CrowdStrike Technology Partner

UiPath™

CROWDSTRIKE

Solution Brief

CROWDSTRIKE FALCON AND UiPATH INTEGRATION

Extend endpoint security to robotic process automation (RPA), enabling full visibility to enhance protection and speed of response

CHALLENGES

Robotic process automation (RPA) makes it easy to build, deploy and manage software “robots” that emulate human actions within your digital systems to improve business productivity at scale and speed. Because RPA requires access to systems and privileges to execute tasks, organizations’ workflows may be at increased risk of attack and exploitation if there isn’t a sufficiently fortified security posture.

Malicious actors can theoretically take advantage of RPA's human emulation by building automations that covertly perform unauthorized tasks or compromise authorized tasks that involve information processing — all without the robot’s awareness. For example, if anything malicious was embedded in a document subsequently opened by a robot, or a website was able to compromise via browser exploit the machine a robot is running on, a robot could be caught as unaware as a human user might be in the same situation.

Today, RPAs are being created without being fully integrated into existing security stacks, which means that many current security solutions are unable to track specific processes triggered by robots and differentiate between robot and human actions. This lack of visibility and security enforcement of RPA processes inhibits teams from hunting, investigating and remediating effectively. Organizations must stop attackers from bypassing defenses and compromising robots to prevent “silent failure" where threats go unnoticed for days or even months, spelling success for the attacker and potential disaster for the organization.

Organizations that use RPAs need greater visibility and better security enforcement of RPA processes to strengthen the security posture of their automations.

SOLUTION

CrowdStrike and UiPath have partnered to deliver a first-of-its-kind RPA and endpoint security solution that proactively addresses the RPA threat vector. The CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry to automatically detect attacker activity, whether initiated by humans or robots, and grants your security team real-time visibility across the environment. The integration with the UiPath Robotic Process Automation (RPA) platform allows your team to accurately identify and track the source of malicious activity to robots and specific RPA-driven processes, in addition to human-initiated activity, to proactively hunt, investigate and remediate threats.

KEY BENEFITS

Fortified protection: Gain unparalleled coverage to defend against all types of attacks — from malware to sophisticated and stealthy nation-state attacks — targeting both human and robotic processes.

Enhanced automation security: Prevent silent failure with full endpoint detection and response (EDR) that captures raw events, including those originating from RPA processes, to ensure automation is included for a strong security posture.

Complete visibility: Get deeper insight into your systems — specifically relevant robot actions — and leverage rich telemetry for improved attack context and faster investigation and response.

Increased efficiency: Connect contextual RPA details to endpoint events, streamlining hunting and investigation in a single console while accelerating granular, targeted response actions that ensure business continuity.

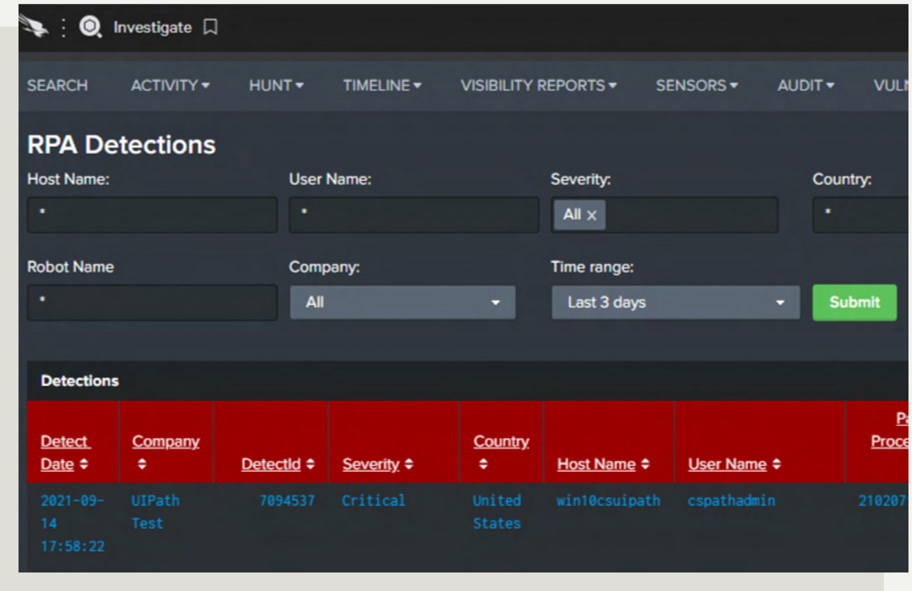
Because the Falcon platform treats robots and RPA-initiated processes like other software processes running on the endpoints, your security team gains an additional layer of protection and enhanced remediation actions. CrowdStrike's accurate and swift remediation actions, enabled from within its single console, allow your team to quarantine compromised hosts without impacting broader RPAs or hosts, ensuring business continuity in the event of an incident. With the Falcon platform and the UiPath RPA platform, you can ensure your organization is equipped with fortified protection and enhanced visibility for your dispersed RPA environment to thwart attackers before damage is done.

