authentication can provide additional log database information; system logs can be configured to detail client administrator access and activity. SSL certificates can be implemented to secure Web communications.

User authentication enforces responsible use of the network and systems. User name and password logins create a log database that shows who edited data and when. As part of our SAS 70 Type II certification, AT&T has implemented a system our employees use to securely log in each time they access a system on a client's behalf. This system creates log databases that detail exactly which system the employee logged into, what level of access they were granted and the amount of time they were in the system.

AT&T maintains stringent controls to manage access from the AT&T management system to the Synaptic Infrastructure, including:

- Logical access to customer system is proxied through a security layer between the AT&T management network and the Synaptic Infrastructure
- Only authorized administrators can access client guests. Privileged escalation processes are in place
- All sessions are monitored. All keystrokes are gathered, logged and routinely audited
- Stringent employee termination management processes and tools are employed

AT&T also performs internal security assessments and employs external organizations to identify weaknesses in our security architecture by conducting penetration tests, vulnerability analyses and threat analyses. Following system deployment, AT&T security resources routinely monitor client environments via proprietary and secure administrative accounts.

Daily, for every production device, AT&T management systems automatically check the age of passwords for system-level accounts, including administrative accounts for Windows and UNIX. If a password age is beyond 90 days, it is reset to an auto-generated password to ensure the security of the solution.

Data Protection

The AT&T Synaptic Infrastructure uses storage area network (SAN) technology to deliver high availability and integrity to client data. To help identify and address any security exposure, a comprehensive SAN security framework is integrated into our processes and tools. Our approach is to zone servers and logical unit numbers (LUNs) through a fibre channel switch, which allows only certain servers access to certain storage elements. This method also provides port-level masking for all the nodes known to the switch, further helping to ensure that clients are only accessing and aware of their files and not other data residing on the SAN.

AT&T Synaptic Hosting customers have the option of including backup and restore services as part of their solution. When client data is being backed up from the SAN to tape, clients have the option of encrypting their data so it is protected while in transit and in media. During a restore, the encrypted data is read from the tape media and transferred across the network to the SAN before decryption. AT&T will own and maintain the encryption key providing full access and ensuring complete security. Client encryption provides data encryption using either 128-bit or 256-bit OpenSSL ciphers. These levels of encryption meet both U.S. government and corporate standards of encryption quality. For organizations with legacy encryption options, AT&T also supports 40-bit and 56-bit encryption methods.

Certifications, Accreditations and Standards

AT&T has for many years applied technical expertise and management resources to support the public, voluntary standards process around the globe. Standards directly affect market success, and customers require standards compliance for the communications products and services they purchase.

AT&T has an entire division that directly participates in technical standards development groups and in industry bodies concerned with administering the voluntary process itself. In addition to the work related to the obvious areas of telecommunications and information technology, this participation spans a wide range of subjects including quality, environmental management and safety. AT&T's participation involves international, regional and national groups around the globe.

Certification Activities

AT&T has demonstrated continuous efforts to obtain and maintain the strictest of industry certifications. This effort demonstrates our commitment to providing a secure environment for our customers' mission-critical business applications.

AT&T's Hosting & Application Services unit has a robust Audits and Compliance team whose focus is to assist customers who are required to comply with complex industry security standards like the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) data security standards and others. When customer auditors need to evaluate our facilities, our team can provide additional support services (subject to security and other limitations), as well.

AT&T holds multiple certifications that assess the effectiveness of our security processes and controls. Our security processes are certified against written security and privacy certification criteria for Microsoft Gold and HP (Compaq) SP Signature certification programs. Each year, a third party assesses our internal systems and controls to ensure we meet the requirements of the American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards #70 (SAS 70 Type II) and SysTrust criteria, demonstrating that we deliver our clients the highest level of data security and privacy possible.

PCI Compliance

AT&T hosting and application services comply with PCI standards, as verified by two separate audits:

1. AT&T Hosting environment and services

2. AT&T Application Management environment and services

AT&T's compliance covers our standard security controls and procedures and applies to all layers of the environment, including the operating system. It does not apply to the application layer, because each customer's application environment is customized.

AT&T achieved PCI compliance to provide customers with verifications that may help in their own PCI audit processes. AT&T audits were conducted by a certified Qualified Security Assessor (QSA).

Any business that accepts, processes or transmits credit card transactions has a responsibility to ensure compliance with PCI standards. AT&T's PCI certifications are not a substitute for each company's own efforts, but they may help meet some of the PCI standards.

AT&T Commitment to Security

AT&T has made an unparalleled commitment to and carried out extensive work in the area of security. Some of our unique qualifications include:

- AT&T maintains a dedicated organization of specialized security professionals. This group supports and secures the largest network in the world and is committed to the impartial development of security recommendations regardless of the service provider, thus ensuring best-of-class design
- Through the forward-looking work being performed at AT&T Labs, we lend our experience to global standards organizations while developing security postures that afford the best protection possible for our customers' and our own critical assets
- AT&T has decades of experience working with government agencies and commercial enterprises on their information security planning, implementation and management. AT&T provides a wide range of security engineering and professional services to civilian and defense agencies on the federal and state level. AT&T's architects and engineers provide security solutions that meet stringent government requirements, anticipated needs in the security arena and our own exacting standards

Conclusion

AT&T is among the pioneers in defining and developing mechanisms to support security and privacy on the Internet. We have applied this security expertise in developing the AT&T Synaptic Hosting service so it can meet the stringent demands of today's mission-critical applications. Customers who chose Synaptic Hosting can feel confident that they are tapping the industry's best practices for protecting their data.

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

02/10/11 AB-1601-01