AT&T Content Delivery Network
Enterprise Traffic Protector

AT&T Business

Security threat protection against ransomware, malware, and phishing

Enterprise Traffic Protector (ETP), from AT&T Content Delivery Network Service, serves as the safe on-ramp for enterprise users and devices to connect more securely to the Internet wherever they happen to be.

Threats such as malware, ransomware, and data exfiltration increase as hackers become better at circumventing security measures. Enterprise Traffic Protector (ETP), built on a global platform and carrier-grade Domain Name System (DNS), utilizes global security monitors to proactively arm security teams with the ability to mitigate targeted threats as well as create, deploy, and enforce unified security and acceptable use policies (AUPs) in minutes. ETP is an easy-to-deploy cloud solution requiring no new hardware or software to maintain. ETP helps to proactively identify and block ransomware, malware, DNS data exfiltration, and phishing. All outgoing traffic is protected against attacks by a cloud security platform that provides enhanced protection with low false-positives.

Benefits:

- Improve security defenses and reduce attacks with effective protection and low false-positives due to frequent rule updates
- Block malicious payloads in real time
- Security for off-network devices as well as guest devices and traffic
- Increase DNS resiliency and reliability
- Enhance direct Internet access performance and reduce latency by only proxying risky traffic
- Protect with a cloud solution – no complexity or hardware
- Easy to configure – takes minutes to deploy, provision, and scale
- Minimize security management time and complexity – administer policies and updates in seconds
- Uniformly enforce compliance and use policies – block access to inappropriate domains and content

AT&T Content Delivery Network
Enterprise Traffic Protector

AT&T Business

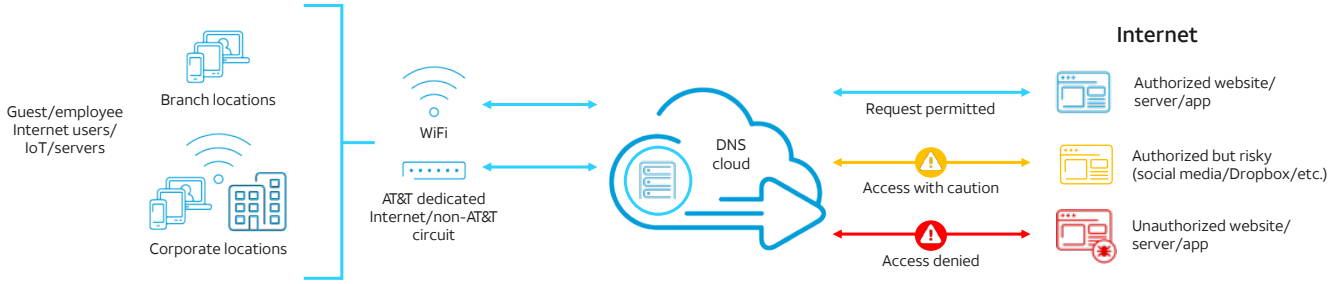
Capabilities

- Up-to-the-minute threat categorization. ETP is built on daily external threat feeds and data from our global cloud security intelligence platform, which manages up to 30% of global web traffic and delivers up to 2.2 trillion DNS queries daily.
- External threat feeds and cloud security intelligence are analyzed to identify new risks and immediately added to the ETP service, to improve near real-time protection against threats for organizations and their employees.
- Integrate customer categorized threat feeds with existing security intelligence capabilities to maximize investment across all security stack layers.
- Customizable Acceptable-Use Policies (AUPs) that limit content that can and cannot be accessed by employees.
- User-Based Policies established by employee profiles and restrictions centered on staff job duties.
- Enforce security for off-net employees and devices as well as protect guests with no need to download a client.
- Reporting and near real-time analysis of all outbound web traffic, threats, and AUP events.
- Additional real-time payload analysis, sandboxing, antivirus protection, and HTTPS inspection.
- 100% availability service level agreement and 30-to-90-day log retention.

ETP protects against:

- Phishing
- Ransomware
- Malware
- Spear phishing
- Trojans
- DNS data exfiltration
- Pharming
- DNSpionage
- Portal access
- Custom policies
- Blacklist
- Whitelist

Enterprise Traffic Protector architecture – all outgoing traffic protected against attacks



How it works

- ETP serves as your Internet on-ramp with multiple layers of protection – DNS, URL, and in-line payload analysis to deliver optimal security with no performance impacts.
  - Good domains – resolved as normal
  - Bad domains – blocked prior to any IP connection being made
  - Risky domains – sent to ETP proxy for URL inspection and payload analysis (HTTP & HTTPS)
- External recursive DNS traffic is directed to ETP.
  - Requested domains are checked against global real-time risk scoring intelligence to proactively block access to malicious domains and content outside the scope of AUP.
- Validation occurs before the IP connection is made.
  - Threats stopped earlier in the kill chain, away from the enterprise perimeter
- Effective across all ports and protocols
  - Protects against malware that does not use standard web ports and protocols.
- Compatible with other security and reporting tools
  - Network-based firewalls, DDOS, SIEMs, most premise-based and network-based applications, and external threat intelligence feeds
  - Ease of implementation – no requirement to set up IPSec tunnels which drives superior reliability with favorable cost

AT&T Content Delivery Network
Enterprise Traffic Protector

AT&T Business

Available service offerings

ETP	ETP roaming	ETP advanced
• Protect Internet circuits from malware and ransomware attacks	• Extend protection to remote users and devices using ETP client	• Add more comprehensive traffic inspection capabilities for outbound traffic • Inbound traffic analysis and sandboxing (HTTP/HTTPS traffic inspection) • Antivirus capabilities

Available security bundles

ETP is compatible with AT&T Dedicated Internet (ADI), Software Defined WAN (SD-WAN), and Network-Based Firewall (NBFW) as packaged offerings. Benefits of these options include: integrated provisioning and customer care; faster implementation; and more favorable pricing.

Cloud-based Luna portal – easy management and up-to-date reporting

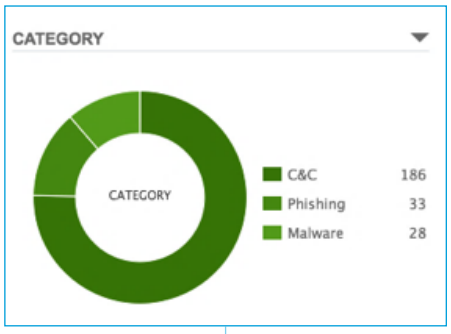
Manage ETP from virtually any location at any time

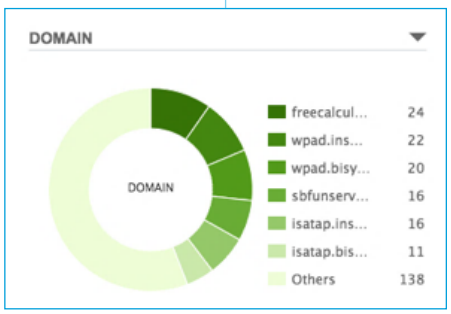
- Configure, manage policies, and implement changes via the web in minutes to validate that locations and devices are updated with the latest threat protection.
- Issue email alerts to security teams on critical policy events to immediately identify, resolve, and remediate potential threats.
- Use the near-real-time dashboard to view DNS traffic, threat events, and AUP activities – 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.

Enterprise Traffic Protector could have saved your organization from:

253 threats

- 17 phishing requests
- 170 malware download requests
- 66 command and control requests





To learn more about AT&T Content Delivery Network enterprise traffic protector, contact your account team or visit att.com/cdn and have us contact you with more information.