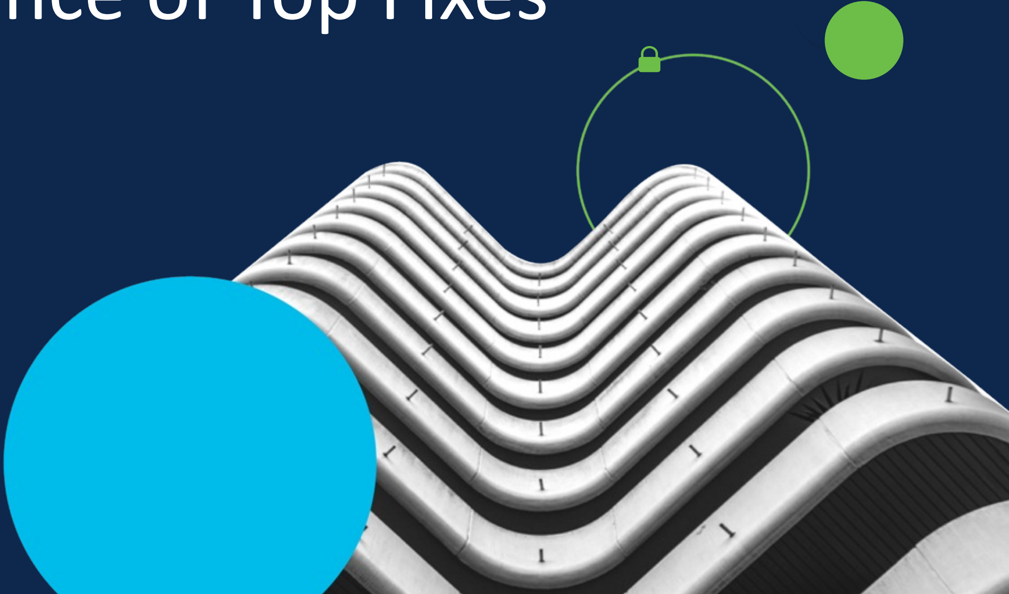
Power User Webinar

CISCO

KENNA Security

Fixology: The Data Science of Top Fixes

08/04/2022



CISCO SECURE

The bridge to possible

Kenna Security is now part of Cisco.

CISCO SECURE

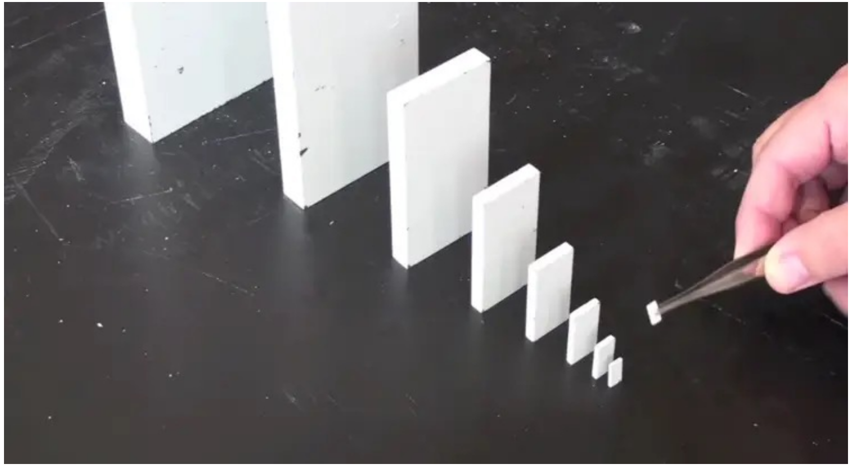
Agenda

- Review Top Fixes – What, Why, and How?
- Top Fixes Demo
- Top Fixes vs Fixes Tab
- When to avoid using Top Fixes
- Top Fixes Best Practices for Remediation Teams
- Q&A

Top Fixes – What, Why, and How

What are Top Fixes?

- A feature of Risk Meters.
- Identifies up to 3 fixes, which fall within the top 10 largest risk reductions for that Risk Meter.
- Gives you the biggest risk reduction for least amount or work.



