servicenow.

CROWDSTRIKE

Solution Brief

CROWDSTRIKE AND SERVICENOW SECURITY INTEGRATION

Unify security and IT to accelerate threat and vulnerability prioritization, response and remediation

CHALLENGES

The ever-evolving threat landscape continues to be a challenge across every industry. Organizations are finding they do not have enough resources to keep up with threats, gain visibility into vulnerable applications and prioritize alerts fast enough. As the number of targeted attacks continues to rise, security teams have become overwhelmed with alerts and struggle to combine data from disparate sources to prioritize incident response efforts.

SOLUTION

The CrowdStrike and ServiceNow integration provides joint customers with streamlined security operations and accelerated identification, prioritization and remediation of threats and vulnerabilities. This enables security teams to quickly perform remediation tasks before an incident results in a breach.

BUSINESS VALUE

Use Case	Solution	Benefits
Expedite Incident Response	CrowdStrike and ServiceNow enable customers with both solutions to automate incident response workflows by sending endpoint event data from the Falcon platform into the Security Incident Response application of ServiceNow Security Operations for immediate identification and prioritization of critical incidents.	Simplify the creation and prioritization of security incidents for faster response, mitigation and remediation of critical events.
Enrich Incidents with Threat Intelligence	Joint customers can automatically send CrowdStrike indicators of compromise (IOCs) to the ServiceNow Threat Intelligence application, part of ServiceNow Security Operations, for reference and to provide context and enrichment when an IOC is connected to a security incident.	Automate IOC detection and correlation within security incidents to get actionable threat intelligence that quickly enables analysts to respond to attacks and threats.
Address Application Vulnerability	CrowdStrike Falcon Spotlight™ provides a scanless, near real-time, zero-impact assessment for endpoint vulnerabilities, with enhanced reporting and visualization. Its integration with ServiceNow's Vulnerability Response provides a risk score to prioritize based on classification.	Gain visibility into your security gaps and which ones are being targeted to improve response time, make better decisions faster and proactively protect against attacks.
Improve Device Hygiene/IT Management	Import endpoint device details into your ServiceNow CMDB for additional visibility and context, and to correlate endpoint ranking in one view.	Improve both security and IT operation outcomes by having access to meaningful asset data in order to get a comprehensive view of the attack surface and address perceived security gaps.

KEY BENEFITS

Automates security incident creation within ServiceNow® based on malicious endpoint event activity detected by the CrowdStrike Falcon® platform

Accelerates investigations within ServiceNow by bringing back all relevant endpoint event activity captured by CrowdStrike
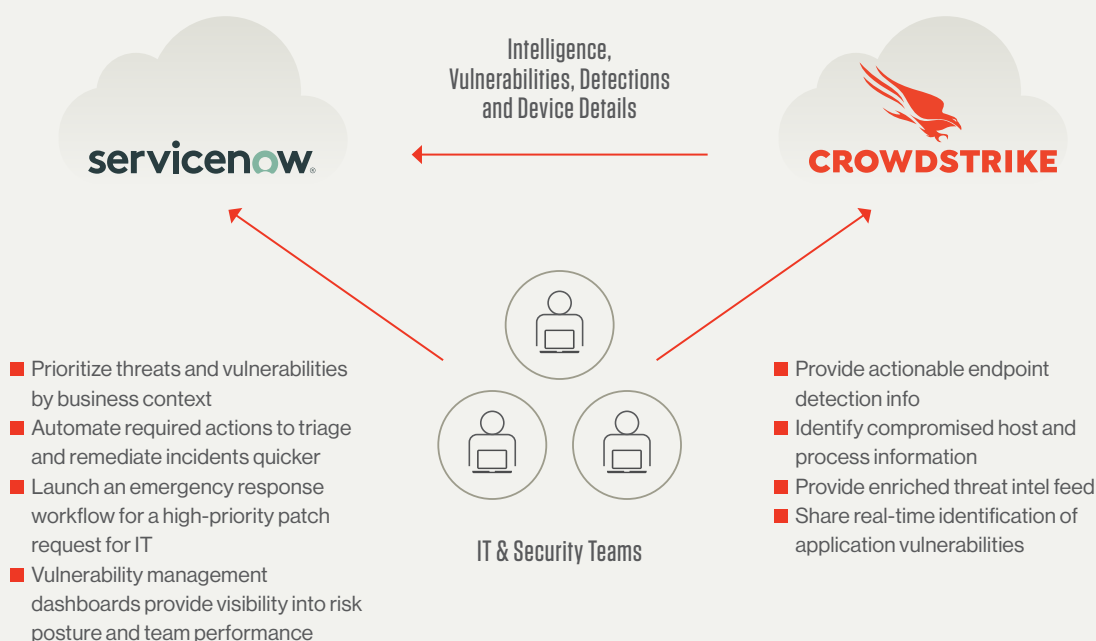
Accelerates threat prioritization and response with the ability to integrate device data from the Falcon platform into your incident response process using the ServiceNow® Configuration Management Database (CMDB) and Identification and Reconciliation Engine (IRE)

