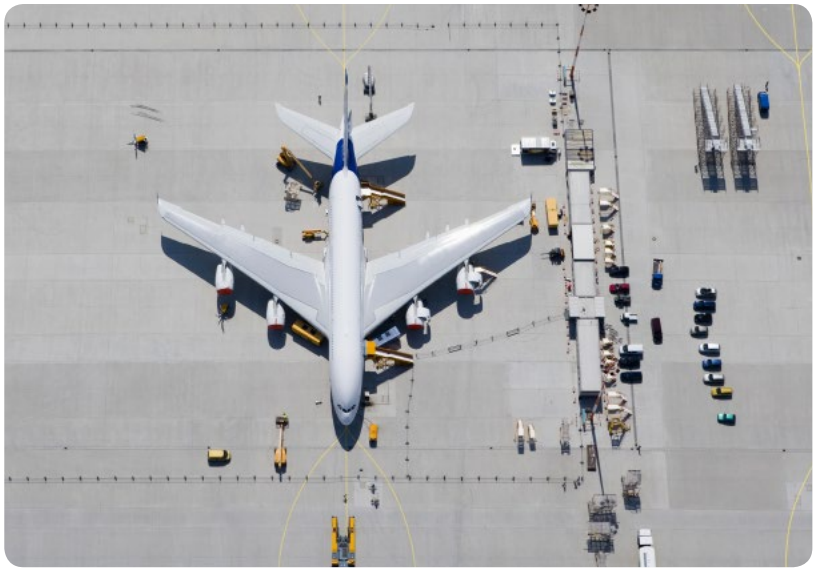
Highly secure connections to your cloud-based applications

Cloud networking with AT&T NetBond®



Enterprise customers are migrating their workloads and applications from their privately owned data centers to third party clouds. The rise of the "mobile" worker (enabled by smart phones and tablets), coupled with the growth of the Internet of Things (IoT) is accelerating the adoption of cloud services. However, security continues to be a critical concern for customers.

Key trends
A **10% increase** in advanced persistent threats and DDoS attacks over the last two years[1]
By 2017, more than 50% of employees will be using their own, rather than organization-supplied, devices[2]
40% of business and technology decision makers report that they have adopted or plan to adopt more than one type of cloud platform[3]
By 2020, there will be **50 billion connected machines** to the Internet[1]

Accessing multiple clouds

AT&T commissioned Clarion Market Research to conduct a blind qualitative survey with some of our key customers. The results showed that one of the top priorities for Security and IT executives was enabling mobile access to applications running in clouds[4].

Today, customers are connecting to multiple clouds to access basic applications such as email, calendars, select customer relationship management platforms as well as travel or expense tools. However, if they believe that robust security is present, customers are willing to access more advanced applications such as human resources, training, content management, collaboration tools and transaction services.

Security is table-stakes

Whether it's a remote employee on a work laptop, an airline tracking their cargo equipment, a sales representative conducting business in a connected car, or a branch office employee - today's businesses are becoming more mobile and require access to cloud services anywhere, anytime, on any device.

Our study found that the security mindset for most respondents could be described as "restrained confidence." Although they were confident they were doing everything they could to protect their businesses from breaches and threats, they also recognized that security needs are constantly changing[4].

Protecting the full path from device to cloud.

Customers view mobile access to cloud based applications as an end-to-end experience that calls for high levels of security for the full path from devices to their applications in the cloud. However, in practice, most customers employed a siloed approach, separately securing individual components, whether it be on the devices, network, or within a cloud environment.

To enable and accelerate cloud adoption, companies must provide a protected pathway from device to cloud as part of a more holistic approach to security. The problem is, the public Internet that often serves as the primary connection between devices and clouds—exposes the enterprise to threats that are growing in both number and severity.

Lack of visibility and control over data.

While data encryption provided by SSL tunneling over the Internet was seen as an option in securing data in transit, the most common security concern is around safeguarding data at rest, whether stored on a connected device or in the cloud[1].

Smart phones and tablets can be easily lost or stolen, compromising sensitive or confidential. The risks increase as the population of IoT devices (connected car, cargo, fleet, watches, etc) grows. Customers are concerned over how to protect cloud-based applications from unauthorized access and with losing visibility into and control over data stored in the cloud[4].

Sensitivity of the data drives the security approach.

The rise of mobile and remote employees, with the migration of mission critical workloads to the cloud has placed demands on access to sensitive data and mission-critical applications. Employees want to conduct financial transactions, access HR and payroll data, use content management tools and collaborate freely beyond corporate walls to include an extended ecosystem of suppliers, partners and customers.

In response to this groundswell of demands, migration from data centers to cloud deployment decisions are being driven by the sensitivity or importance of the data involved. The more sensitive the data is on the device or in the cloud, the more secure the path should be to protect it[4].

