ENSIGHTEN

Website Security

Next Generation Website Security and Performance Management

The leading cybersecurity solution providing client-side protection against data loss, journey hijacking and intrusion while enhancing website performance

Protect against data leakage

For many organizations their website and mobile applications are the cornerstone of their business, and from here web applications have evolved to enable greater functionality by leveraging client-side capabilities. As such, security evolution must follow.

Payment card and web skimming exploits are regularly hitting the headlines, highlighting a clear need for organizations to review the security risks within their website supply chain. A compromise of a website supply chain vendor through an injection of malicious JavaScript can be detrimental to an organization operationally and financially as well as harming your reputation.

Prevents theft, disclosure or leakage of sensitive information to third parties

2018 saw the rise of hacking threat group Magecart, who successfully exploited data from over 300,000 websites

Prevents website code being changed or altered without notification

If maliciously compromised, this code can leverage your website visits to mine cryptocurrency or steal customer data

Prevents third-party code invoking additional JavaScript calls often known as tag piggybacking
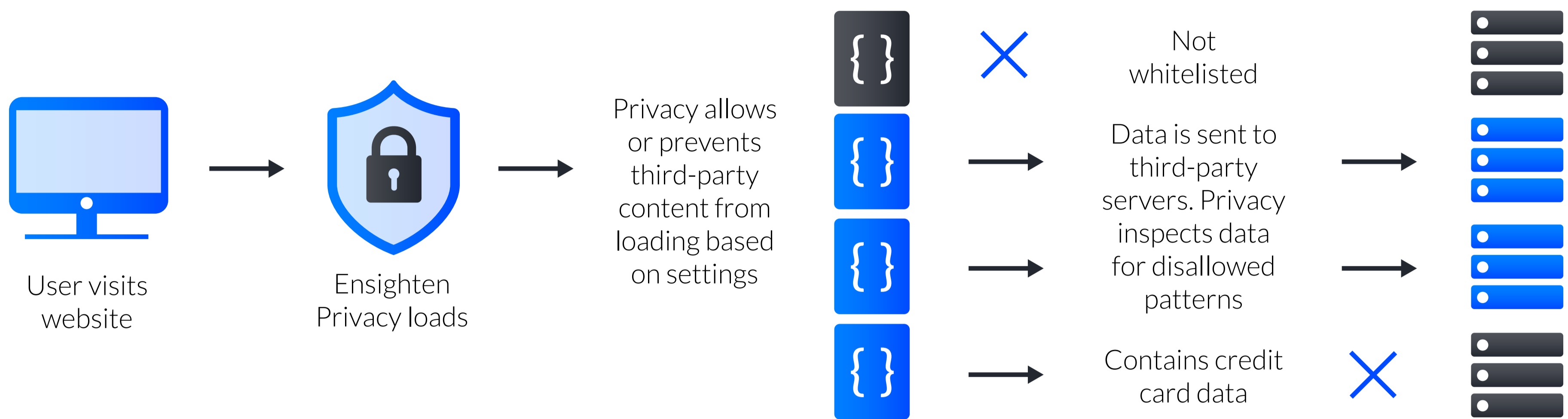
This creates a potential breach and aggravates various security considerations

"Ensighten provide the most important piece of tech that we use. We know that our website is our weak point - the minute we implemented Privacy in observe mode we saw scripts we did not recognize. Now that we are live we trust that Ensighten protects the data we collect from attack"

Leading global ecommerce organization, January 2019

MarSec™ client-side website security

The Ensighten Marketing Security (MarSec™) platform is an approach favoured by leading enterprise brands looking to implement real-time, client-side website application security without adding overhead to already stretched development teams, whilst avoiding a compromise on website performance, functionality and usability.

User visits website → Ensighten Privacy loads → Privacy allows or prevents third-party content from loading based on settings

Not whitelisted

Data is sent to third-party servers. Privacy inspects data for disallowed patterns

Contains credit card data

1. Deploy
Easily deploy our Privacy gateway through a single line of code

2. Observe
The Ensighten Privacy gateway monitors all network requests made through the DOM or XHR

3. Configure
White- or blacklist scripts and URLs, and set data leak prevention policies for credit card and sensitive data

4. Enforce
Enforce mode activates configurations in real time to ensure adherence to data governance policies

5. Report
Intuitive interface details blocked requests for review and identifies brand impersonation and malicious proxy sites

Protection against data leakage through MarSec™

Real-time website monitoring
Monitor all network requests coming into or out of your website to detect any potential malicious threats

Privacy gateways
Block unknown and unwanted website trackers, technologies and tags to prevent them from firing on site and collecting data

Blocking of unauthorized network calls
Block Magecart style attacks, CSS hacks and man in browser to protect end-users and stop data breaches

White- and blacklisting of third-party technologies
Define permissions of the appropriate third-party vendors you want to allow to receive data, or block vendors from receiving specific types of data

Automated website privacy audit and alerts
Detect risks to your organization's privacy rules; website scanning will check for unapproved technologies that might have access to your customer data

Masking of sensitive data
Determine unique data patterns to prevent being exposed within the URL and avoid sensitive data from being passed to unauthorized third-party technologies

Ensighten has protected over 12 billion website visits since January 2018

ENSIGHTEN