Enables faster remediation by security teams, minimizing downtime and impact from breaches

TECHNICAL SOLUTION

CrowdStrike Falcon on ServiceNow provides users with the ability to integrate alert and detection data from the Falcon platform into their security incident response process by automatically creating ServiceNow Security Incident Response incidents. Endpoint security events detected by CrowdStrike are sent to ServiceNow for centralized analysis, automated workflow and streamlined response. CrowdStrike's threat intelligence enriches ServiceNow security incidents to provide additional insight into the scope of the incident and attacker attribution. Investigations and remediation are accelerated within ServiceNow by integrating all relevant endpoint event activity captured by CrowdStrike.

Intelligence,
Vulnerabilities, Detections
and Device Details

servicenow.

CROWDSTRIKE

■ Prioritize threats and vulnerabilities by business context
■ Automate required actions to triage and remediate incidents quicker
■ Launch an emergency response workflow for a high-priority patch request for IT
■ Vulnerability management dashboards provide visibility into risk posture and team performance

IT & Security Teams

■ Provide actionable endpoint detection info
■ Identify compromised host and process information
■ Provide enriched threat intel feed
■ Share real-time identification of application vulnerabilities

KEY SOLUTION CAPABILITIES

1. Falcon X™ Intelligence feeds actionable insights about the top threat actors, attack vectors and threat intelligence trends to ServiceNow® Security Operations.

2. CrowdStrike Falcon combines next-generation antivirus, endpoint detection and response (EDR) and managed threat hunting to detect and prevent attacks, providing actionable real-time event data to ServiceNow for additional analysis and automated response.

3. Falcon Spotlight provides scanless, near real-time identification of endpoint vulnerabilities as well as verification of patched vulnerabilities with enhanced reporting and visualization.

4. The ServiceGraph Connector for CrowdStrike on ServiceNow provides users with the ability to integrate device data from the Falcon platform into their incident response process.

5. ServiceNow® Security Operations consumes the near real-time identification threat intelligence and endpoint event activity from CrowdStrike to automatically create security incidents in ServiceNow Security Incident Response. Additionally, ServiceNow Vulnerability Response's workflows, automation and deep IT integration and hygiene combine to speed response and remediation of critical vulnerabilities.

ABOUT SERVICENOW

ServiceNow (NYSE: NOW) is making the world of work, work better for people. Its cloud-based platform and solutions deliver digital workflows that create great experiences and unlock productivity for employees and the enterprise. Within ServiceNow Security Operations, ServiceNow offers two solutions: Security Incident Response and Vulnerability Response, designed to help security and IT teams to respond faster and more efficiently to incidents and vulnerabilities.

For more information, visit: **www.servicenow.com**.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), 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 3 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.

There's only one thing to remember about CrowdStrike: **We stop breaches.**

Learn more **www.crowdstrike.com**