SecurityScorecard

DATA SHEET

Internet Intelligence API

Unrivaled Global Telemetry for Proactive Defense and Threat Hunting

The Security Scorecard Internet Intelligence API is a massive-scale infrastructure intelligence engine designed for the world's most advanced security teams. By integrating the high-fidelity scanning technology with Security Scorecard's industry-leading attribution, we provide the raw telemetry required to identify, hunt, and remediate threats across the entire global attack surface.

The Data Quality Differentiators

Port-Agnostic Capture

Standard scanners only look where it's easy. We look where it's hidden. Our bespoke protocol discovery algorithms are port-agnostic, meaning we identify services (Web, SSH, Database, C2) based on their protocol behavior, not their port number. Whether a service is on port 80 or port 31337, we see it, identify it, and index it.

Advanced Infrastructure Fingerprinting

We go beyond simple banners to analyze the fundamental netcode of the internet. Our API provides unique, persistent identifiers that link infrastructure across the IPv4 and IPv6 space.

- **JARM Fingerprints:** A signature of the server's TLS stack. Use JARM to find default malware C2 configurations (e.g., Cobalt Strike, Trickbot) regardless of the host or IP.
- **JA4TScan Fingerprints:** A signature of the server's TCP netcode. Identify the underlying OS and device type even when banners are stripped. Detect proxies, VPNs, and load balancers with ease.
- **Favicon Hashing:** Trace phishing kits and mirrored fraudulent infrastructure by searching for unique application-layer visual icons.

Proprietary Passive Intelligence

Our API is enriched by one of the largest passive data collection networks on the planet.

Global Sinkhole

2 billion+ malware requests daily from 14 million infected IPs. Identify compromises in your supply chain without ever deploying a sensor.

Global Honeypot Network

Real-time logging of active scanners and exploit attempts from cybercrime hotspots, providing high-confidence malicious IP reputation.

Dark Web & Leaks

Access to 7 billion+ leaked credentials and PII records sourced from 600+ normalized data files found on hacker forums.

Capability	Security Scorecard Internet Intelligence API	Other CTI
Discovery Speed	Full sweep every 7-10 days	Often 15+ days or variable
Port Coverage	3,500+ ports + Port-Agnostic	Limited standard ports or slow all-port sweeps
Attribution	Mapped to 11M+ Rated Organizations	Primarily technical/ASN only
Shadow IT Discovery	Deep Domain/Cloud linkage	Limited to known ranges
Fingerprinting	Pervasive JARM & JA4TScan	Limited or manual implementation required

Internet Intelligence Use Cases

Threat Hunting

Pivot from a single malicious IP to find an attacker's entire global infrastructure using JARM hashes and SSH keys.

Attack Surface Management

Discover exposed RDP, database, or admin panels on non-standard ports that standard scanners miss.

Third-Party Risk

Evaluate the true security posture of vendors by seeing their total internet exposure, including forgotten cloud assets.

Phishing Detection

Search for your company's favicon hash globally to identify unauthorized look-alike domains before they are used in a campaign.