Data Sheet

VULCAN CYBER: VULNERABILITY REMEDIATION ORCHESTRATION

Enforcing cyber hygiene, from scan to fix

CHALLENGES

Many vulnerabilities that are exploited by malicious actors are already known to security teams. A 2019 Ponemon Institute study noted that 60% of breaches exploited unmitigated and unremediated vulnerabilities where a patch was available but not applied, underscoring the need for organizations to do a better job of reducing their vulnerability exposure.

Unfortunately, the existing vulnerability management market has a “fix” problem — vulnerability management tooling notoriously falls short of delivering desired remediation outcomes. Most vulnerability management tools stop after simply scanning and prioritizing vulnerabilities, which is less than half of what is needed to protect your business from the ever-present threat of vulnerability exposure.

SOLUTION

Vulcan Cyber delivers the exact priorities, remedies, insights and automation security that IT teams need to fix vulnerabilities at scale. The Vulcan platform orchestrates and visualizes remediation campaigns from start to finish, helping teams quickly and efficiently fix what matters most.

Vulcan Cyber integrates with the CrowdStrike Falcon® endpoint protection solution across the vulnerability remediation lifecycle to automate vulnerability mitigation for enterprise endpoint infrastructure. Vulcan Cyber uses Falcon endpoint asset data and the vulnerability module to inform, identify and prioritize the work of remediation and mitigation. It turns complex remediation processes into simple step-by-step workflows, then automates all of the tedious work of mitigation by using Falcon endpoint security for real-time response at scale, with mitigating actions such as stop service and registry changes.

KEY BENEFITS

Reduce vulnerability risk with real-time mitigating actions

Protect the business while buying time for IT teams to deploy patches and permanent fixes

Rapidly mitigate difficult, zero-day, unique vulnerabilities

Get fixes done at scale with fully orchestrated and automated vulnerability mitigation

BUSINESS VALUE

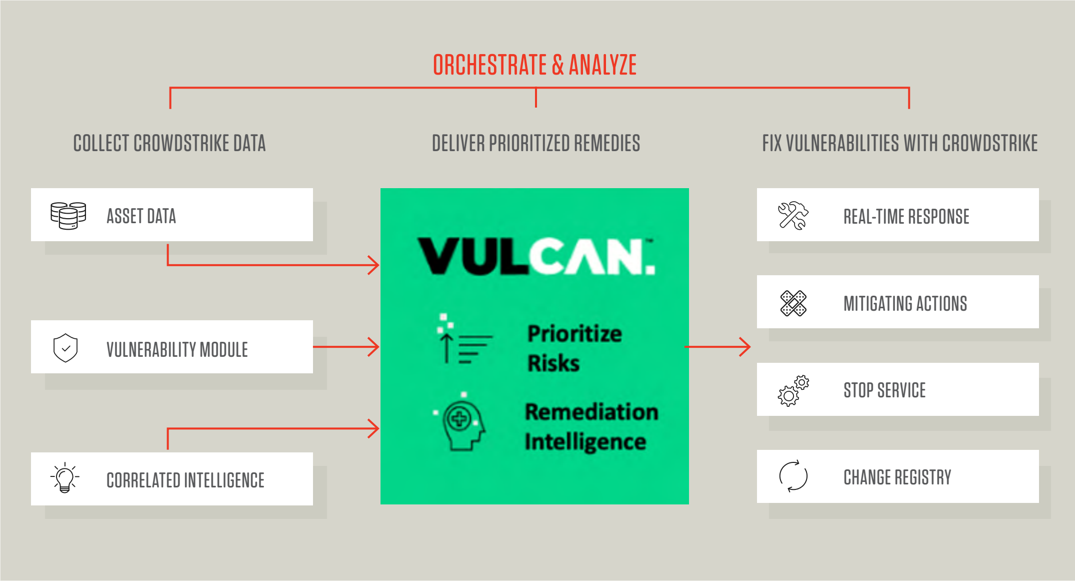
Use Case/Challenge	Solution	Benefits
Vulnerability identification and prioritization	Vulcan Cyber ingests endpoint asset and vulnerability data from Falcon and correlates it with threat severity and intelligence.	Endpoint vulnerabilities are prioritized by risk and criticality to your unique business, enabling efficient mitigation and remediation.
Remediation intelligence	Vulcan Cyber provides curated fixes and remedies in the form of Falcon mitigating actions integrated with IT service and collaboration platforms.	IT teams receive prioritized remediation tasks, with the specific mitigation intelligence needed to automate real-time response in Falcon.
Real-time response and automated endpoint protection	Vulcan Cyber passes prioritized mitigation actions to Falcon for automated endpoint control.	True endpoint protection through full-lifecycle, scan-to-fix vulnerability remediation is orchestrated, automated and measured through Vulcan Cyber and CrowdStrike Falcon.

