Ensighten MarSec™

Block Customer Journey Hijacking and Win Back Lost Revenue

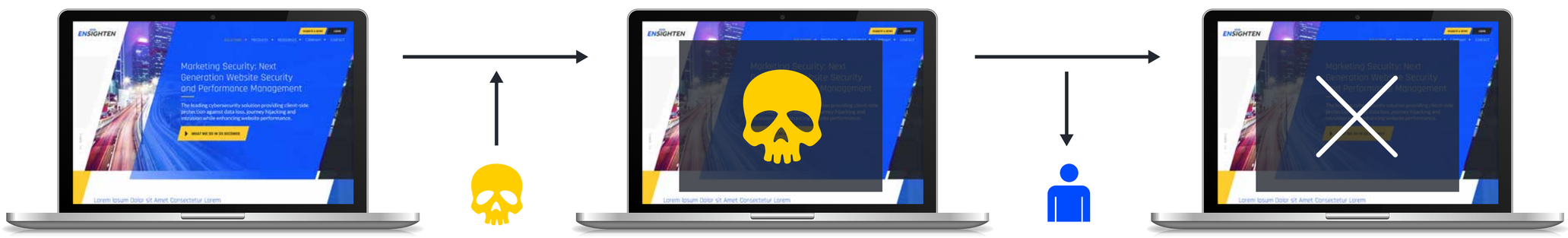
Stop your competitors from stealing your customers and revenue by blocking unauthorized ads and adware on your website

Customer journey hijacking and adware injection is a rapidly growing problem. Online visitors are being targeted with unauthorized ads which plague their online experience with product ads, pop-ups, banners and in-text redirects, disrupting their experience and driving them to competitor or malicious websites.

Not only does this create a frustrating experience for your customers, but you could lose valuable business to other companies – without realizing it is even happening.

How does it happen?

Unwanted software such as adware is injected into your website visitors' browsers without their permission. It then targets them with advertising to encourage traffic to this unauthorized source, thus driving your customers to competitor or malicious websites - and ultimatelity decreasing your conversion rates and revenue. This type of attack happens client side, meaning that as a website owner you have no visibility into what's happening and are likely to be unaware of how and when this is happening, along with just how much it is affecting you.



User visits your website and adds items to shopping cart

Meanwhile, competitor advert is injected into your site

User is presented with a competitor advertisement, using compelling offers to attract your visitor to click on the advert

Potential customer leaves your site to transact with your competitor

This leads to lost revenue and poor user experience

"You could lose valuable business to other companies without realizing it is even happening"

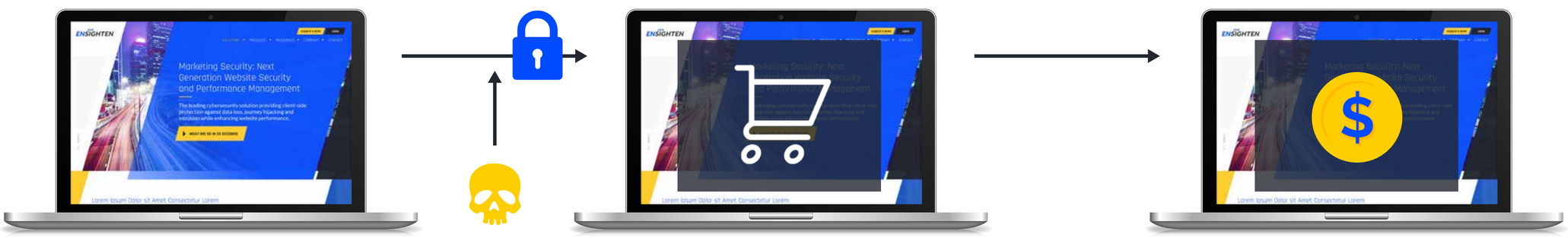
Solution

There is a way to win back stolen revenue and prevent adware and online customer journey hijacking. Our solution allows you to detect and prevent customer journey hijacking where previously it flew under the radar.

Our solution enables you to detect, manage and block any unauthorized advertising and malware injected into visitor sessions - and stop your customers from being diverted to other websites. Through our platform we will enable you to:

- Keep your web visitors on your site to increase conversion rates
- Win back stolen revenue through blocking potential diverted web visits
- Decrease your shopping cart abandonment figures
- Enhance and protect customer experience through a distraction-free online journey
- View attempted ad injections on your website in real time
- Block ad injection, adware and malware on your website

Our customer journey hijacking tool provides full visibility into any potential treats or hijacked sessions, and can be easily integrated with your existing software toolset.



User visits your website and adds items to shopping cart

Meanwhile, Ensighten blocks all unauthorized adverts from appearing on your website

The user continues with online shopping experience to transact

There is no disruption of competitor ads or adware

You retain control of revenue and customer experience on your website

"Ensighten has not only ensured our website is protected from client-side data leakage and cyberthreat groups, but also enabled us to block malicious and competitive advertising which had effected our conversion rates and revenue. We saw an immediate uplift in conversions and sales as soon as we implemented the solution"

Leading global retailer, August 2019

About Ensighten

Ensighten is a global cybersecurity leader, offering next generation client-side protection against data loss, journey hijacking and intrusion. Through the Ensighten solution, organizations can access privacy risk and stop unauthorized leakage or theft of data, as well as complying with CCPA, GDPR and other data privacy regulations. Ensighten's MarSec™ platform protects some of the largest brands in the world from data leakage, whilst ensuring maximum web page performance.

Phone: 1-650-249-4712 | www.ensighten.com | Email: info@ensighten.com | Twitter: @ensighten | LinkedIn: @ensighten

ENSIGHTEN