Why would you use top Fixes?

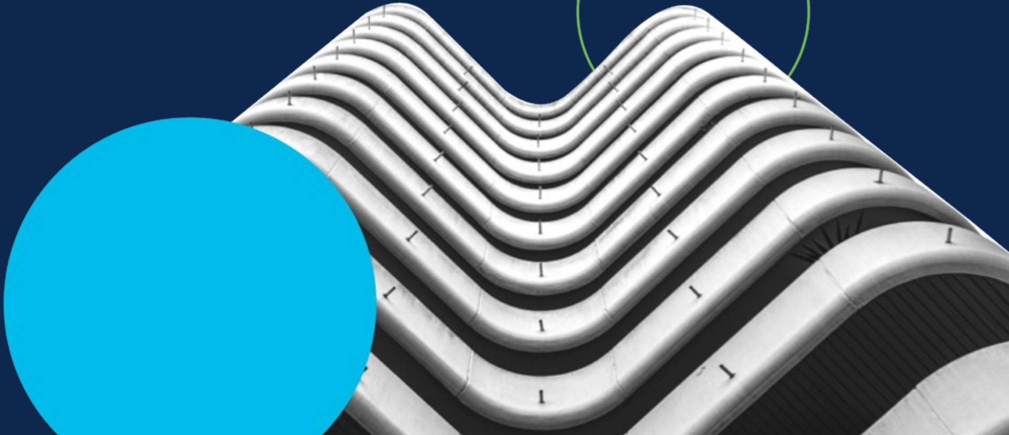
- Great place to start with Kenna or when your overall risk score is high.
- Quick wins for remediation teams looking to make the biggest impact on risk score reduction.
- Easy to use self-service tool.
- Increased efficiency by identifying where to spend time for the greatest impact.
- Provides a daily up-to-date action plan.

How do Top Fixes work?

- Based on an algorithm that looks at the possible risk reduction achievable to the average risk meter score.
- Looks at the prevalence of vulnerabilities across the group considering their affect on asset scores.
- Remember, assets are scored based on the highest vulnerability on the asset. Therefore, Top Fixes will look to see which fix groups will address the most vulnerabilities responsible for the highest asset scores.
- Top Fix suggestions are re-calculated on a daily basis, providing an ongoing and every-changing action plan.

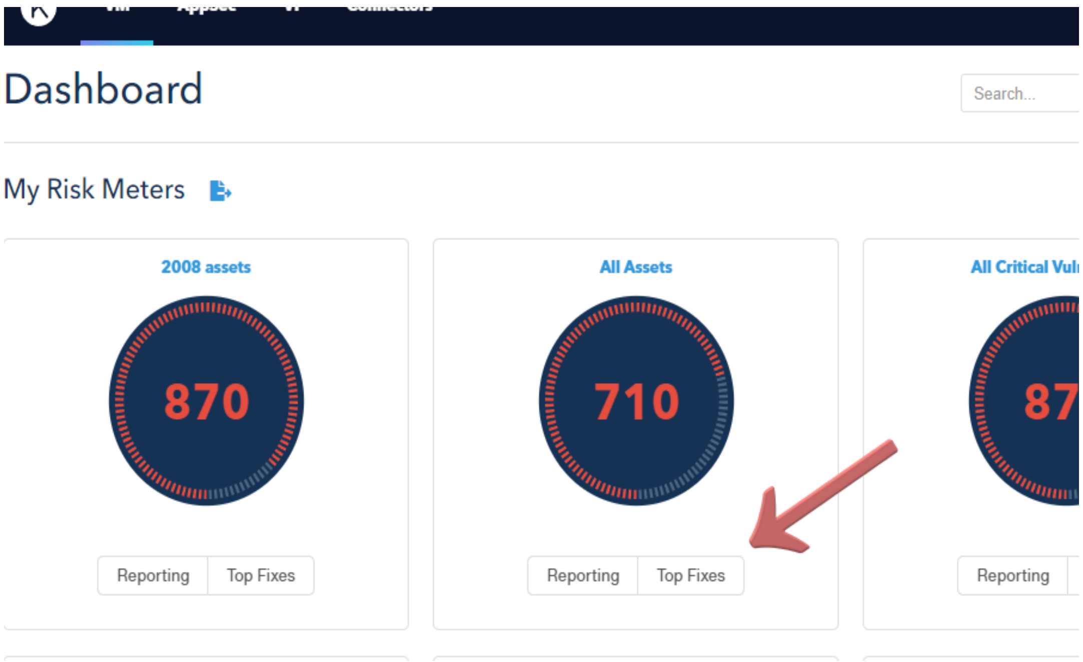
HAL 9000
"This mission is too important for me to allow you to jeopardize it."
comicbookandbeyond.com