BUSINESS VALUE

Use Case/Challenge	Solution	Benefits
RPAs are created without being integrated with existing security stacks	With CrowdStrike's powerful endpoint capabilities within your UiPath environment, you can boost security enforcement and effectively detect and respond to malicious activity targeting robots and RPA processes — all within the Falcon platform.	■ Enhance your security posture with CrowdStrike's unparalleled detection and response capabilities ■ Avoid context switching and manage your RPA security within Falcon's single console
Current solutions lack the visibility to correlate events to originating RPA processes	CrowdStrike and UiPath provide rich, contextual telemetry of RPA processes, giving you an in-depth understanding of attacks and enabling you to identify and track the source of malicious activity for robots and RPA processes.	■ Eliminate blind spots with enriched end-to-end coverage for all RPA processes within your environment ■ Reduce time and effort to investigate and respond with proactive threat context
Advanced attackers are covert and can achieve "silent failure" by bypassing defenses and compromising robots	CrowdStrike's powerful EDR prevents silent failure by capturing raw events, including those originating from RPA processes, to ensure automation is included to strengthen your security posture.	■ Speed up detection with full EDR capabilities to catch elusive attackers ■ Accelerate response by quarantining compromised hosts without impacting broader RPAs or hosts

TECHNICAL SOLUTION

The Falcon platform and UiPath RPA platform integration leverages CrowdStrike Falcon Insight™ EDR capabilities to track and display both malicious and benign UiPath RPA activity. RPA information is used in connection with sensor events collected by Falcon, enabling analysts to identify RPA-driven processes. Falcon then automatically detects attacker activity, whether initiated by humans or robots, and grants your security team real-time visibility across the environment for proactive threat hunting, incident investigation and remediation. The CrowdStrike and UiPath integration works out of the box, with no configuration necessary for joint customers on v3.66+ of Falcon and 21.10+ of UiPath, and with no additional licensing fees required.



RPA Detections

Host Name: *

User Name: *

Severity: All ×

Country: *

Robot Name *

Company: All

Time range: Last 3 days

Detections

Detect Date ⬍	Company ⬍	DetectId ⬍	Severity ⬍	Country ⬍	Host Name ⬍	User Name ⬍	Pa Proce
2021-09-14 17:58:22	UIPath Test	7094537	Critical	United States	win10csuipath	cspathadmin	210207

KEY CAPABILITIES

- **Access intuitive dashboards:** Within the Falcon console's Investigate dashboard, new RPA-specific dashboards provide visibility into RPA activity.
- **See RPA involvement:** The Suspicious RPAs dashboard shows all CrowdStrike detections with associated RPA activity, giving analysts the insight they need to further investigate suspicious and malicious activity involving RPA.
- **Monitor activity:** The RPA Operations dashboard allows for general monitoring of RPA activity. Analysts can view RPA event count over time, top RPA processes and top applications invoked, and filter this data by host, RPA job ID and RPA process name.
- **Build custom queries:** For deeper hunting and investigation, analysts can write custom queries in event search.

UiPath is a trusted **CrowdStrike Technology Alliance Partner**, offering innovative integrated solutions based on CrowdStrike's rich open APIs, extending the Falcon platform with UiPath's RPA capabilities.

ABOUT UiPATH

UiPath has a vision to deliver the Fully Automated Enterprise™, one where companies use automation to unlock their greatest potential. UiPath offers an end-to-end platform for automation, combining the leading **Robotic Process Automation** (RPA) solution with a full suite of capabilities that enable every organization to rapidly scale digital business operations.

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (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.**

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

Start Free Trial
of Next-Gen AV

Learn more **www.crowdstrike.com**