AT&T Business

Introducing targeted threat mitigation in the cloud

The enterprise threat landscape is evolving fast. As threats such as malware, ransomware, and data exfiltration increase, malicious actors are getting better at circumventing traditional security approaches.

Combined with the adoption of SaaS, Cloud, and IoT in the enterprise, sophisticated threat delivery introduces new visibility challenges, control-point complications, and security gaps. Powered by unique global insights into Internet and Domain Name System (DNS) traffic, enterprise threat protector services from AT&T Content Delivery Network Service helps security teams to proactively mitigate targeted threats and enforce acceptable use policies across the enterprise.

Enterprise traffic protector services

Built on our global platform and carrier-grade DNS, enterprise threat protector service (ETP) is an easy-to-deploy cloud solution requiring no new hardware or software to deploy or maintain. ETP utilizes near real-time cloud security intelligence monitors and a global recursive DNS platform to proactively identify and help block threats such as ransomware, malware, DNS data exfiltration, and phishing.

Potential benefits

- Significantly helps improve cyber security defenses
- Quickly add a layer of protection without adding complexity or hardware
- Stand up new applications and provision users fast
- Helps reduce management time
- Quickly and uniformly enforce compliance and use policies
- Quickly increase DNS resilience and reliability

Key capabilities

- Automatically categorize threats, based on a combination of over 150 billion daily DNS requests
- Customer categorized threats integrated with customer's existing security investments
- Acceptable use policies allow you to limit which content categories can and cannot be accessed
- Analysis and reporting with near real-time insights
- Logging – DNS logs are retained for seven days and may be exported to .csv or SIEM services
- DNSSEC is enabled on all DNS requests sent to the enterprise traffic protector service

AT&T Business

How it works

DNS is the foundation for most Internet services, yet many malicious domains, including sources for malware, ransomware, and associated command and control (CnC) servers, use recursive DNS for attacks.

When an enterprise's external recursive DNS traffic is directed to ETP, requested domains are checked against global, near real-time domain risk scoring intelligence, which help enterprises to proactively block users from accessing malicious domains and services. As validation occurs before the IP connection is made, threats are stopped earlier in the security kill chain, farther from the enterprise perimeter. In addition, DNS is effective across all ports and protocols, helping to protect against malware that does not use standard web ports and protocols.

Domains can also be checked to determine the type of content an employee is attempting to access, and blocked if the content violates an enterprise's acceptable use policy (AUP). Enterprise threat protector services can be used with other security and reporting tools — including Secure Web Gateways, Next-Generation Firewalls, and SIEMs, as well as external threat intelligence feeds — allowing businesses to maximize their investments across all layers of their security stack.

The cloud security intelligence (CSI) database

ETP is built on data gathered every day from our global cloud security intelligence platform, which manages up to 30% of global web traffic and delivers up to 150 billion DNS queries daily. This intelligence is enhanced with external threat feeds, and the combined data set is analyzed using advanced behavioral analysis. As new threats are identified, they are immediately added to the ETP service, helping to improve near real-time protection against threats for enterprises and their employees.

Cloud-based management portal

All configuration and ongoing management of ETP may be performed using the cloud-based Luna portal, enabling management to be done via the web from virtually any location at any time.

Policy management is quick and easy. Changes can be pushed out globally in minutes to validate that all enterprise locations and employee devices are updated with the latest threat information. Email alerts can be configured to signal security teams about critical policy events so that immediate remediation steps can be taken to quickly identify and resolve potential threats. A near real-time dashboard provides an overview of DNS traffic, threat events, and AUP activities. Detailed information on any activity can be viewed through drilldown on individual dashboard elements. This detailed information provides a valuable resource for analysis and remediation of security incidents. All portal functionality can be accessed via APIs, and DNS data logs can be exported to a SIEM, allowing Enterprise Threat Protector to easily and effectively integrate with your other security solutions and reporting tools.

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