imperva

DATASHEET

Client-Side Protection

Prevent data theft from client-side attacks like formjacking, digital skimming, and Magecart.

There’s a lot of untrusted, untested code running on enterprise websites that no one knows is there, making for a lucrative attack surface for fraudsters and bad actors. The widespread use of JavaScript services on web applications has created a blind-spot for security teams. They struggle to keep inventory of all these services executing in their applications at any given moment. Even with proper tracking of these services, the risk of a familiar third-party service becoming compromised is real. Once compromised, client-side attacks like formjacking, digital skimming, and Magecart can exploit it to steal sensitive data directly from the client. Due to the stealthy nature of these attacks, they often go undetected for extended periods of time, resulting in a massive customer data breach.

Imperva’s Client-Side Protection

Client-Side Protection mitigates the risk of your customers’ most sensitive data landing in the hands of bad actors. It prevents supply-chain fraud from Client-Side attacks like formjacking, Magecart and other online skimming attacks. Client-Side Protection automatically scans for existing and newly added services on your site, eliminating the risk of them being a blind-spot for the security team. By providing clear visibility with actionable insights as well as easy controls, it empowers your security team to effortlessly determine the nature of each service, and block any unapproved ones.

KEY CAPABILITIES

DISCOVERY

- Discovers current services
- Continuously discovers new services
- Needs Review alerting
- Domain search and filtering

BLOCKING

- Out-of-the-box blocking of known malicious services
- Easily block unapproved services with just 1-click
- Identifies all allowed or blocked services

INSIGHTS

- Visibility into service status
- Understand requested resource type
- Domain country origin
- Service discovery date
- Certificate status check of domain
- External domain insights
- Service location with code

Continuously monitors for new JavaScript services

Websites are constantly improved and updated with new code and functionality. Unfortunately, security teams are typically blind to any new services being executed. If any of these services are compromised, the website could become the victim of a client-side attack like formjacking. Imperva's Client-Side Protection gives security teams visibility and control over any third party JavaScript code embedded in your web applications. With continuous monitoring, the security team is alerted to any new services being executed.

Provides actionable insights to security teams

Beyond just identification of services and blocking known malicious ones, Imperva's Client-Side Protection offers detailed insights about all JavaScript services on your website. The domain risk score adds a credibility rating for each service, making it easier for security to determine the nature of each service, and decide whether it should be allowed to run or not. Client-Side Protection helps security professionals make informed decisions by providing meaningful and actionable insights.

Identifies compromised code and reveals data transfers

Client-Side Protection alerts users when a newly added service is detected, while automatically blocking ones that are known to be malicious. Any new service or changes are blocked until authorized, and if any JavaScript code is compromised, and attempts to send data elsewhere, your security team is the first to know.

Safe, one-click deployment

As part of Imperva's Cloud Application Security solution stack, the deployment of Client-Side Protection is safe, simple and fast. Once onboarded, detection starts in minutes, and websites receive all the benefits of extra client-side security with no additional latency. More importantly, because it requires no code changes, it won't break your website.

Comply with data security standards

Client-side attacks are as severe of a data breach as stealing data directly from the server. This is why a script management solution such as Client-Side Protection is now recommended by PCI DSS and is essential for complying with other data-security standards and regulations such as GDPR, CCPA and others. Client-Side Protection acts as a script management solution that provides security teams with full visibility, insights and control over all JavaScript embedded on their websites, reducing the risk of them being sensitive customer data being exfiltrated through compromised Javascript.

IMPERVA WEB APPLICATION & API PROTECTION (WAAP)

Clint-Side Protection is a key component of Imperva's Web Application & API Protection (WAAP), which reduces risk while provideing an optimal user experience. Our solutions safeguard applications on-premises and in the cloud with:

- Web application firewall (WAF)
- API Security
- Distributed Denial of Service (DDoS) protection
- Advanced Bot Protection
- Account Takeover Protection
- Runtime Application Self Protection (RASP)
- Actionable security insights
- Security-enabled application Delivery

Learn more about Imperva Application Security
at +1.866.926.4678 or online at
imperva.com

Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.