Enjoying the benefits of a secure connection

AT&T NetBond® is a cloud networking solution that delivers highly-secure connectivity to your cloud based applications. AT&T NetBond connects your AT&T Virtual Private Network to a growing list of leading cloud service providers (CSPs) via our API's and SDN approach.

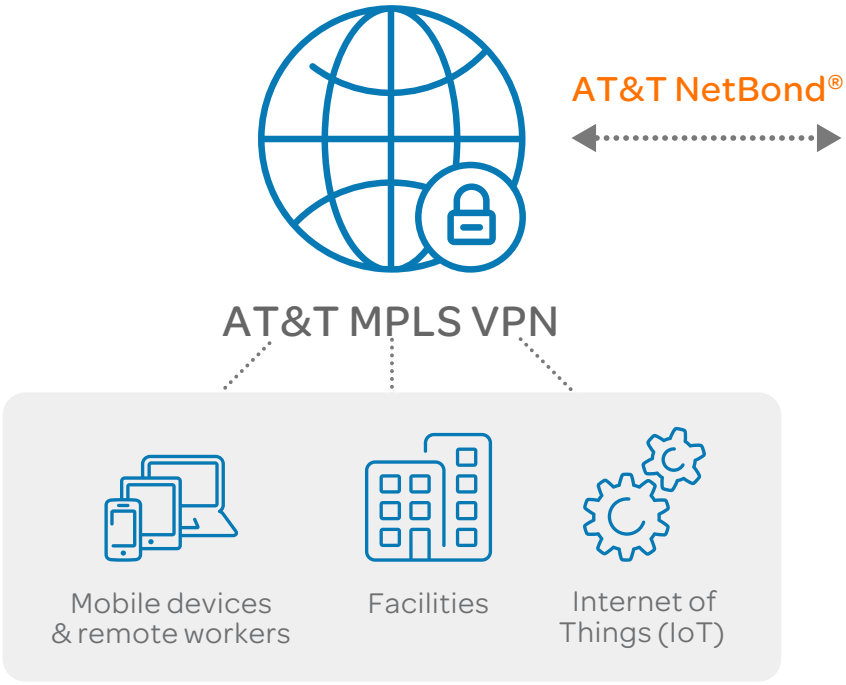
We help protect your business from online threats like DDoS (Distributed Denial of Service) attacks by:

- Allowing you to avoid routing your traffic on the public Internet
- Creating a highly secure connection between your VPN and the cloud
- Isolating your cloud's traffic from that of other customers via proprietary technology

In addition, AT&T NetBond is built on a robust and scalable technology platform to provide the availability and performance enterprise applications and transactional workloads demand. Compared to cloud connectivity over a traditional Internet connection, AT&T NetBond can deliver as much as 50 percent lower latency as compared to alternate cloud connectivity models. Unlike other cloud solutions that require manual intervention, cloud and network resources scale automatically and dynamically in tandem, you can easily meet changing performance needs.

With this solution, the cloud service and network are pre-integrated to get you up and running quickly. No additional infrastructure expenses such as equipment or access lines are needed. Also, our self-service portal gives you visibility and control in that you can provision a cloud service and bandwidth level in minutes!

We are working with leading cloud service providers who have joined our NetBond ecosystem program to deliver an integrated network and cloud solution to our customers:



Service availability for some of these providers is currently being enabled and will be available in the future

Use case: highly-secure connectivity for IoT devices

By 2020 there could be as many as 50 billion connected machines (IoT devices)[1]. However, many of the IoT devices connecting to the Internet or to the cloud today lack the security protocols required by IT departments.

The use case highlights the following AT&T solutions:

- AT&T Commercial Connectivity Service (CCS)
- AT&T VPN
- AT&T NetBond®

Customer Need	A consumer packaged goods company wants to ensure the security of the data (residing in the cloud) which it collects from its network of 5,000 vending machines.
Solution	A direct, highly-secure connection between vending machines and the cloud using AT&T NetBond and other solutions, which provides robust protection for traffic on their network to help prevent exposure to malware or viruses.
Outcome	Highly-secure, reliable transmission of sensitive customer and financial data to protect strategic company data.

Sources:

[1] AT&T, 2015.
[2] Gartner, Mobile Device Proliferation Is Forcing Network Leaders to Redesign Enterprise Wireless LANs, 19 May 2014, Gartner Foundational, 12 June 2015
[3] Forrester, 2014 Forrester Research Business Technographics Infrastructure Survey
[4] Clarion Market Research for AT&T, Secure Mobile Cloud, March 5, 2015.

Share this with your peers

To learn more about NetBond from AT&T, visit www.att.com/netbond or have us contact you.

Scan this code to learn more.