Demo Time



Locating Top Fixes

'Top Fixes' can be accessed from the 'Dashboard'

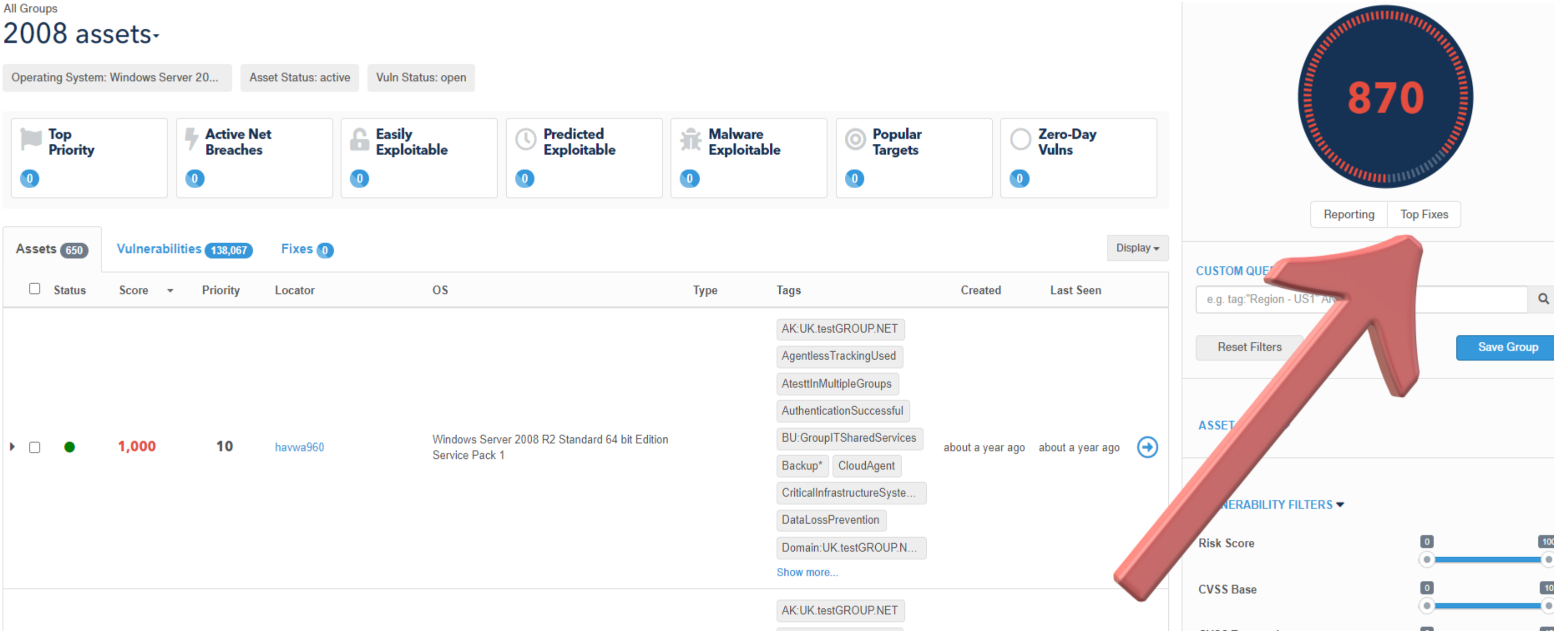


Dashboard

My Risk Meters

Locating Top Fixes

Also available via the button under the risk score for the group from the ‘Explore’ page.



