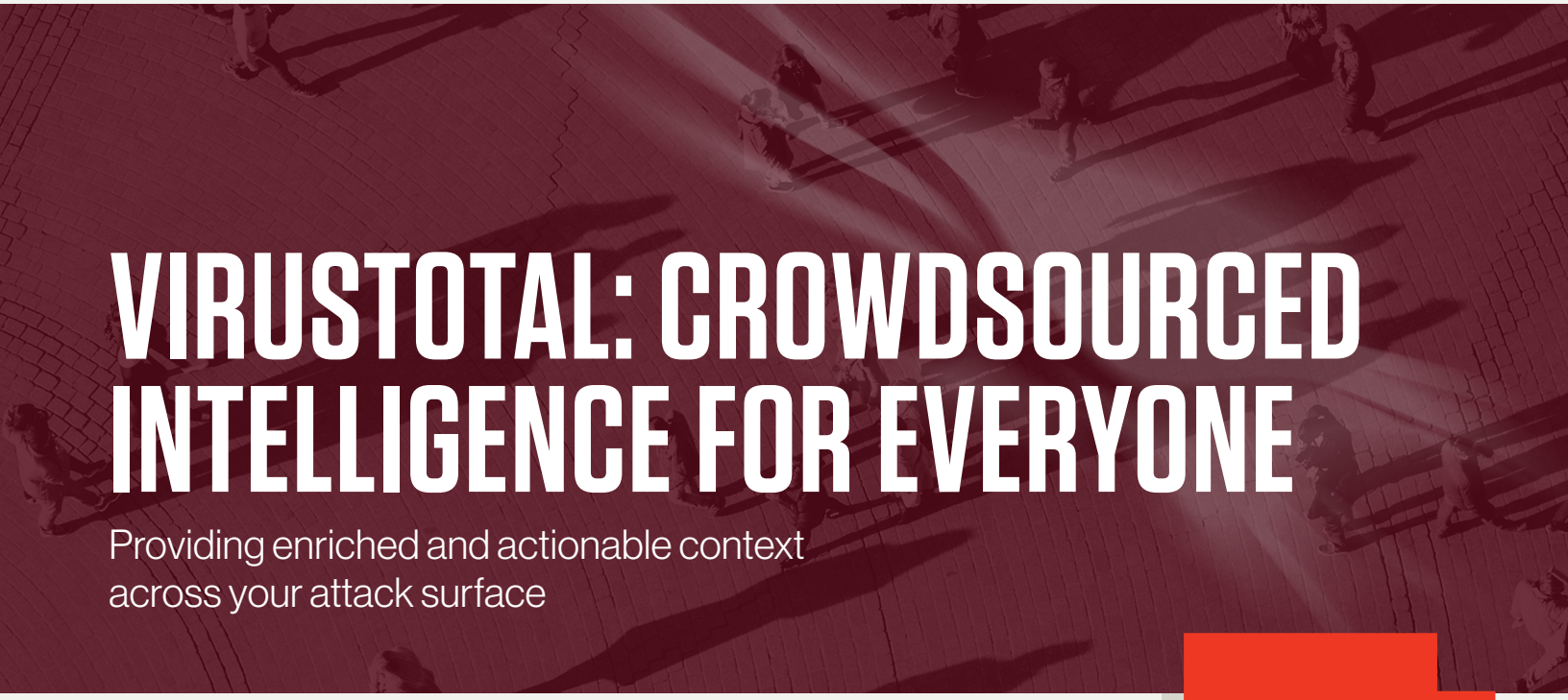
CrowdStrike Store

VIRUSTOTAL

CROWDSTRIKE



VIRUSTOTAL: CROWDSOURCED INTELLIGENCE FOR EVERYONE

Providing enriched and actionable context across your attack surface

CHALLENGES

As attack surfaces grow and security teams struggle to retain talent, analysts are plagued with alert fatigue, work overload and a lack of funding — all of which can diminish the quality and speed of incident response, potentially leading to missed threats or costly breaches. In addition, security teams are challenged to work within budget constraints to optimize their existing investments and derive more immediate value. To protect your organization, your team needs to focus on collecting the right intelligence with speed so you can respond accurately and efficiently.

SOLUTION

VirusTotal integrates with the CrowdStrike Falcon® platform to provide the needed context around any suspicious activity to help accelerate threat detection and response. Get the actionable data you need for any observable, and use it to quickly pivot and find related artifacts and indicators.

VirusTotal is a rich, interlinked and close-to-real-time crowdsourced malware corpus. By including security data coming in from over 70 security vendors, crowdsourced YARA rules, sandboxed dynamic analysis, Sigma rules acting on detonation behavior, IDS detections on network traffic, and a myriad of other security tools and datasets, your team is empowered with a unique multi-angular approach to automate alert triage and false positive remediation. Get rich and relevant contextual threat information for any suspicious indicator to expedite your incident response. You can also empower your analysts to unearth threats unknown to the industry and add unmatched context to boost your security stack. Track adversaries and implement proactive defenses to eliminate blind spots in your organization so you can get more from your existing investments.

