CrowdStrike Store

IPQUALITYSCORE
PROACTIVELY PREVENT FRAUD

CROWDSTRIKE

Data Sheet

IPQUALITYSCORE (IPQS): ENTERPRISE THREAT ENRICHMENT

Elevate protection with enriched threat intelligence for domains, URLs and IP addresses

CHALLENGES

Increasingly complex cyber threats are a nuisance for any business with a strong online presence. Filtering noise from legitimate customers and potentially suspicious behavior can make it difficult to accurately identify true threats. In addition, many current solutions are unable to detect sophisticated and fraudulent threats because of a lack of contextual insights into bad actors, making it harder to minimize false positives and focus the security operations center (SOC) team's efforts on critical tasks. To effectively prevent fraud, organizations need rich context for all threats in their environment at speed.

SOLUTION

With CrowdStrike and IPQualityScore (IPQS), you can confidently identify bad actors to prevent fraud, using industry-leading threat intelligence and insight into IP address, domain and URL reputation to minimize friction and speed up your SOC team's response. IPQS enables your team to act with accuracy by enriching threat context surrounding detections within the CrowdStrike Falcon® platform. By gaining rich threat insights into complex cyberattacks — including malware, phishing, account takeover, credential stuffing, bots and much more — all within a single console, you can more easily identify and stay ahead of sophisticated threat actors committing fraud or abuse. The expansive IPQS threat network provides you with immediate insights into online bad actors, including abuse reports for hijacked devices, stolen credentials, botnets and abusive users.

Accurately identify sophisticated threats with Fraud Fusion™, the IPQS community blocklist program that enterprises and Fortune 500 companies feed data into when they detect suspicious behavior online. You can also empower your team with improved context through Abuse Shield™, which collects data from over 10,000 proprietary honeypots in the IPQS threat network to detect abusive proxies, VPNs, residential botnets and similar abusive or compromised IP addresses. Within the Falcon platform, you can gain better insight with IPQS context enrichment to identify phishing, malware and suspicious links, even for complex attacks. You can also leverage zero-day detection algorithms that are built with machine learning to identify known patterns of malicious behavior across any industry or audience, allowing you to gain full security coverage for elusive threats.

KEY BENEFITS

Get zero-day protection: Safeguard your organization from phishing and malware domains and URLs.

Eliminate blind spots: Prevent bot attacks, account takeover, credential stuffing, fake accounts and similar high-risk behavior with deep insight into IP address reputation.

Gain full visibility: Identify attacks from sophisticated botnets and residential proxies.

Find true threats: Benefit from worldwide coverage and intelligent blocklists that prevent false-positives.

BUSINESS VALUE

Use Case/Challenge	Solution	Benefits
Many traditional solutions cannot detect sophisticated threats.	Access the most advanced threat feeds with on-demand lookups within the Falcon platform for IP address reputation, and domain or URL risk.	Easily identify complex threats alongside Falcon detections that traditional vendors may misclassify. Increase your confidence in decision making for blocking threats and suspicious behavior.
False positives cause SOCs to focus on the wrong targets.	Get the right context for your unique needs with 50+ customizable settings that can be tailored to your use case.	Use the freshest data to avoid misclassifying legitimate users. IPQS uses a very short lookback period for reputation checks to avoid false positives based on old data.
Teams are hindered by limited coverage for international audiences and certain industries.	The proprietary IPQS honeypot network consists of 10,000+ websites that attract fraudsters from every global region.	Seamlessly access industry-leading data in any region for the best insight into bad actors and suspicious behavior — without leaving the Falcon console.

"IPQS's accuracy is impressive. It's never been easier for our security team to identify high-risk threats and differentiate between legitimate behavior."

— Cyberthreat Analyst, Leading Fortune 500 company

TECHNICAL SOLUTION

The IPQS context enrichment integration with the Falcon platform enriches IP addresses, domains and URLs with deep reputation analysis for enterprise threat detection. Accurately identify advanced bad actors and complex attacks even when cybercriminals are using new tactics, residential botnets and sophisticated behavior to mask their online signature. Quickly classify advanced threats and enrich network data with the best threat intelligence across any region or industry. Empower your security team to free up resources and more efficiently detect threats without impacting the user experience. IPQS and CrowdStrike also allow you to scan URLs and domains to detect malware and phishing links, identify parked domains, track compromised servers, monitor suspicious URLs and detect disposable email domains.

IPQUALITYSCORE (IPQS): ENTERPRISE THREAT ENRICHMENT

KEY CAPABILITIES

- **Advanced machine learning threat detection:** Quickly identify complex threats from sophisticated bad actors, even when other vendors are unable to classify the threat.
- **Over 50 customizable settings:** Tailor CrowdStrike threat detection algorithms for your exact audience and use case.
- **Fresh data:** Access the freshest data across any industry, as IPQS receives over 10,000 abuse reports per minute.
- **99.99% uptime:** Experience reliable infrastructure for on-demand lookups at any time.

Try out IPQS in the CrowdStrike Store.

ABOUT IPQUALITYSCORE

IPQualityScore (IPQS) is a leading provider of enterprise-grade IP address reputation, threat intelligence and fraud prevention data. Our mission is to provide the cybersecurity and business community with the best tools to accurately identify sophisticated threats including botnets, zero day malware and phishing, credential stuffing, account takeover (ATO), fake users, fraudulent payments and much more. With over 10 years of technology expertise, IPQS can deliver industry best detection rates and minimize friction from false-positives for any industry or audience. For more information, please visit **https://www.ipqualityscore.com**.

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more:
https://www.crowdstrike.com/

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today:
https://www.crowdstrike.com/free-trial-guide/

Start Free Trial
of Next-Gen AV

Learn more **www.crowdstrike.com**