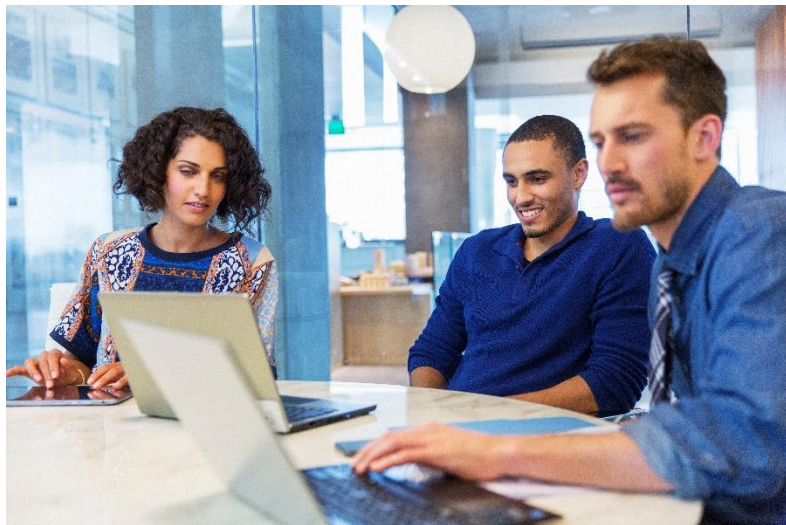# Get security you can trust with AT&T Managed Vulnerability Program (MVP) Client-Side application security
powered by Feroot

Businesses spend millions of dollars annually to protect their networks from direct threats and attacks. However, many companies fail to also protect from attacks on their client-side web applications.

Client-side security is necessary for any companies that conduct business with users digitally via marketing landing pages, e-commerce technologies, user portals, and other technologies that allow communication and collaboration directly with their customers.

In any organization, multiple groups would benefit from the addition of client-side security solutions:

- Cybersecurity professionals are the last line of defense against client-side cyber threats.

- Application engineers and developers build class-leading web applications that must remain safe and secure indefinitely.

- Application security professionals work to ensure customer data collected has proper protections and controls in place.

Potential benefits

- Significantly reduce the manual burden of client-side security

- Speed up the response to threats

- Replace multiple, time-consuming processes and technologies with one simple, automated process

- Receive reports and remediation advice on vulnerabilities

- Recognize first- and third-party code issues and how to fix them

- Discover and classify web assets to enable secure innovation

- Prevent data exposure and exfiltration

- Gain a comprehensive overview of all web assets used and data captured

Do these pain points sound familiar?

- Inability to detect and respond to client-side threats in real time

- Complexity of third-party JavaScript security

- Building secure client-side web applications and keeping them safe from cyber attacks

- Complying with increasingly stringent privacy regulations

Feroot Client-Side Security from AT&T

AT&T Managed Vulnerability Program (MVP) team now offers enhanced application security and monitoring powered by Feroot Security solutions. These new services allow the MVP team to inspect and monitor customer web applications for malicious JavaScript code that could jeopardize customer and organization security. With well-publicized security breaches based on script injection and Magecart, weaknesses such as cross-site scripting, these protections are critical to ensure the ongoing security of your customer's web experience.

The solutions, PageGuard and Inspector, discover all web assets a company utilizes to conduct business with its customers in seconds. The solutions detect and outline abnormal application behaviors, so that security teams can take remediation action and shorten the time the organization and their customers are exposed to malicious activities. By providing an accurate view of the client-side attack surface and revealing previously undetected threats and backdoors, customers can increase the security of their mission-critical JavaScript applications.

The solutions detect Magecart skimming attacks, malicious code changes in first- and third-party scripts, abnormal behaviors in application code, unauthorized data transfers, and many more client-side security issues. This allows cybersecurity, application security, or application development teams to take quick and correct responsive actions. With notifications provided via in-app alerts and API integrations with security technologies and ticketing systems, including integration support and ongoing monitoring from the MVP team, these insights are easy to incorporate into existing workflows.

Delivering outcomes:

AT&T is helping customers strengthen their cybersecurity posture and increase their cyber resiliency by enabling organizations to align cyber risks to business goals, meet compliance and regulatory demands, achieve business outcomes, and be prepared to protect an ever-evolving IT ecosystem.

To learn more about how AT&T MVP can help fortify your security contact your AT&T sales professional.

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.