KEY BENEFITS

Automate alert triage and false positive remediation

Expedite and augment incident response

Discover unknown threats and take preventive measures

Track adversaries and implement proactive defenses

VIRUSTOTAL: CROWDSOURCED INTELLIGENCE FOR EVERYONE

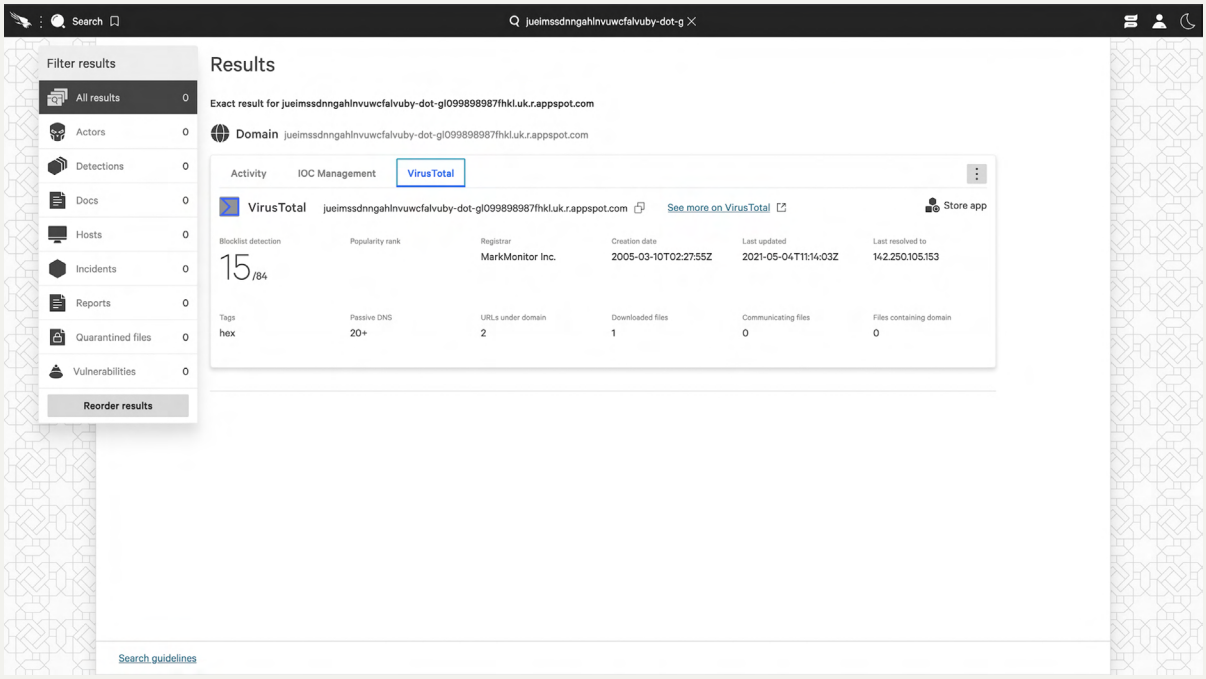
BUSINESS VALUE

Use Case / Challenges	Solution	Benefits
Automate alert triage and false positive remediation	Leverage API and SIEM/SOAR integrations to confirm, prioritize or discard alerts.	Increase accuracy and reduce alert fatigue by pulling in security data from over 70 security vendors.
Expedite and augment incident response	Explore VirusTotal's threat graph to understand the full attack chain and map out threat campaigns.	Instantly pivot to related infrastructure, and identify indicators of compromise (IOCs) to feed your SIEM and network perimeter defenses.
Discover unknown threats, and take preventative measures	Deploy generic hunting YARA rules, and use anomalous pattern searches to surface malware.	Eliminate blind spots with automatic IOC feeds derived from dynamic campaign monitoring.
Track adversaries, and implement proactive defenses	Understand the global threat landscape, monitor specific actors targeting your industry and make data-driven infrastructure hardening decisions.	Profile adversaries, conduct proactive TTP-based hunts and automatically generate detection rules for deployment in your EDR.

VirusTotal provides the context, telemetry and crowdsourced intelligence you need to properly respond to any threat.

TECHNICAL SOLUTION

VirusTotal integrates into the Falcon platform to provide the most relevant and rich contextual information for any suspicious indicators across endpoint telemetry. The data provided includes antivirus detection ratio; threat label and category; submission uniqueness; number of submitters; crowdsourced YARA matches; and other valuable details. Get the actionable data you need for any observable, and use it to quickly pivot to the VirusTotal website to find related artifacts and indicators to help enrich incident response workflows.



VIRUSTOTAL: CROWDSOURCED INTELLIGENCE FOR EVERYONE

KEY CAPABILITIES

- **Threat Insights:** Get rich and relevant contextual threat information for any suspicious indicator.
- **Actionable Data:** Obtain antivirus detection ratios, crowdsourced YARA matches and submission details.
- **Accelerated Response:** Use data point to one-click into VirusTotal for related artifacts and indicators.
- **Blind Spot Elimination:** Profile adversaries, conduct proactive TTP-based hunts to automatically generate detection rules.

ABOUT VIRUSTOTAL

VirusTotal is the world's richest, most interlinked and closest to real-time crowdsourced malware corpus. By applying Google's planet-scale infrastructure and instant search capabilities, as well as VirusTotal home-grown innovations such as YARA, we have built the most actionable threat intelligence suite on the planet. To the extent that it has become a necessary layer in any defense-in-depth security strategy, the "Google" of malware. G2K companies and the largest governments on Earth use it every day to shed light into their security telemetry, unearth compromises and outsmart their adversaries.

Learn more: **www.virustotal.com**

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 5 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Start Free Trial
of Next-Gen AV

Learn more **www.crowdstrike.com**