TECHNICAL SOLUTION

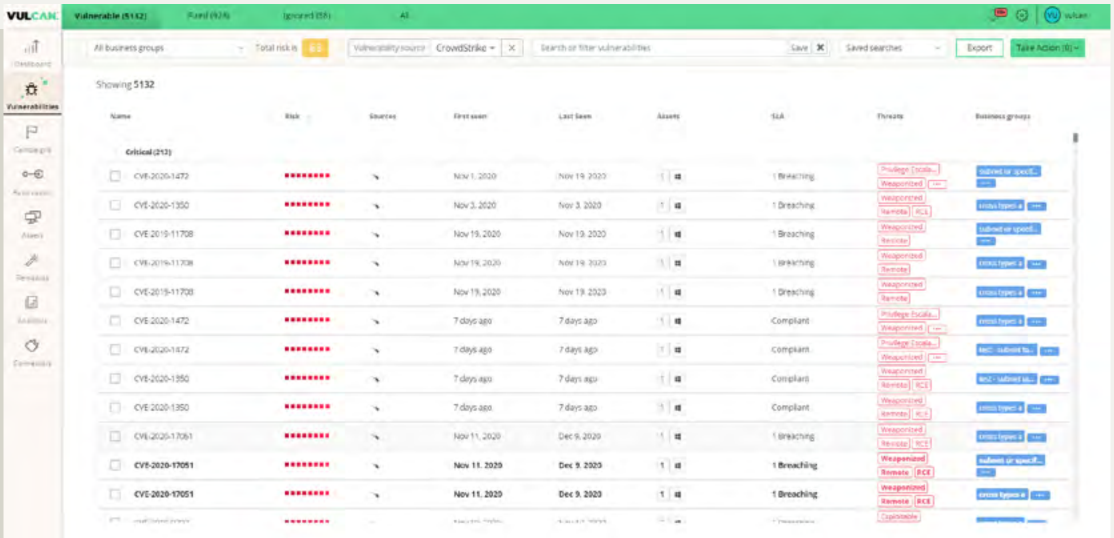
The Vulcan Cyber vulnerability remediation orchestration platform integrates with best-of-breed IT security tools to drive remediation outcomes and get fixes done. Vulcan Cyber integrates with several CrowdStrike Falcon endpoint security solutions through certified SaaS (software as a service), on-premises and API connectors. Vulcan and CrowdStrike integrate asset and vulnerability data to real-time response and mitigating actions, orchestrating and measuring the entire process, from scan to fix.

> “Old-fashioned scanners give you 20,000 vulnerabilities, 11,000 of which are critical, and say, ‘There you go. Good luck.’ Using Vulcan, our DevOps team quickly closed 30% of server vulnerabilities in a key environment. This is the vulnerability management solution we’ve been waiting for.”

