Improve security threat protection against ransomware, malware, and phishing.

AT&T CDN Enterprise Traffic Protector (ETP)

What is ETP?

AT&T Content Delivery Network Enterprise Traffic Protector (ETP) is a cloud-based security service that uses the Domain Name System (DNS) to provide a proactive layer of defense. ETP inspects outgoing internet traffic to help prevent access to sites and apps that host malicious content as well as to those that violate Acceptable Use Policies (AUPs).

DNS is the foundation for all internet services, yet many malicious domains—including those hosting malware and ransomware and the associated command and control (CnC) servers—use recursive DNS for attacks. ETP checks requested domains against our real-time global threat intelligence platform and blocks connections before your users are exposed to threats or content that violates your policies.

ETP easily integrates with other security and reporting tools—including next-generation firewalls, security information and event management (SIEM) systems, and external threat intelligence feeds. As a result, you can add DNS security capabilities to your current systems while continuing to take advantage of past investments.

Security	Simplicity
	
Protects vital sensitive data.	**Simplifying the process.**
Help protect sensitive data vital to the organization. You need to protect your valuable data, systems, and brand from the latest sophisticated threats.	Simplify the process of managing your system. You need a security solution that doesn't burden your IT staff with complex hardware and software management requirements.

Enterprise Traffic Protector (ETP) service options include:

1. **ETP**

   Protects internet circuits from malware and ransomware attacks

2. **ETP Roaming**

   Extends protection to remote users using an ETP client

3. **ETP Advanced**

   Adds more comprehensive traffic inspection capabilities for outbound traffic to provide a full Secure Web Gateway (SWG) implementation:

   •Inbound traffic analysis and sandboxing (HTTP/ HTTPS traffic inspection)
   - Payload inspection
   - Antivirus capabilities
   - Data loss prevention

AT&T Cybersecurity

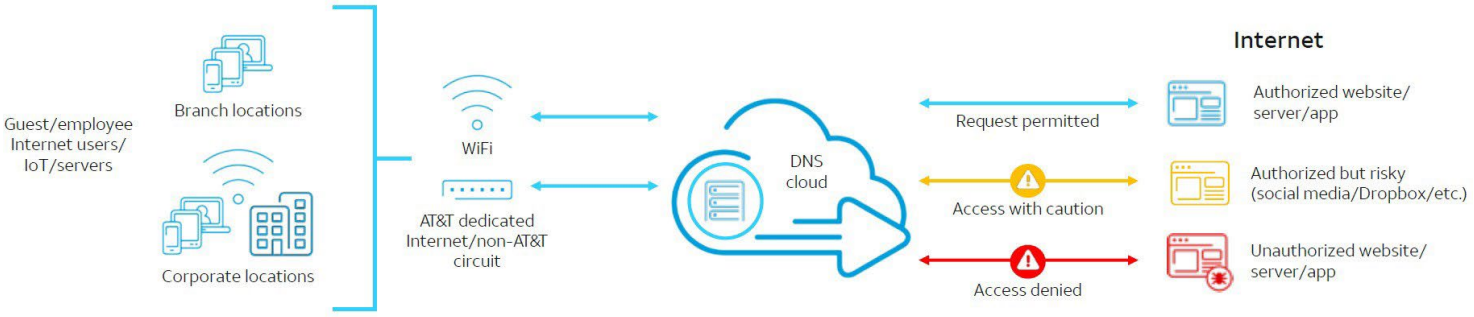
How to use ETP

Using ETP is easy.

Simply, direct your external recursive DNS traffic to our ETP DNS servers to check requested domains against AT&T Content Delivery Network threat intelligence for real-time domain risk scoring.

This verification allows you to proactively block users from accessing malicious domains and services. As this validation happens before an IP connection is made, ETP is designed to stop threats earlier in the security kill chain, farther away from your network perimeter.

In addition, ETP is effective across all ports and protocols, thus protecting against malware that doesn't use standard web ports and protocols. It can also check domains to determine the type of content a user is attempting to access and block the request if the content breaches your Acceptable Use Policy (AUP).



AT&T Content Delivery Network Enterprise Traffic Protector (ETP) gives you these features:

Comprehensive Threat Detection

Protects against phishing, spear phishing, ransomware, malware, Trojans, DNS data exfiltration, pharming, DNSpionage, lexical attacks, and command and control requests. You can even protect off-network employees when they download a lightweight ETP client. As a result, you get a safe on-ramp to connect more securely to the internet, reducing risks to your operations and reputation.

Threat Intelligence

Updates ETP via daily external threat feeds from a global cloud security intelligence platform, which manages up to 30% of the world's web traffic and delivers up to 2.2 trillion DNS queries daily. The platform quickly identifies emerging threats and immediately adds them to your ETP service. So, you get near real-time protection against the latest threats. In addition, the frequent rule updates minimize the incidence of annoying false positives.

Customizable Acceptable Use Policies (AUPs)

Allows you to control the content that your employees can access. You can even set up user-based policies that vary according to employee profiles and job duties. As a result, you can help improve employee productivity and discourage inappropriate or risky activities.

Control Center Portal

Let's you easily configure your service, manage policies, review reports, and issue alerts. The online portal includes a near real-time dashboard to view DNS traffic, threat events, and AUP activities. You can review detailed information to analyze security events, and you get up to 90 days of log retention. Portal access is conveniently available via a web browser as well as APIs, so you can export DNS data logs to your security information and event management (SIEM) system to integrate ETP with other security solutions and reporting tools.

Cloud-Based Service

Requires no hardware and is easy to configure. It only takes minutes to initiate service, add users, and administer policies. You avoid complexity and burdening your IT staff with this easy to manage solution. And you get reliable service with a 100% availability Service Level Agreement (SLA) and low impact on internet access performance and latency because ETP only proxies' risky traffic.

Security Bundles

Let's you combine ETP with AT&T Dedicated Internet or Software-Defined Wide Area Network (SD-WAN) as soft-bundled offerings. Benefits of these options include integrated provisioning and customer care, faster implementation, and pricing discounts.