Supporting schools & students with safety protocols for mobile connectivity.

Enterprise Traffic Protector (ETP), from AT&T Content Delivery Network Service, serves as the safe on-ramp for K-12 and higher education users and devices to connect more securely to the Internet.

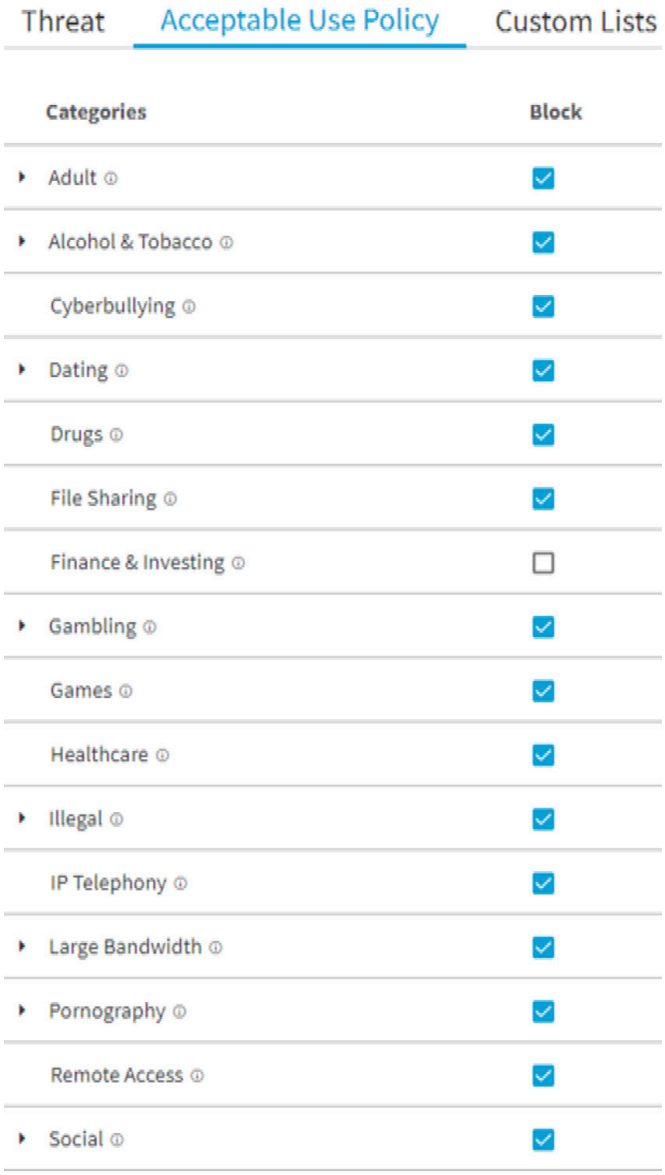
Assist schools in their efforts to meet CIPA compliance by enforcing acceptable use policies (AUPs) to block access to inappropriate websites/applications. Enterprise Traffic Protector (ETP), built on a global platform and carrier-grade Domain Name System (DNS), utilizes global security monitors to mitigate targeted threats. ETP is an easy-to-deploy cloud solution requiring no new hardware or software to maintain. All outgoing traffic is protected by a cloud security platform that provides enhanced protection.

Benefits

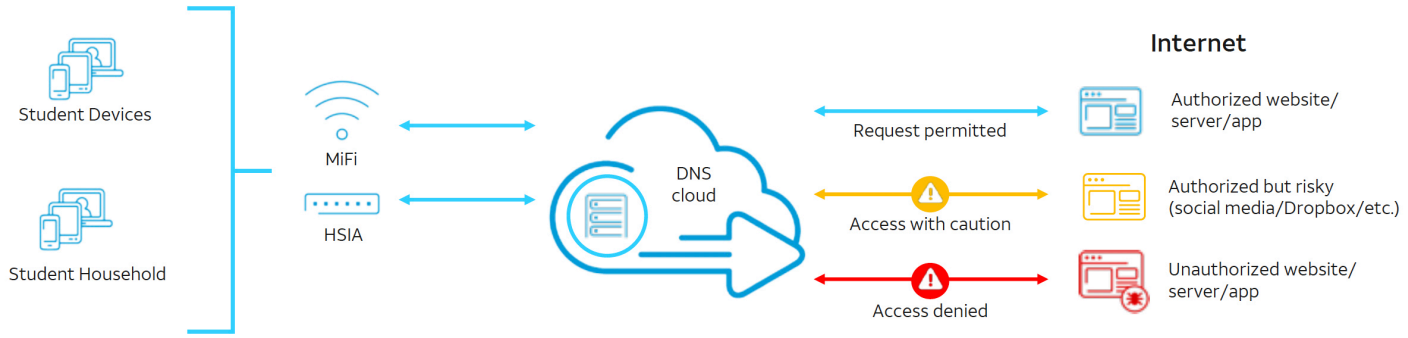
- Uniformly enforce compliance and use policies for students – block access to inappropriate domains and content.
- Provide effective threat protection against phishing and malware attacks.
- Provides protection over wireless and wireline services. Can protect students at home and in the classroom.
- Protect with a cloud solution – no complexity or hardware.
- Easy to configure – takes minutes to deploy, provision, and scale.
- Minimize content filtering management time and complexity – updates can be administered in seconds.
- Increase DNS resiliency and reliability.
- 24 x 7 customer support.
- Monthly Service Charge – $1.00 per end user device

