Security threat protection against ransomware, malware, and phishing

Benefits:

- Improve security defenses and reduce attacks with effective protection and low false-positives due to frequent rule updates
- Uniformly enforce compliance and use policies – block access to inappropriate domains and content
- Minimize security management time and complexity – administer policies and updates in seconds
- Protects circuits and devices (including the Internet of Things – IoT)
- Security for off-network devices
- Block malicious payloads in real time
- Reduce latency by only proxying risky traffic
- Protect with a cloud solution – No hardware needed
- Easy to configure – takes minutes to deploy, provision, and scale
- Prevent breaches/exfiltration of sensitive data and encrypted files being uploaded to the web (Data Loss Prevention)
- Increase Domain Name System (DNS) resiliency and reliability

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.

Hackers are getting better at bypassing security measures and using malware, ransomware, and data exfiltration more often. Enterprise Traffic Protector helps to keep these tactics and phishing in check by using global security monitors to keep security teams proactively informed. This solution, built on a global platform and carrier-grade domain name system (DNS), helps them to create, deploy, and enforce unified security and acceptable use policies (AUPs) in minutes. ETP is easy to deploy and requires no new hardware or software to maintain. All outgoing internet traffic is protected by this cloud security platform that provides enhanced protection and confidence due to its low false-positives.
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 45% of global web traffic and delivers up to 2.7 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.
- More effective in stopping attacks early in the kill chain (at the DNS level) to improve overall security posture.
- 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.
- Reporting and near-real-time analysis of all outbound web traffic, threats, and AUP events.
- Additional near-real-time payload analysis, sandboxing, antivirus protection, and HTTPS inspection.
- 100% availability service level agreement and 30-to-90-day log retention.
- Full support of DNS over TLS (DoT) and DNS over HTTPS (DoH)

ETP protects against:

- Malicious software
  - Worm
  - Trojan
  - Ransomware
  - Fileless
  - Cryptojacking
  - Adware
  - Spyware
  - Virus
- Phishing
  - Spear phishing
  - Whaling
- Command and Control
- DGA - domain generation algorithm
- Lexical attacks

*TLS – Transport Layer security; HTTPS – Hypertext Transfer Protocol Secure
Enterprise Traffic Protector architecture – all outgoing internet traffic protected against attacks

- 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 and 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 Acceptable Use Policy.
- 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, distributed denial of service (DDOS), security information and event management (SIEM), 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.

Available service offerings

<table>
<thead>
<tr>
<th>ETP</th>
<th>ETP mobile</th>
<th>ETP advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Protect Internet circuits from phishing, malware and ransomware attacks</td>
<td>• Extend protection to users in remote locations using Windows, Mac, iOS and Android devices</td>
<td>• Add more comprehensive traffic inspection capabilities for outbound traffic</td>
</tr>
<tr>
<td>• Support acceptable use policies (AUPs)</td>
<td>• Provides protection when accessing the internet over wireline, wireless, or WiFi</td>
<td>• Inbound traffic analysis (payload inspection) and sandboxing (HTTP/HTTPS traffic inspection)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Antivirus capabilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data loss prevention (DLP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Application visibility and control</td>
</tr>
</tbody>
</table>
Available security bundles

Enterprise Traffic Protector is compatible with AT&T Dedicated Internet (ADI), software defined wide area network (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 portal – easy management and up-to-date reporting for greater visibility on resource usage, location statistics, policies, lists and more.

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 …

93K domain threats

- deaths... 64K
- auong... 10K
- ogefsr... 10K
- hhtuep... 5.5K
- Others 3.5K

93K DNS events

- Phishing 53K
- C&C 27K
- Other 12K
- Malware 1K

To learn more about Enterprise Traffic Protector (ETP), from AT&T Content Delivery Network Service, contact your account team or visit att.com/cdn and have us contact you with more information.

© 2021 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property. All other marks are the property of their respective owners. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change. | 385602-102821