THE MEDIA TRUST

Media Scanner for Retail Websites and Mobile Apps

Protect your digital properties from malware, data leakage and site performance issues by monitoring all third-party code on a 24/7 basis

Forecasted to continue its double-digit growth rate, online shopping is now a primary revenue source for many retailers. With their high-volume traffic and access to consumers' credit cards, these sites also serve as revenue sources for hackers and fraudsters, who find retailers' reliance on third-party vendors especially appealing.

Unbeknownst to many retailers, the third-party vendors they use to render their websites—payment systems, automated marketing services, videos, product reviews, social media tools, content recommendations and more—can unintentionally function as a conduit for malware. More specifically, hackers identify a vendor with weak security controls and then compromise their servers. With control of these servers, the hackers can negatively impact the consumer's browsing experience in many different ways—download harmful exploit kids, steal credit card numbers and other personal information, redirect the consumer to a propaganda site or leverage the third-party code to deface the retailer's website.

Web-based malware can attack with such impunity because very few IT/InfoSec and ecommerce teams manage the third-party code executing on their website. They don't realize each piece of external code represents a potential entry point for web-based malware. They have no idea of the path each domain and cookie took to their site so they cannot know if and where malware was injected. It's this lack of real-time control and visibility that allows web-based malware to attack ecommerce sites so easily.

Unfortunately, traditional security tools can do little to prevent such attacks. While these tools can protect against malware targeting corporate networks, email systems and the web apps behind the corporate firewall, they fail to address and manage the risks associated with third-party source code executing on a website's "external layer"—the location where the site renders on the consumer's browser. It's here that web-based malware attacks with no fear of detection for days, weeks and even months by traditional security tools.

Media Scanner for ecommerce sites

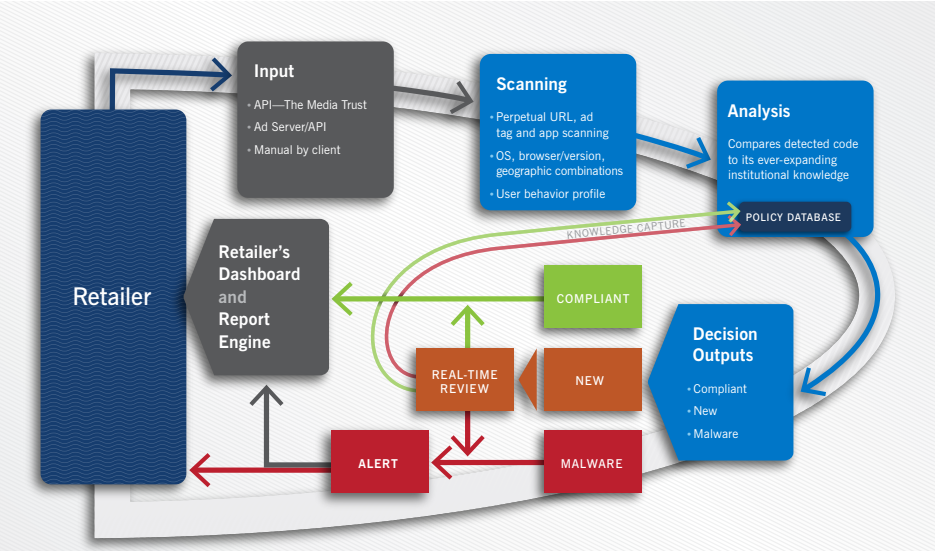
To protect against third-party code's inherent risks, IT/InfoSec and ecommerce teams must constantly monitor—in real time—the code executing on their sites. A comprehensive, SaaS-based service that scans ecommerce sites and apps on a continuous, 24/7 basis, The Media Trust's Media Scanner service automatically detects and analyzes all third-party code accessing the retailer's site or app and sends an immediate alert on any instance of unknown, suspicious or malicious codes so that IT/InfoSec and ecommerce teams can remove and then block it.