All Groups

2008 assets▾

Operating System: Windows Server 20... | Asset Status: active | Vuln Status: open

Top Priority 0 | Active Net Breaches 0 | Easily Exploitable 0 | Predicted Exploitable 0 | Malware Exploitable 0 | Popular Targets 0 | Zero-Day Vulns 0

Assets 650 | Vulnerabilities 138,067 | Fixes 0

Display ▾

□	Status	Score ▾	Priority	Locator	OS	Type	Tags	Created	Last Seen
□	●	1,000	10	havwa960	Windows Server 2008 R2 Standard 64 bit Edition Service Pack 1		AK:UK.testGROUP.NET AgentlessTrackingUsed AtestInMultipleGroups AuthenticationSuccessful BU:GroupITSharedServices Backup* CloudAgent CriticalInfrastructureSyste... DataLossPrevention Domain:UK.testGROUP.N... Show more...	about a year ago	about a year ago
							AK:UK.testGROUP.NET		

870

Reporting | Top Fixes

CUSTOM QUE

e.g. tag:"Region - US1" AN

Reset Filters | Save Group

ASSET

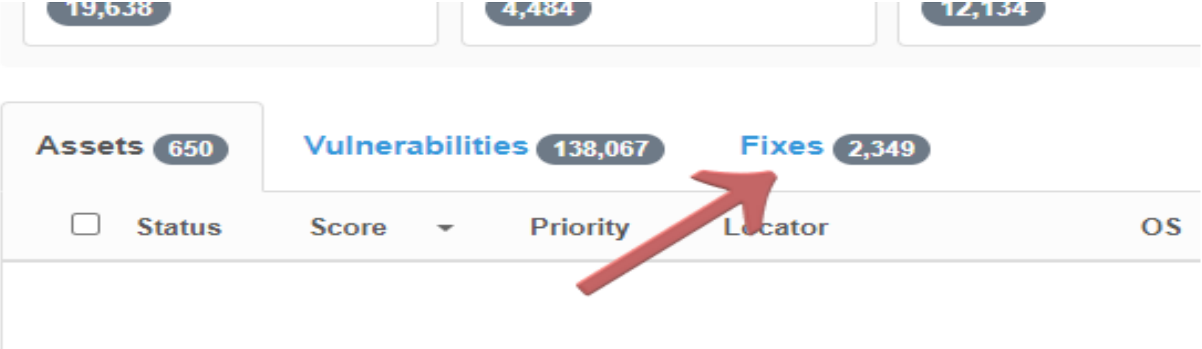
NERABILITY FILTERS ▾

Risk Score 0 100

CVSS Base 0 10

Top Fixes v Fixes Tab

The ‘Fixes’ tab on the Explore page will show all available fixes for the vulnerabilities/assets being displayed. Fixes are sorted by the number of associated vulnerabilities only. Each Fix displays all the related CVEs and each of the assets affected by those CVEs.



Here, you can filter by risk score and threat vectors to display the highest risk items and view the number of assets and vulnerabilities that would be involved but make no recommendation for least effort remediation.

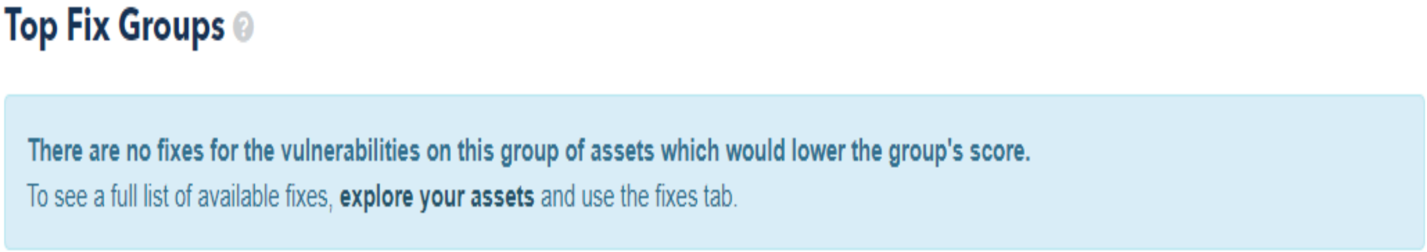
Caveats to using Top Fixes!

