AT&T Cybersecurity

AT&T Business

Enterprise Traffic Protector from AT&T Cybersecurity defends your network against phishing, malware, and ransomware

Named a worldwide **"leader"** in the IDC MarketScape[1]

Your safe internet on-ramp for users and devices. Connect more securely to the internet—wherever you happen to be.

Hackers are getting better at bypassing security measures and using phishing, malware, ransomware, and data exfiltration more often. These attacks shut down online operations, disrupt IT systems, and steal business data.

Enterprise Traffic Protector (ETP) from AT&T Cybersecurity helps keep hackers in check. It uses using global security monitors to keep security teams proactively informed.

Built on a global platform and carrier-grade domain name system (DNS), this solution helps security teams 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 our cloud security platform. This platform enhances protection and gives you greater confidence due to its low false positives. You can even add protection for your mobile devices connected to the internet though any mobile network.

[1] AT&T named a worldwide "leader" in the IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment

Benefits

- Blocks malicious internet requests before outbound internet connections are made
- Improves security defenses and reduce attacks due to frequent threat rule updates
- Enforces compliance and use policies to block inappropriate domains and content
- Protects circuits and devices including Internet of Things (IoT)
- Adds protection for mobile devices connected to the internet through all mobile networks
- Administers policies and updates in seconds; minutes to deploy, provision, and scale
- Prevents breaches/exfiltration of sensitive data being uploaded to the web

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. This improves real-time protection against threats for organizations and their employees.
- Stops attacks early in the kill chain (at the DNS level) to improve overall security posture.
- Integrates 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.
- Enforces security for, and protects off-net employees.
- Reporting and 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-day log retention with archive capabilities.
- Full support of DNS over TLS (DoT) and DNS over HTTPS* (DoH)
- Available for all AT&T internet connections, including mobile devices connected over all mobile networks.
- Seamless protection for users in and out of the office; same policies and tools for mobile protection as used for internet circuit.
- Extend protection to users in remote locations using Windows, Mac, iOS and, Android devices

ETP Protects Against

Malicious software

- Worm
- Trojan
- Ransomware
- Fileless
- Cryptojacking
- Adware
- Spyware
- Virus

