AT&T Cybersecurity

AT&T Business

# AT&T Managed Vulnerability Program (MVP) Web application shielding powered by RedShield

Shielding your application vulnerabilities, so you can get on with business

Virtually every business uses a combination of web portals, mobile applications, and Application Programming Interfaces (APIs) to conduct their business. These mechanisms are critical to success and for growing the business. Yet many applications still have vulnerabilities that needs some type of security patching and the rise of exploitation of these vulnerabilities continues to grow exponentially.

Risk optimisation is the process of achieving an optimal balance between risk and return (reward) within a specified portfolio. It is important to focus on fixing known broken things rather than blocking attacks, it is also important to satisfy expectations for application security.

Security vulnerabilities in your applications are a significant risk for organizations of all sizes. Some challenges they pose:

- They can be exploited by third parties, causing serious reputational damage and financial impact.
- Fixing vulnerabilities is time consuming and expensive, and as a result often gets delayed, deprioritized, or even ignored, leaving you unnecessarily exposed and unable to get on with business.

## Potential benefits

- Free up limited internal resources to work on other critical
- Extend life of legacy applications that cannot be patched
- Allow for delayed patching or code remediation
- Achieve compliance and meet regulatory or accreditation requirements e.g., PCI
- Proactively protect against newly discovered exploits
- Managed vulnerabilities in developer security backlogs
- Protect applications post functional development and reduce release cycles
- Optimize risk and security posture

## Do these situations appear familiar?

- I have legacy apps and no way to access the code to remediate
- The web applications are important and cannot afford downtime
- How do I shield the known vulnerabilities?
- Cannot afford to wait for patches
- Cannot afford to reallocate resources away from other projects

**Shielding from AT&T**
Shielding from AT&T is a cloud based managed service that help prevent exploitation of web application or API vulnerabilities and protects them against DDoS attacks. It does this by:

- Deploying a unique technology “shielding” applications by front-ending them as a hardened proxy compensating for patching, logic and code flaw vulnerabilities.
- Wrapping this technology with a fully managed service that constantly scans for new vulnerabilities, deploys new shields as required and reports on shielding efficacy.

This helps protect your business against the exploitation of application vulnerabilities and allows you the time to patch or rewrite the application code or to work with your software vendor or SaaS partner to correct the code. An additional benefit is that it may immediately improve your cybersecurity posture as reported by publicly available assessment services and tools.

**How does shielding work?**
Shielding works in several ways, but in general, once a vulnerability is identified as present in an application our engineers determine the triggering event or events in the application traffic flow and craft a shield that triggers on that. The shield/s are built to modify or transform requests and/or responses in the traffic flow so that the vulnerability and exploit are mitigated or remediated. All if this is done without modifying the underlying application code. This allows shields to work for any application including 3rd party written applications, frameworks, hosting platforms, etc.

**Delivering outcomes:**
Coupling Shielding from AT&T with AT&T’s Managed Vulnerability Program to find vulnerabilities in your internal and external systems and AT&T’s penetration testing services can help deliver material outcomes for your cyber teams and organization. Some of these include optimizing risk and security posture immediately and on an ongoing basis, allowing for delayed patching, code remediation or replacement, achieving compliance and freeing up internal resources to work on priority projects.

AT&T Cybersecurity

AT&T Cybersecurity helps reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our Software-as-a-Service (SaaS)-based solutions with advanced technologies (including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™), and our relationship with more than 40 best-of-breed vendors help accelerate your response to cybersecurity threats. Our experienced consultants and Security Operations Center (SOC) analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.