You may encounter problems with Top Fixes when:

- Identifying “legacy” devices with lots of vulnerabilities.
- Finding big wins when machines and vulnerabilities in a group are very dissimilar.
- Finding quick wins when there are more than three vulnerabilities at the same score level on many of the assets (this mostly means you are in a good place however in your remediation journey in this group).
- No individual fixes would change the overall score of a Risk Meter.

Why are there no top fixes?

When no individual fixes would change the overall score of a Risk Meter, no ‘Top Fixes’ are visible, and the following message is displayed:



Top Fix Groups

There are no fixes for the vulnerabilities on this group of assets which would lower the group's score.

To see a full list of available fixes, **explore your assets** and use the fixes tab.

Best Practices for Remediation Teams

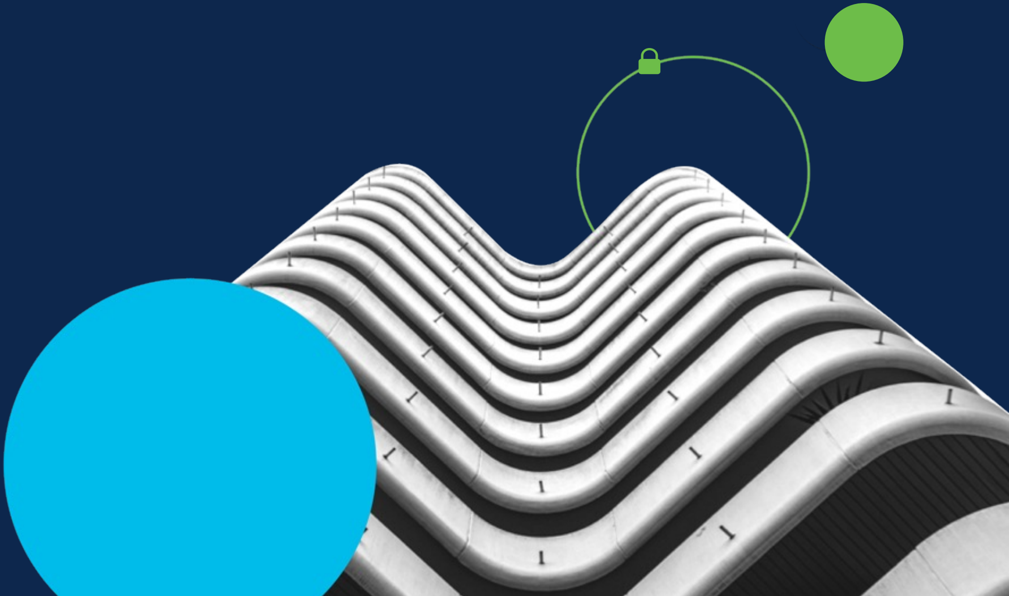
✓ Top Fixes are invaluable for fast reduction of overall risk. They should however be considered a ‘serving suggestion’ for effective and visible ROI and *not relied upon as a long-term remediation strategy*.

✓ Top Fixes should be used in conjunction with filtering high priority vulnerabilities on the Fixes tab.

✓ Top Fixes will only be suggested when:

1. There are a good number of assets that have the *same vulnerabilities* in the Risk Meter, **and,**
2. a score reduction can be found with *three or less fixes* applied.

Helpful Links & Resources



Links are in the Resource List Widget

- Why don't I see all assets requiring a fix in Top Fixes?
- Fixes and Top Fix Groups
- Predicted Exploits & Top Fixes
- Role permissions & Top Fixes
- Customizing your Dashboard & Top Fixes
- Power User Webinar - Best Practices for Remediation

Thank You!