Powered by The Media Trust's proprietary technology, which continually assimilates and acts on emerging threat vectors, Media Scanner provides ecommerce sites and apps with:

- **Malware Prevention**: Issues real-time alerts on all unknown or suspicious code, halting its delivery before it morphs into overt malware.
- **Data Protection**: Detects and alerts on unknown and unauthorized code designed to capture valuable website audience data (first-party) without consent—code that causes privacy violations and compromises the ability to monetize this data.
- **Third-party Content Management**: Identifies and monitors the domains of third-party providers executing on a site, including analytics, data management, dynamically-served content, third-party video, mapping applications, local info, native advertising, advertorials and microsites. Tracks vendors by tag, host and URL to ensure only authorized activity.
- **Encryption Compliance**: Automates the process of enforcing and maintaining HTTPS compliance across all third-party vendors, ensuring every call in the chain remains secure.

The Media Trust's Media Scanner for ecommerce sites and apps:

- Scans millions of websites and more than 10 million ad tags every day
- Operates on a 24/7 basis from more than 500 cities in 65 countries
- Detects a new malware vector every 60 seconds
- Delivers 99.95% alert accuracy
- Ensures 100% HTTPS encryption compliance
- Uses a variety of browser, OS, geography and behavior profile combinations to root out detection-evading strategies
- Provides robust reporting of detailed website activity
- Counts 40 of the Top 50 comScore Ad Focus leaders—the world's most heavily trafficked websites—as clients



Process flow for Media Scanner

How Media Scanner works

To start using the service, retailers input their relevant site information into Media Scanner using either an API or manual entry. With this information, using a wide variety of browser, OS, geography and behavioral profile combinations, the system immediately initiates the scanning of all ecommerce sites and apps, analyzing all third-party code executing on the site or app and comparing it to client-defined "white lists" and "black lists" of domains and cookies.

This analysis generates a decision output that determines if the code is compliant with existing policies, is unknown to the system, is known malware or indicates data leakage of the site's first-party data. Compliant third-party code requires no interaction—the system automatically captures and archives this result in the retailer's dashboard. Third-party code indicating the presence of malware or data leakage results in Media Scanner auto-generating an immediate alert to the retailer and a report to the dashboard.

New, never-before-seen code is reviewed by The Media Trust's Malware and Data Protection Teams to determine if it is compliant or violates any security or data policies, which eliminates false positives. Media Scanner then posts the results of this analysis to the client's dashboard and the system's database.

This self-perpetuating, virtuous cycle allows the system and the Malware and Data Protection Teams to continually cultivate their deep institutional knowledge of anomalous and malicious code and ensures The Media Trust is always at the forefront of web-based malware and first-party data protection.

Protecting the browser experience

The Media Trust's daily monitoring of millions of ecommerce, media and corporate websites and mobile apps—not to mention more than 10 million ad tags—provides it with a panoramic view of the global online and mobile ecosystem. As a result, Media Scanner provides retailers with:

- Actionable intelligence on their ecommerce site's vendors, domains, cookies and, if applicable, ads
- High-frequency, continuous and automated monitoring of both sites and mobile apps, regardless of audience browsing habits
- Real-time visibility of all external code executing on their site, which ensures the removal of anomalies before they can render on consumers' browsers
- Control over website vendor utilization by documenting which department—marketing, legal, IT, etc.—authorized the vendor and its designated services
- Real-time, actionable intelligence on active threats occurring elsewhere in the online and mobile ecosystems

The Media Trust
1749 Old Meadow Road
Suite 500
McLean, VA 22102
703.893.0325
www.themediatrust.com
@TheMediaTrust

About The Media Trust

With a physical presence in 65 countries and more than 500 cities around the globe, The Media Trust's proprietary website and ad tag scanning technology provides continuous, non-stop protection against malware, site performance issues and data leakage, which can lead to lost revenue and privacy violations. The Company also enables comprehensive quality assurance of an ad campaign's technical and creative components and provides publishers with visual ad verification for geographically-targeted campaigns, ensuring thousands of media buys are executed correctly, reducing discrepancies, errors and make-good scenarios in-flight.

More than 500 publishers, ad networks, exchanges, agencies and enterprises—including 40 of comScore's AdFocus Top 50 websites—rely on The Media Trust's suite of continuous, non-stop monitoring, detecting and alerting services to protect their websites, their revenue and, most importantly, their brands.