DATASHEET

Instart Web Security

Comprehensive protection for your website

Instart provides carrier-grade security for your website powered by intelligent features and a unique on-client presence, with easy management and low cost of ownership.

Web security overview

The security capabilities of Instart DX Cloud are designed to protect your website from large and small scale attacks, fraud, bot attacks, and other vulnerabilities. We process, inspect, and control all application traffic in our cloud, to prevent direct access to your application servers, monitor and manage all bot traffic, and prevent large scale DDoS attacks. Our platform maintains SOC 2 Type II certification, PCI certification and healthcare industry compliance standards.

Web application firewall

Our web application firewall (WAF) is built from the ground up to protect your applications from large scale, sophisticated attacks. We deploy a combination of industry best practice rules, anomaly scoring, and our proprietary ruleset to protect against everything from typical OWASP top 10 vulnerabilities to much more sophisticated attacks. As a major global cloud-based system, Instart learns from novel attacks directed at individual customers and uses these learnings to automatically protect all of our customers. Our WAF also supports virtual patching and custom rule creation, allowing full customization for every organization. Both encrypted and unencrypted traffic can be inspected and controlled to give you complete protection for all of your cloud, web and mobile applications.

DDoS protection

Our cloud infrastructure automatically scales on-demand to prevent most DDoS attacks from ever interrupting your service. Additionally, since our platform inspects and controls all of your application traffic, we can prevent invalid HTTP requests from making it through to your servers. For ultra large, targeted attacks we can route traffic through scrubbing centers where malicious traffic will be identified and dropped, and only valid user requests will be permitted through to your applications. Our DDoS protection is fully customizable, with full-time or on-demand scrubbing deployments available, allowing every organization to address their DDOS protection needs.

Bot protection

Instart offers a unique approach to bot protection: We deploy a small, JavaScript-based container that is transparently injected into the browser of every visitor, providing full control of all application and browser resources. With this virtualization layer, we are able to develop a deep fingerprint of malicious bot activity such as devices lying about their identity - like Headless Chrome claiming to be Firefox, verify correct script behavior - browsers requesting scripts but not executing them, verify user behavior matches device - correlate touch or mouse input events to device information, and much more. With this fingerprinting, we are able to block sophisticated attacks like botnets attempting credit card and gift card fraud, credential stuffing attacks, and fraudulent reservation holding. We also provide robust policy management capabilities that give you precise control as to whether to allow, throttle or based on each heuristic the system detects.

Client-side data protection

Protect sensitive customer data stored or entered on the browser with browser-level access controls to protect form fields and cookies from unauthorized third-party access. Instart sits between the browser and your website, intercepting all API traffic of third-parties trying to access form fields or cookies, and block or grants access as specified.

Benefits

Comprehensive – End-to-end protection from the browser to your servers

Robust – Protection against the most sophisticated attacks

Enterprise-grade – Trusted partner in securing your website

Effortless – Seamless integration with existing tools and workflows

Unified administration and SIEM integration

Implementing and maintaining a strong security posture with Instart is simple from our unified, web-based administrative portal. Security teams can create and manage new policies easily with changes being propagated globally within minutes. From our built-in security and WAF dashboards, teams can monitor and update individual rules, investigate incidents and react to attacks in real time. Instart can also stream log and event data directly to your on-premise or cloud-based SIEM tools.

Reliable and secure

The Instart platform is one of the largest and most reliable globally distributed cloud services in the world, processing more than 60 billion transactions and serving more than 250 million consumers per day. Our cloud runs in premier peering centers around the world, interconnected with all major carriers and cloud service providers, and we maintain SSAE-16 SOC 2 Type II certification, Payment Card Industry (PCI) certification, General Data Protection Regulation (GDPR) and healthcare industry compliance standards. When needed, our dedicated support engineers are available 24/7/365 and are always a single phone call away, with a 30-minute maximum response service level agreement for urgent issues.

Features

Worldwide hybrid cloud platform

DX Cloud is built on a globally distributed cloud platform that processes more than 12 billion transactions per day and inspects over 10,000 requests per second - and has massive and redundant capacity to absorb and mitigate denial of service attacks for our customers.

Client presence

A unique client-cloud architecture provides exceptional detection and control capabilities that complement network and cloud-based controls.

Web application firewall

Our low latency WAF can inspect, process and control all application traffic - blocking all suspicious, malicious or otherwise suspect activity with very little added overhead.

DDoS protection

The platform automatically scales to protect from the largest DDoS attacks, and only allows valid HTTP traffic to your origin. On-demand and full-time scrubbing services are available.

Bot protection

Unique bot detection capabilities that enable you to allow, block, and throttle sophisticated bot attacks.

Browser data access control

Prevent unauthorized third-party services from accessing form fields and cookies containing sensitive user data.

Managed security service

Dedicated, proactive security resources available to discuss your security posture, tune and create security rules, monitor for traffic spikes and other anomalies or activity of concern.

Closed loop attack response

Drill down to specific attack details and then easily build custom security rules to block attacks all from within one screen.

Virtual patches

Virtual patching is available to help protect against any known vulnerabilities existing in your website or application, enabling your security team to deploy the exact protections needed.

REST APIs

Management and control of your security services through our REST APIs, integrating easily into existing workflows.

Dashboards and analytics

Manage WAF and Security events from within our platform, with the ability to drill down based on specific event characteristics such as location, IP address or user agent. Export all logs to 3rd-party tools via automatic delivery or manual CSV export.

About Instart

Instart helps thousands of leading brands around the world deliver amazing web experiences through continuous insights and AI driven optimizations. Visit us at www.instart.com for more information.

INSTART