Capabilities

- Customizable AUPs that limit content that can and cannot be accessed by students.
- Device agnostic on AT&T Mobile devices (MiFi, phones, WiFi) and can provide protection on internet circuits within the school.
- External threat feeds and cloud security intelligence are analyzed to identify new risks and are immediately added to the ETP service, to improve near real-time protection against threats for school districts and their students.
- 100% availability service level agreement.



ETP architecture – all outgoing traffic protected against attacks



How it works

- ETP serves as your Internet on-ramp with multiple layers of protection – DNS and URL to deliver optimal security with no performance impacts.
- External recursive DNS traffic is directed to ETP.
  - Requested domains are checked to proactively block content outside the scope of a schools AUP and prevent access to malicious domains.
- Validation occurs before the IP connection is made.
  - Threats stopped earlier in the kill chain, away from the student.
  - Ease of implementation – no requirement to set up IPSec tunnels which drives superior reliability with favorable cost.

Cloud-based Luna portal – easy management and up-to-date reporting (customer access to Luna portal only supported with a Private APN)

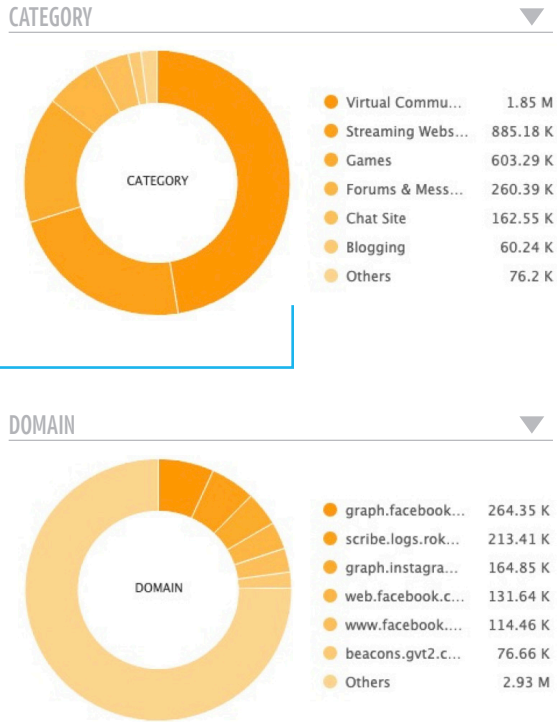
Manage ETP from virtually any location at any time.

- Configure, manage content filtering, and implement changes via the web in minutes to validate that devices are updated with the latest threat protection.
- Use the near-real-time dashboard to view DNS traffic, AUP activities and threat events – drill down on detailed information for security event analysis.
- Access the portal via APIs and export DNS data logs to a SIEM to easily and effectively integrate ETP with other security solutions and reporting tools.

ETP could have prevented:

Multiple AUP violations

- streaming sites
- games
- chat
- blogging
- social media



Important Information: Enterprise Traffic Protector (ETP) is available only to customers with a qualifying business agreement. Additional requirements apply that limit the availability to qualified institutions. May not be available for purchase in all areas. ETP is provided subject to the business agreement between AT&T and customer, the AT&T Content Delivery Network Service Guide, located at http://serviceguidenew.att.com/sg_flashPlayerPage/CDN, including applicable General Provisions. Additional Service and Equipment Related terms are found at http://att.com/abs-addtl-terms. ETP filtering applies to outbound Internet traffic directed to the Access Point Name (APN) provided by AT&T. Customer may select either a shared APN (pre-set, noncustomizable content filter) or private APN (customizable content filter). Additional provisioning interval may apply for private APN. Enterprise Traffic Protector can be used as part of a customer program to implement the Children's Internet Protection Act (CIPA) by identifying the content category of a requested Internet domain (example.com) to enable blocking under an acceptable use policy. Customer is responsible for determining whether use of Enterprise Traffic Protector (using either the shared or private APN option) satisfies customer CIPA requirements. Availability, security, speed, accuracy and reliability ETP is not warranted or guaranteed. ETP is subject to change and/or discontinuation without notice.