Secure your web properties and APIs using a single platform with AT&T App and API Protector

Take your security strategy to the next level with an adaptive self-tuning solution that keeps critical web applications and data safe and secure.

Web applications and APIs make it easy to do business and connect with customers and third-party partners. To make sure your websites, applications, and APIs remain trusted and secure, you need a web application and API protection (WAAP) solution that automatically learns, adapts, and defends against new and existing threats across all your attack surfaces.

AT&T App and API Protector strengthens your security strategy with a single WAAP solution that monitors and inspects incoming traffic at the edge to halt attacks before they happen.

Why choose AT&T App and API Protector

With so many applications and APIs to keep track of, it's hard to identify every loophole or vulnerability. AT&T App and API Protector is purpose-built to address this evolving application landscape. We combine advanced automation, machine learning, and adaptive self-tuning to protect against volumetric distributed denial of service (DDoS), automated botnet, injection, and API-based attacks to defend your network and applications.

Features

- Adaptive self-tuning security offers precise, accurate, threat-based detection
- Extensive security controls detect and stop unwanted bots
- Security policies stay up to date
- Seamless protection scales to meet traffic demands with accelerated performance

Benefits

- Single solution protects websites, apps, and APIs from a broad range of threats including DDoS, botnets, injection, and API-based attacks
- Frictionless maintenance
- Significantly reduces API attack surfaces
- Optimizes spending

Security that is adaptive and self-tuning

Modern applications and APIs use lots of moving parts, shared components, and third-party services. To prevent unauthorized access, AT&T App and API Protector checks every web and API request against the latest threat intelligence to identify attacks and reduce false positives that need to be investigated. Adaptive decision-making capabilities monitor inbound network traffic to guard against a wide range of common and targeted attacks. From there AT&T App and API Protector uses machine learning to analyze each threat and make policy recommendations that can be added to your existing protocols, quickly and easily.

Advanced API detection

The best offense is a lockdown defense. That's why AT&T App and API Protector scans all APIs in your web traffic by default and inspects them for errors, changes, and harmful code. It also collects information related to API endpoints, definitions, and profiles in the event of unexpected updates. And registering new APIs is done in just a few clicks. Our optional Advanced Security Management tool provides additional protection at the network edge to secure against unauthorized or suspicious API behavior.

Real-time bot visibility and mitigation

Using a directory of thousands of known bots, AT&T App and API Protector detects, monitors, and defends against harmful bots and DDoS attempts without impacting the work of registered bots that make life easier for your users.

> "AT&T is my first stop for security and technology."
>
> Stephen Locke
> Chief Information Officer, NHS Management, LLC

DevOps integration and collaboration

AT&T App and API Protector includes programmable APIs and security information and event management (SIEM) integration to speed software development, IT operations, and policy decision making. It also improves collaboration across teams and workflows to ensure your security keeps pace with the changing threat landscape.

Optimal performance, maximum protection

Your website is essential to the success of your business. AT&T App and API Protector scales to meet your traffic demands, monitoring and adjusting central processing unit (CPU) and memory resources to keep you protected during times of peak activity. Cached content is delivered to the edge, along with image and video optimization, API acceleration, and edge computing capabilities to ensure your applications always perform at their best.

Advanced security management

Our optional Advanced Security Management module offers flexibility and control when customized security measures are needed. A manual update option lets you review new updates alongside existing protections, so you understand what is being updated and how you'll benefit. It also includes additional tools to manage web and API protections, including access to internet protocol (IP) threat intelligence data to verify the authenticity of the requests you're receiving.

Additional capabilities

- Automatic updates
- DoS/DDoS protection
- Network lists block malicious requests from specific IPs or traffic
- Custom rules
- Hostname evaluation
- Response actions
- Site Shield
- Dashboard, alerting, and reporting tools
- Simplified onboarding

Secure your network and your business with AT&T App and API Protector.
877.287.5676

Why AT&T

Technology is complex. Transformation is fast. Are you making the right choices for your cybersecurity? What you want is simple advice that you can easily understand and apply. We deliver the right insights, guidance, and solutions for you.

Contact your AT&T Cybersecurity representative to learn more.