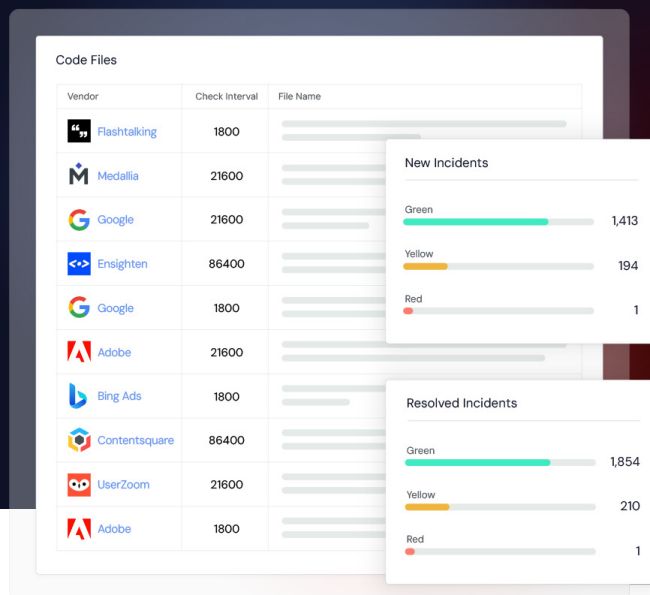# Hacked Martech Opens Doors to All the *Wrong People*

Even with all you've done to secure your site, hacked third-party martech can open entry points to attackers. Vault JS Secure finds those vulnerabilities as quickly as they emerge.

Vault JS provides day-zero visibility into third-party risks, allowing enterprises to terminate high-risk partner access immediately.

Code Files

Vendor	Check Interval	File Name
Flashtalking	1800	
Medallia	21600	
Google	21600	
Ensighten	86400	
Google	1800	
Adobe	21600	
Bing Ads	1800	
Contentsquare	86400	
UserZoom	21600	
Adobe	1800	

New Incidents

Green		1,413
Yellow		194
Red		1

Resolved Incidents

Green		1,854
Yellow		210
Red		1

Damaged Reputations, Millions in Fines

EQUIFAX
$575M

BRITISH AIRWAYS
$230M

"We feel like we've augmented our staff with Vault JS's AI and real-life security analyst. A really good one!"

General Manager of Digital Technical Products
Top 5 Global Airline

A Third-Party Martech Watchtower

Martech can offer attackers the easy entry points they're looking for unless you get there first. Vault JS Secure tells you where to look.

Get full visibility of your martech vulneratibilities and pull in your Data Thief Welcome mats

Vault JS was architected with security in mind. It automates martech oversight with no additional security investments

The value is immediate. See 80% of Vault JS's value right away, with no human help

Vault JS' constant surveillance can help identify and prevent third-party martech hacks like the 24/7.ai data breach.

In this case, hackers infected the popular customer service software, 24/7.ai, leading to the theft of names, addresses, and credit card information for hundreds of thousands of Sears, Kmart, and Best Buy customers. Protect your customers' information with VaultJS Secure.

How Vault JS Secure Works

Vault JS protects your data using a dynamic, mutliphase approach to stop attackers seeking to steal it or commit Magecart attacks.

AI-driven Code Analysis

Vault JS's proprietary Code Analysis Engine incorporates our deep technical expertise in tag management.

Human Review

With the analysis engine set to Highly Sensitive, our subject matter experts ensure zero false positives.

Fingerprinting

Identify when vendors are tracking your users, even when they aren't using cookies.

Code Analysis Archive

We maintain a full audit history of every scan: when code arrived, what changed, what broke.

Monitor Secure Areas of the Site

Use our Automated Users feature to log in to an area of a site and analyze it for vulnerabilities.

Vault JS Secure

Before our leadership team founded Vault JS, they first created the tag management industry with ground-breaking, patent-winning solutions that are widely used today. Vault JS was created in direct response to their unique understanding of the threats posed by placing third-party JavaScript on a website.

In addition to holding multiple patents, they have previously raised $100M+ in venture capital and served the privacy and security needs of some of the world's largest enterprises.

Vault JS