Omer Singer
Head of Cyber Security Strategy,
Snowflake

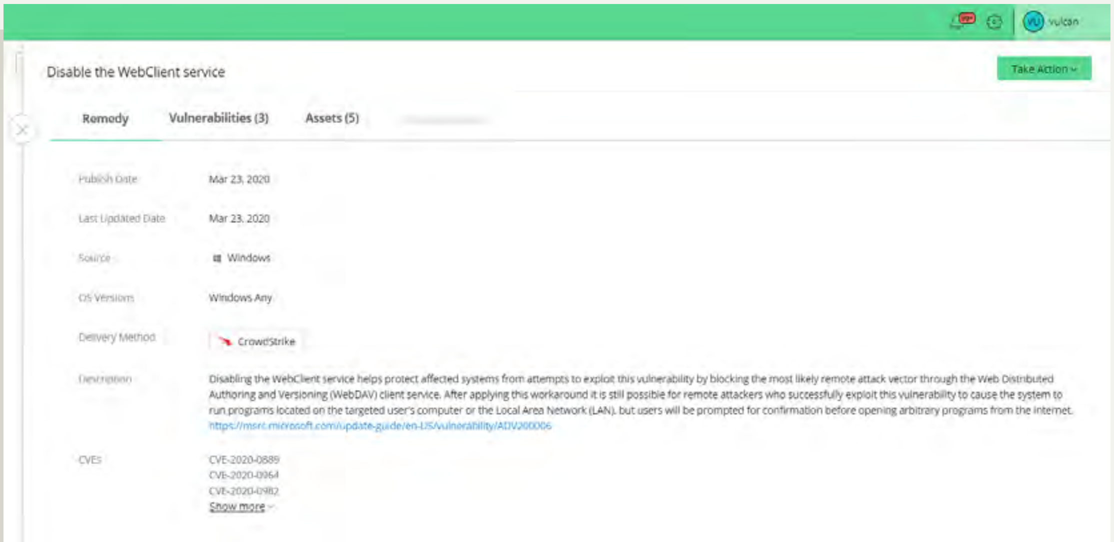


VULCAN CYBER



Showing 5132

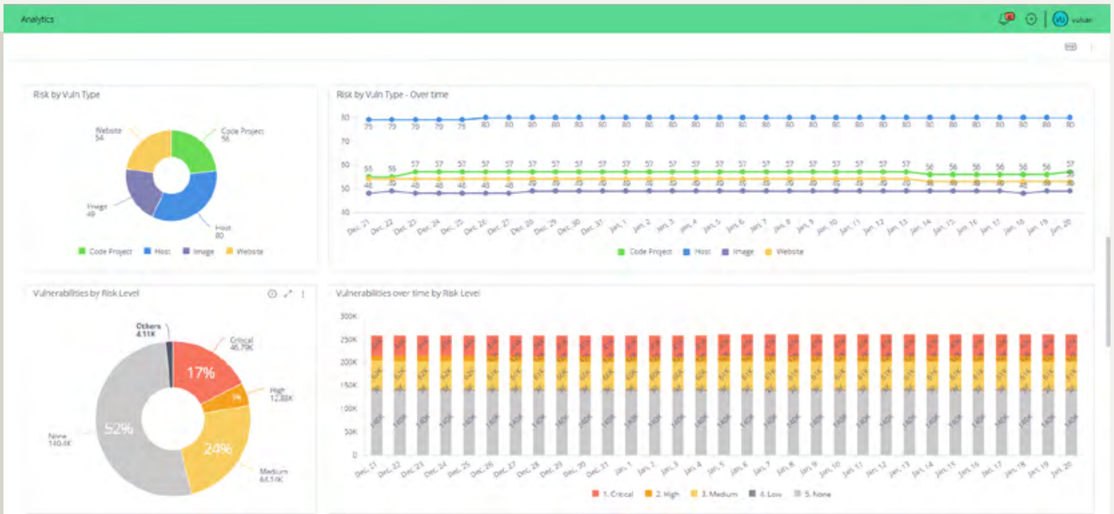
Name	Risk	Sources	First seen	Last Seen	Assets	SLA	Threats	Business groups
Critical (213)								
□ CVE-2020-1472	■■■■■■■■		Nov 1, 2020	Nov 19, 2020	1	1 Breaching	Privilege Escala... Weaponized ···	subnet or specif... ···
□ CVE-2020-1350	■■■■■■■■		Nov 3, 2020	Nov 3, 2020	1	1 Breaching	Weaponized Remote RCE	cross types a ···
□ CVE-2019-11708	■■■■■■■■		Nov 19, 2020	Nov 19, 2020	1	1 Breaching	Weaponized Remote	subnet or specif... ···
□ CVE-2019-11708	■■■■■■■■		Nov 19, 2020	Nov 19, 2020	1	1 Breaching	Weaponized Remote	cross types a ···
□ CVE-2019-11708	■■■■■■■■		Nov 19, 2020	Nov 19, 2020	1	1 Breaching	Weaponized Remote	cross types a ···
□ CVE-2020-1472	■■■■■■■■		7 days ago	7 days ago	1	Compliant	Privilege Escala... Weaponized ···	cross types a ···
□ CVE-2020-1472	■■■■■■■■		7 days ago	7 days ago	1	Compliant	Privilege Escala... Weaponized ···	test - subnet fa... ···
□ CVE-2020-1350	■■■■■■■■		7 days ago	7 days ago	1	Compliant	Weaponized Remote RCE	test2 - subnet sa... ···
□ CVE-2020-1350	■■■■■■■■		7 days ago	7 days ago	1	Compliant	Weaponized Remote RCE	cross types a ···
□ CVE-2020-17061	■■■■■■■■		Nov 11, 2020	Dec 9, 2020	1	1 Breaching	Weaponized Remote RCE	cross types a ···
□ **CVE-2020-17051**	■■■■■■■■		**Nov 11, 2020**	**Dec 9, 2020**	**1**	**1 Breaching**	**Weaponized** **Remote RCE**	subnet or specif... ···
□ **CVE-2020-17051**	■■■■■■■■		**Nov 11, 2020**	**Dec 9, 2020**	**1**	**1 Breaching**	**Weaponized** **Remote RCE**	cross types a ···
□ [illegible]	■■■■■■■■		[illegible]	[illegible]	1	[illegible]	Exploitable	[illegible]



