JOINT PARTNER SOLUTION BRIEF

CrowdStrike Partner Solution Brief

While defense-in-depth strategies can make a difference, today's enterprise IT is dynamic with often rapidly shifting perimeters. The interconnected nature of applications, devices, users and data across multiple environments—the relationships and dependencies—that drive a digital enterprise, create the potential for many exploitation paths internally and externally, leading to an increased attack surface that is vulnerable to a multitude of attacks including malware and ransomware.

The Challenge

The threat of malware attacks has been rising for many years. According to DataProt, there are more than 1 billion malware programs out there, with 560,000 new pieces detected every day, and ransomware attacks targeting corporations increased 20% from 2019 to 2020. The threat comes with a steep cost to enterprises. NetDiligence estimates that ransomware costs on average $559,000 per incident and up in 2020, a 40% increase from 2019.

The key to protecting the digital enterprise from malware and ransomware is to manage the security policies through understanding the relationships and dependencies between the users and assets. The end-to-end visibility is required to provide insight for action that extends from endpoint to cloud and datacenter.

The Solution

vArmour Relationship Cloud integrates with CrowdStrike Falcon Data Replicator (FDR) through a standard connector framework to collect and process workload telemetry from CrowdStrike. Through this integration, enterprises can visualize the applications and their relationships in ways that are meaningful to the business. The new connector lets enterprises see the baselined behavior to create application-centric security decisions, which can be further enhanced by the CrowdStrike Falcon platform.

Together, the integration allows customers to construct consistent cybersecurity controls, through observing and managing application relationships and dependencies. The end-to-end visibility reveals gaps and vulnerabilities to the entire IT landscape, giving enterprises the transparency and insight to take actions against threats.

Joint Value of Partnership

Together, the partnership of vArmour and CrowdStrike allows customers to enact consistent cybersecurity policies to reduce attack surface and protect the IT infrastructure, through observing and managing application relationships and dependencies.

The end-to-end visibility reveals gaps and vulnerabilities to the entire IT landscape, giving enterprises the transparency and insight to take actions against threats.

From toxic relationships, unsanctioned applications, policy assurance gaps, IT & cyber resiliency improvements, customers gain continuous operational efficiencies, risk and compliance, providing massive financial savings and accelerating security initiatives at the speed of digital transformation.

Key Benefits

- Reduce cyber risk through a better understood and protected attack surface, avoiding ransomware damage that costs on average $1.85M per incident in 2021.
- Improve resiliency by uncovering unknown dependencies that can cause unexpected service outages during planned changes, avoiding costly disruptions exceeding $300,000 per hour on average.
- Provide continuous regulatory assurance through monitoring and reporting of application environments and validation of controls, saving thousands of person hours and up to USD $10 million from the manual process.

Find out more about vArmour

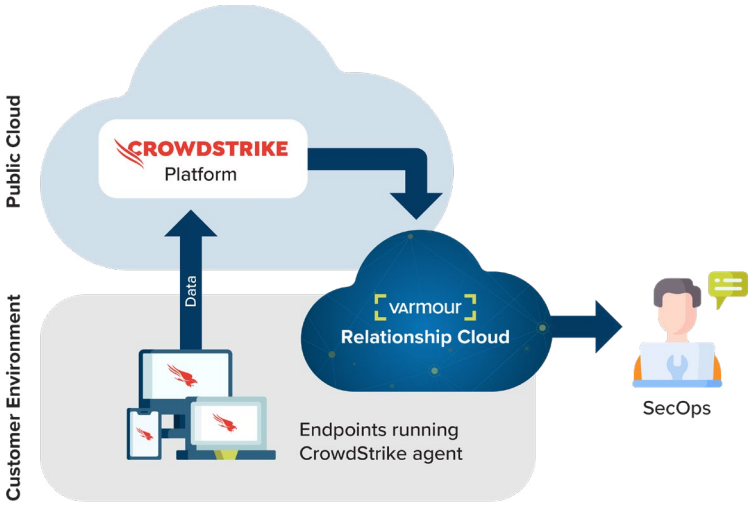

Figure: vArmour provides pervasive visibility using CrowdStrike telemetry

Benefits

The partnership of vArmour and CrowdStrike ensures enterprises can extend industry-leading endpoint protection across their complex hybrid IT environments to prevent breaches caused by malware and ransomware. The integration of vArmour with CrowdStrike helps enterprises:

- Reduce risks of breaches through a well-defined attack surface
- Extend consistent security controls across the environments and to endpoints
- Compute, simulate and enforce effective security policy faster based on baselined behavior
- Protect applications, workloads and data from unauthorized lateral movements or access

About CrowdStrike

CrowdStrike, 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. Learn more at www.CrowdStrike.com.

About vArmour

vArmour, the leader in application relationship management software, reduces cyber risk across the entire attack surface with its ability to discover, observe and control applications, infrastructure, users, devices, and data across an organization. vArmour reduces complexity and provides immediate time-to-value to reduce vulnerabilities like Ransomware, and accelerate initiatives like Zero Trust and Cloud Security. Enterprises around the world, including the world's largest banks, multinational telcos and Fortune 500 companies, trust vArmour to provide necessary visibility across their digital estate and strengthen their security posture. Learn more at www.vArmour.com.

650.564.5100 | info@varmour.com | 270 3rd Street, Los Altos, CA 94022