CROWDSTRIKE

CrowdStrike Products

Data Sheet

CrowdStrike QuickScan Pro

Get lightning-fast threat detection with rapid, scalable file scanning

Speed, scale and savings in malware detection

Organizations today face the challenge of analyzing millions of externally uploaded files each year for potential threats. Traditional malware analysis tools are either too slow, too costly or ineffective when it comes to detecting novel threats or overcoming anti-analysis techniques. CrowdStrike® QuickScan Pro addresses these issues by offering a fast, scalable and cost-effective approach to malware analysis, integrating both static and dynamic techniques powered by industry-leading threat intelligence.

Key capabilities

Improve efficacy and time-to-respond

- **Rapid Threat Detection:** QuickScan Pro delivers threat verdicts in seconds, significantly faster than traditional sandbox technologies, which can take over 10 minutes per file. This speed enables faster incident response and minimizes operational disruptions.
- **Scalability:** Designed to handle large volumes of file uploads, QuickScan Pro is ideal for organizations processing millions of external files annually. Its ability to process files up to 256MB makes it suitable for a wide range of use cases, from email scanning to website file validation.
- **Comprehensive Malware Detection:** QuickScan Pro integrates multiple advanced technologies — including allowlist/denylist checks, YARA rules, machine learning and unpacking techniques — to detect both known and novel threats. It also includes a lightweight detonation environment for in-depth behavior analysis when necessary.
- **Clear, Actionable Insights:** Each threat verdict is accompanied by a detailed "Verdict Reason" and "Verdict Source," providing analysts with the context they need to make informed decisions quickly and confidently.

Key benefits

- Delivers threat verdicts in seconds, enabling faster triage and incident response
- Efficiently handles millions of files across diverse use cases
- Minimizes sandbox reliance, reducing operational costs significantly
- Easily integrates with SIEM and SOAR workflows for automation

Unlock greater security efficiency and cost savings

- **Improved Efficiency:** By triaging files quickly, QuickScan Pro reduces the volume of files sent to more resource-intensive sandbox environments. This not only streamlines workflows for security teams but also lowers associated costs.
- **Cost-Effective:** By reserving expensive sandbox analysis for only the most suspicious files, organizations can achieve significant cost savings while maintaining a high level of security. QuickScan Pro's static and dynamic analysis methods provide a comprehensive solution without the high costs of traditional tools.
- **Seamless Integration:** QuickScan Pro easily integrates into existing SIEM and SOAR workflows, enabling security teams to automate and prioritize threat response actions. Its API allows for smooth integration into email systems and other internal processes.

"We need to scan large email attachments including ZIP archives with 500+ files, and analyze each for maliciousness. I believe CrowdStrike QuickScan Pro is the answer."

Global Financial Institution

Popular use cases

Customers can integrate QuickScan Pro via its API for rapid file analysis, providing actionable insights within seconds without disrupting operations. Key use cases include:

- **Email Scanning:** Automate incoming email scans for quick verdicts and quarantine actions, as used by a global financial institution for malware and phishing protection.
- **File Validation for Website Upload/Download:** Support safe file uploads/downloads with real-time scanning and verdicts to maintain a seamless user experience.
- **Optimizing SIEM/SOAR Workflows:** Automate triage, verdicts and context to prioritize incident response, helping SOC teams eliminate false positives and focus on real threats.

About CrowdStrike

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

Powered by the CrowdStrike Security Cloud and world-class AI, 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 delivers 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/

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

Request a Demo