AT&T Content Delivery Network (CDN) with Web Security

Kona Web Security Solutions

High-performance content delivery networks (CDNs) can be ideal when you need to speed rich digital media, highly interactive web applications and personalized content to your customers.

With bandwidth-hungry videos, software, images and JavaScripts cached on local, strategically distributed proxy servers across the CDN – instead of origin servers in a data center – you can accelerate content delivery to a range of wired and wireless devices.

While security solutions are often in place to protect the data center, the enterprise network and devices, the proxy servers that handle the majority of CDN traffic can remain exposed to risks. AT&T Content Delivery Network (CDN) with Web Security can help close this security gap for you.

Multi-Level Web Security

The AT&T CDN with Web Security suite helps defend your CDN from Distributed Denial of Service (DDoS), web application and DNS infrastructure attacks. Growing in number and sophistication across industries, these threats increase downtime and bandwidth costs while putting confidential business and customer data at risk.

Used in conjunction with the AT&T security portfolio, AT&T CDN Kona is a critical element in a complete, end-to-end web security solution – extending protection from the data center and the network to the CDN and mobile devices.

DDoS Mitigation

DDoS attacks can severely impact productivity, revenue streams and your brand. AT&T CDN with Web Security provides a perimeter of defense that extends beyond the data center to help:

- Authenticate valid CDN traffic at the network edge
- Mitigate risks natively in-path, close to the source of attack
- Stop DDoS attempts from infiltrating the application and network layers and origin servers
- Monitor the rate of requests to block suspicious activity and identify the client source
- Cap bursting fees to help control CDN bandwidth costs

Web Application Protection

Web Application Firewall (WAF)

With WAF protection, you can detect and deflect threats in HTTP and HTTPS traffic, targeted at the application layer. It offers:

- Common rules for addressing the most recent and populavr threats
- ModSecurity CRS 2.26 support
- Application layer controls to set policies for handling SQL Injections, Cross-Site Scripting and other attacks
- Ability to create custom rules to prevent vulnerabilities caused by new threats
- A security monitor for real-time visibility into security events and trends

Potential Benefits

- Reduced downtime to help protect your revenue and reputation
- Faster content delivery to promote a positive customer experience
- Protection from DDoS, web application and DNS infrastructure threats
- Reliable CDN performance and uptime, even during an attack
- Cost-effective handling of spikes in attack traffic
- On-demand scalability
- Self-service portal for insight, reporting and control
- End-to-end solution to help close security gaps
- A single provider for increased enterprise security

Features

- DDoS mitigation
- Web Application Protection Firewall
- Origin cloaking
- Security Monitor
- User Validation Module (optional)
- Enhanced DNS protection (optional)

Want to learn more?
Have us call you.

Share this with your peers

Network Layer Controls

AT&T CDN with Web Security can help you respond and mitigate network threats quickly by enabling you to:

- Create and enforce IP white lists and black lists that allow or inhibit requests
- Restrict requests from specific IPs
- Block requests from specific geographies
- Update and propagate the list across a global CDN within minutes
- Administer network layer controls via a Representational State Transfer (REST)-based API

Adaptive Rate Controls

Monitor the number of requests to help defeat HTTP flooding attacks. Rate controls can help you:

- Detect potential threats based on behavior patterns
- Identify attackers hiding behind proxies
- Block IP addresses with excessive rates of forward requests
- Spot and mitigate slow rate resource attacks
- Prevent bandwidth and origin overload to help maintain performance

Site Shield

Site Shield adds another layer of protection for the origin servers that send content to users through your CDN, without impacting CDN performance and reliability. To help prevent direct-to-origin attacks, Site Shield cloaks origin servers from the public internet, removing them from DNS resolution and direct client communication via IP. Only a designated set of proxy servers in your CDN are allowed access to origin servers.

Enhanced DNS Protection

Without adequate Domain Name Server (DNS) protection, you leave end user devices vulnerable to attacks, such as DNS cache poisoning, which directs users to fraudulent sites.

Enhanced DNS protection, an optional feature in AT&T CDN with Web Security, helps to ensure legitimate users get direct access to your website and applications. It utilizes the global reach, scalability, security and reliability of the AT&T CDN DNS infrastructure, which can provide primary or secondary authoritative name servers. To strengthen DNS security, this solution also supports Domain Name System Security Extensions (DNSSEC).

User Validation Module

This optional AT&T CDN with Web Security module can reduce your exposure by helping you develop a better understanding of who or what is targeting your website or web application. By requiring the browser to test and validate clients requesting access to your CDN, the module differentiates between allowable human-generated requests and machine-based bots with malicious intentions that need to be denied.

Simplified Security from a Single Vendor

If you want a single source for end-to-end security and enterprise-wide threat protection, talk to your AT&T representative about AT&T CDN with Web Security and the entire family of AT&T CDN Service offerings.

Share this with your peers

For more information contact an AT&T Representative or visit www.att.com/cdn-services.

Scan this code to learn more.

Want to learn more?
Have us call you.

07/25/16 AB-2672-01

© 2016 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo and other marks are trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein 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.