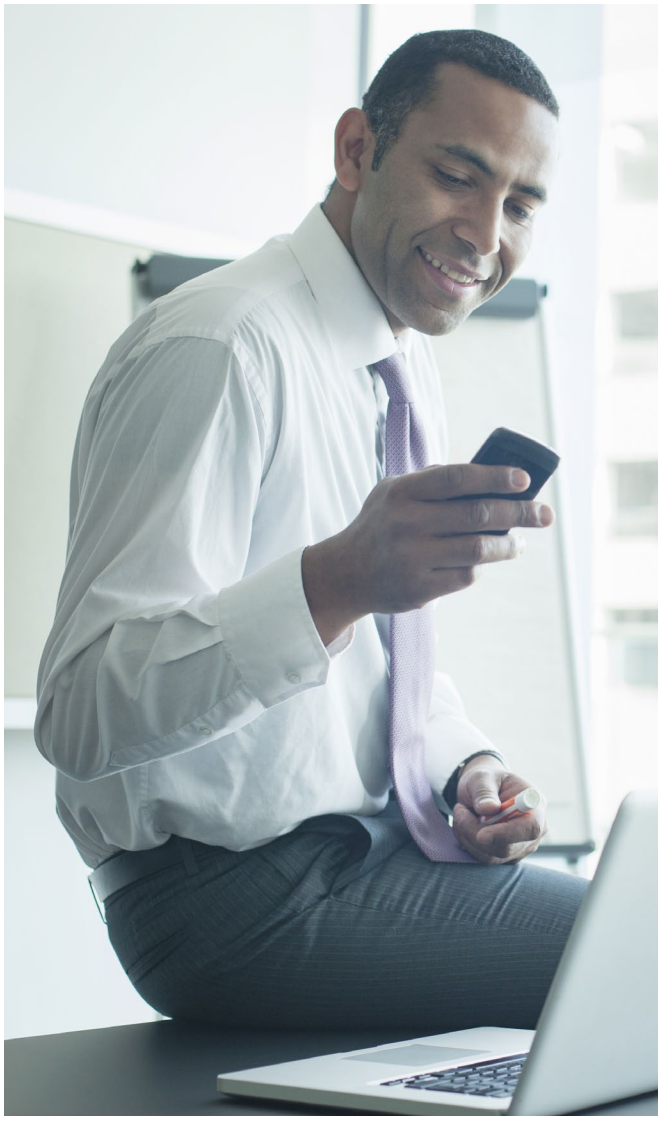
Phishing

- Spear phishing
- Whaling

Command and Control

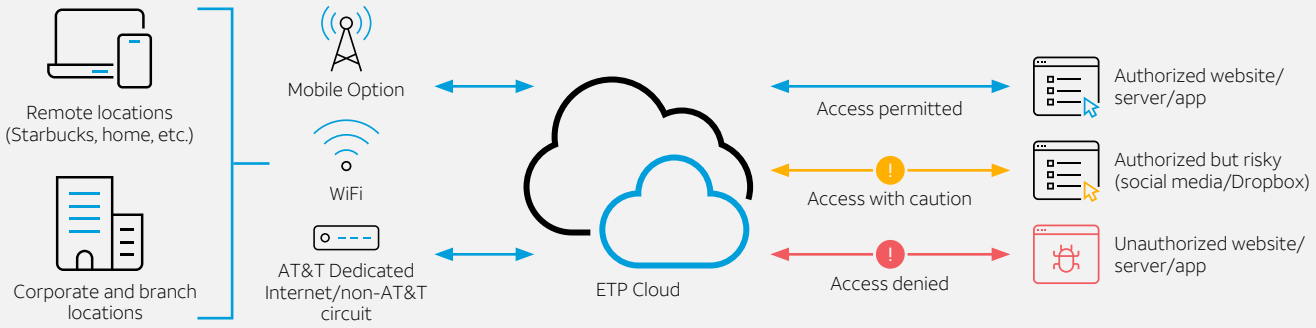
DGA (domain generation algorithm)

Lexical attacks



* TLS: Transport Layer security; HTTPS – Hypertext Transfer Protocol Secure

Enterprise Traffic Protector architecture – all outgoing internet traffic protected against attacks



How it works

- ETP serves as your safe 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 are stopped earlier in the kill chain, away from the enterprise perimeter.

The solution is effective across all ports and protocols, protecting against malware that doesn't use standard web ports and protocols.

It's compatible with other security and reporting tools, such as 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.

It's easy to get up and running: you don't need to set up IPSec tunnels, so you get superior reliability with favorable cost.

Available service offerings

ETP	ETP mobile	ETP advanced
• Protect internet circuits and connected devices from phishing, malware, and ransomware attacks • Support acceptable use policies (AUP's)	• Extend protection to users in remote locations using Windows, Mac, iOS, Android, and Chromebook devices • Provides protection for off net devices accessing the public internet over wireless or WiFi • Protecting mobile devices is as easy as downloading an application and an activation code	• Add more comprehensive traffic inspection capabilities for outbound traffic • Inbound traffic analysis (payload inspection) and sandboxing (HTTP/ HTTPS traffic inspection) • Antivirus capabilities • Data loss prevention (DLP) • Application visibility and control

Available security bundles

Enterprise Traffic Protector is compatible with AT&T Dedicated Internet (ADI), AT&T Broadband, 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
- More favorable pricing

Cloud-based portal

Based in the cloud, this solution offers 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 locations and devices are updated with the latest threat protection.

Unique ability to manage AUPs for both mobile and internet circuits from one portal

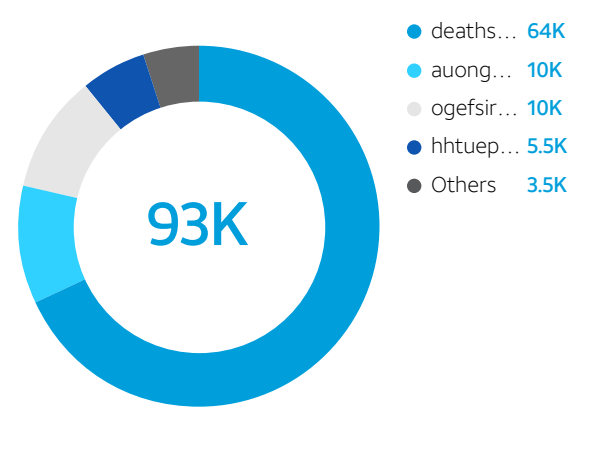
Issue email alerts to security teams on critical policy events to immediately identify, resolve, and remediate potential threats.

Use the real-time dashboard to view DNS traffic, threat events, and AUP activities; drill down on detailed information for security event analysis.

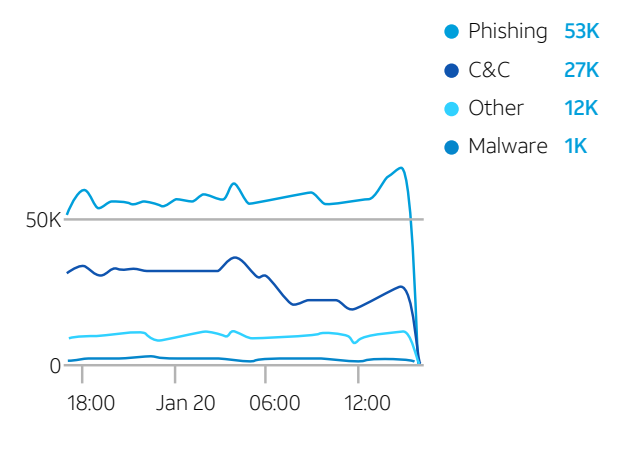
Access the portal via APIs and export DNS data logs to a SIEM to easily and effectively integrate ETP with other security solutions and reporting tools.

Enterprise Traffic Protector could have saved your organization from …

… 93K domain threats



… 93K DNS events



Why AT&T

Choosing the right cybersecurity solutions can be challenging. Evolving technologies and threats continually redefine the digital landscape. We deliver the right fit of insights and guidance, so you feel confident in your ability to drive outcomes and defend your network.

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

*For details of the service level agreement, click here.