Disable the WebClient service

Remedy | Vulnerabilities (3) | Assets (5)

Publish Date	Mar 23, 2020
Last Updated Date	Mar 23, 2020
Source	Windows
OS Versions	Windows Any
Delivery Method	CrowdStrike
Description	Disabling the WebClient service helps protect affected systems from attempts to exploit this vulnerability by blocking the most likely remote attack vector through the Web Distributed Authoring and Versioning (WebDAV) client service. After applying this workaround it is still possible for remote attackers who successfully exploit this vulnerability to cause the system to run programs located on the targeted user's computer or the Local Area Network (LAN), but users will be prompted for confirmation before opening arbitrary programs from the internet. https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV200006
CVEs	CVE-2020-0889 CVE-2020-0964 CVE-2020-0982 Show more



KEY CAPABILITIES

Vulcan Cyber correlates security threat intelligence with CrowdStrike Falcon IT asset data and insights to recommend the most impactful remediation and mitigation actions for a customer's unique business requirements. The Vulcan Cyber platform then passes prioritized actions to Falcon vulnerability detection and response automation for rapid, closed-loop mitigation.

Together, Vulcan Cyber and CrowdStrike help enterprise security teams reduce vulnerability risk with immediate, automated mitigation actions, ultimately protecting critical business assets from fast-moving threats.

Vulcan Cyber can be used to orchestrate Falcon mitigating actions such as stop and disable services, port blocking and registry key changes.

ABOUT VULCAN CYBER

Vulcan Cyber has developed the industry's first vulnerability remediation orchestration platform, built to help cybersecurity and IT operations teams to collaborate and "get fix done." The Vulcan platform orchestrates the remediation lifecycle from found to fix by prioritizing vulnerabilities, curating and delivering the best remedies, and automating processes and fixes through the last mile of remediation. Vulcan transforms vulnerability management from find to fix by making it possible to remediate vulnerabilities at scale. The unique capability of the Vulcan Cyber platform has garnered Vulcan Cyber recognition as a 2019 Gartner Cool Vendor and as a 2020 RSA Conference Innovation Sandbox finalist.

Learn more at **https://vulcan.io** or start using Vulcan today with the free remediation intelligence Remedy Cloud at **https://vulcan.io/remedy-cloud**.

Learn more at **www.crowdstrike.com**

ABOUT CROWDSTRIKE

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

Powered by the CrowdStrike Security Cloud, 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 enables customers to benefit from 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**