PARTNER BRIEF

Cloudflare and IONIX

IONIX maps your web attack surface and assesses Cloudflare WAF coverage to identify exploitable risks, not just vulnerabilities.

Customer challenge

As enterprises expand across cloud environments and digital ecosystems, their external attack surface becomes increasingly fragmented and difficult to secure. Security teams struggle to maintain continuous visibility of internet-facing assets and third-party exposures, while trying to distinguish meaningful risk from background noise. Manual processes and siloed tools delay response, and critical misconfigurations—like exploitable DNS or exposed infrastructure—often go undetected until it’s too late. Without unified insight or automated defense, organizations are left reactive, vulnerable, and blind to the threats targeting their most exposed assets.

What IONIX does

IONIX delivers continuous, external exposure management that goes beyond surface-level discovery. It actively maps your complete internet-facing footprint—including shadow IT and third-party dependencies—and determines which exposures are truly exploitable. IONIX simulates attack paths, detects misconfigurations, and provides prioritized remediation guidance. It ensures that your digital risk is understood in the full context of your security controls.

What Cloudflare does

Cloudflare provides advanced web application protection through its globally distributed Web Application Firewall (WAF). Sitting at the edge of the network, Cloudflare inspects every request in real time, blocking malicious traffic before it reaches your infrastructure.

Its WAF defends against OWASP Top 10 threats, zero-day exploits, bots, and more—leveraging threat intelligence from millions of internet properties. With customizable rules, instant updates, and seamless integration with DDoS, API, and bot protection, Cloudflare ensures consistent, low-latency defense across all web assets.

Better together: Unified visibility and risk assessment

Together, Cloudflare and IONIX empower security teams with complete visibility into their web exposure—ensuring that every internet-facing asset is both discovered and properly protected. Cloudflare provides real-time web application defense at the edge, while IONIX continuously verifies that coverage is in place and effective, even across shadow IT and third-party-managed assets. IONIX correlates security findings with Cloudflare’s WAF configuration and enforcement, providing a holistic risk assessment that reflects not just the presence of vulnerabilities, but their true exploitability in the context of existing defenses. IONIX also identifies exposed assets that are not currently protected by the Cloudflare WAF but should be, allowing security teams to ensure compliance with security policy. This integration eliminates blind spots, reduces alert fatigue, and enables smarter, faster prioritization of what truly matters.

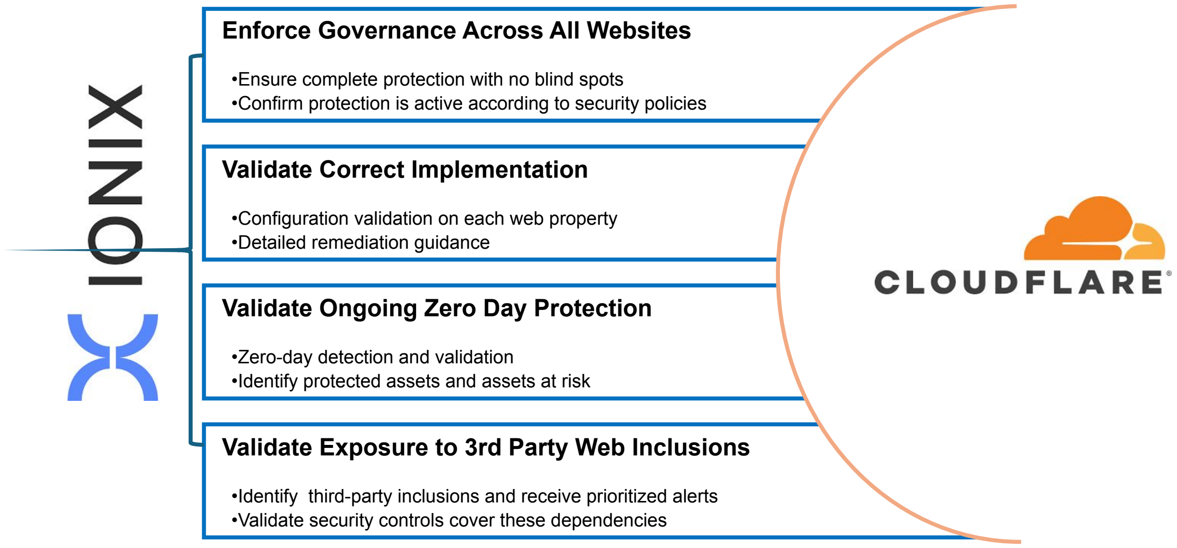
Cloudflare and IONIX

IONIX maps your web attack surface and validates Cloudflare WAF coverage to highlight exploitable risks, not just vulnerabilities.

Customer outcomes

- **Extend Cloudflare protection across all web properties:** Ensure complete protection with no blind spots. IONIX continuously discovers and monitors your complete web footprint, including shadow IT and forgotten domains, to confirm Cloudflare protection is active everywhere it's required according to the organization’s security policies. Identify unprotected assets automatically and receive alerts when new web properties are deployed without Cloudflare protection.
- **Validate correct implementation of Cloudflare:** Configuration errors can leave you vulnerable despite having Cloudflare protection in place. IONIX validates that Cloudflare is correctly configured on each of your web properties, ensuring WAF rules, SSL settings, direct origin access and security policies are properly implemented. Detect misconfigurations immediately and receive detailed guidance for remediation before attackers can exploit them.
- **Validate ongoing zero day protection:** When new zero-day threats emerge, rapid response is critical. IONIX automatically validates that your Cloudflare protection effectively shields you against emerging threats in real-time. Receive immediate alerts that confirm which assets are protected and which require additional attention.
- **Secure third-party web dependencies:** Third-party scripts and services often introduce invisible risk. IONIX identifies and monitors all third-party elements on your Cloudflare-protected websites, validating that your security controls extend to these dependencies. Detect supply chain risks and receive prioritized alerts when third-party inclusions introduce new attack vectors.

Together, Cloudflare and IONIX provide comprehensive web protection with continuous exposure validation, enabling security teams to accurately assess risk, enforce policies with confidence, and maintain complete visibility across all internet-facing assets.



Enforce Governance Across All Websites

•Ensure complete protection with no blind spots
•Confirm protection is active according to security policies

Validate Correct Implementation

•Configuration validation on each web property
•Detailed remediation guidance

Validate Ongoing Zero Day Protection

•Zero-day detection and validation
•Identify protected assets and assets at risk

Validate Exposure to 3rd Party Web Inclusions

•Identify third-party inclusions and receive prioritized alerts
•Validate security controls cover these dependencies