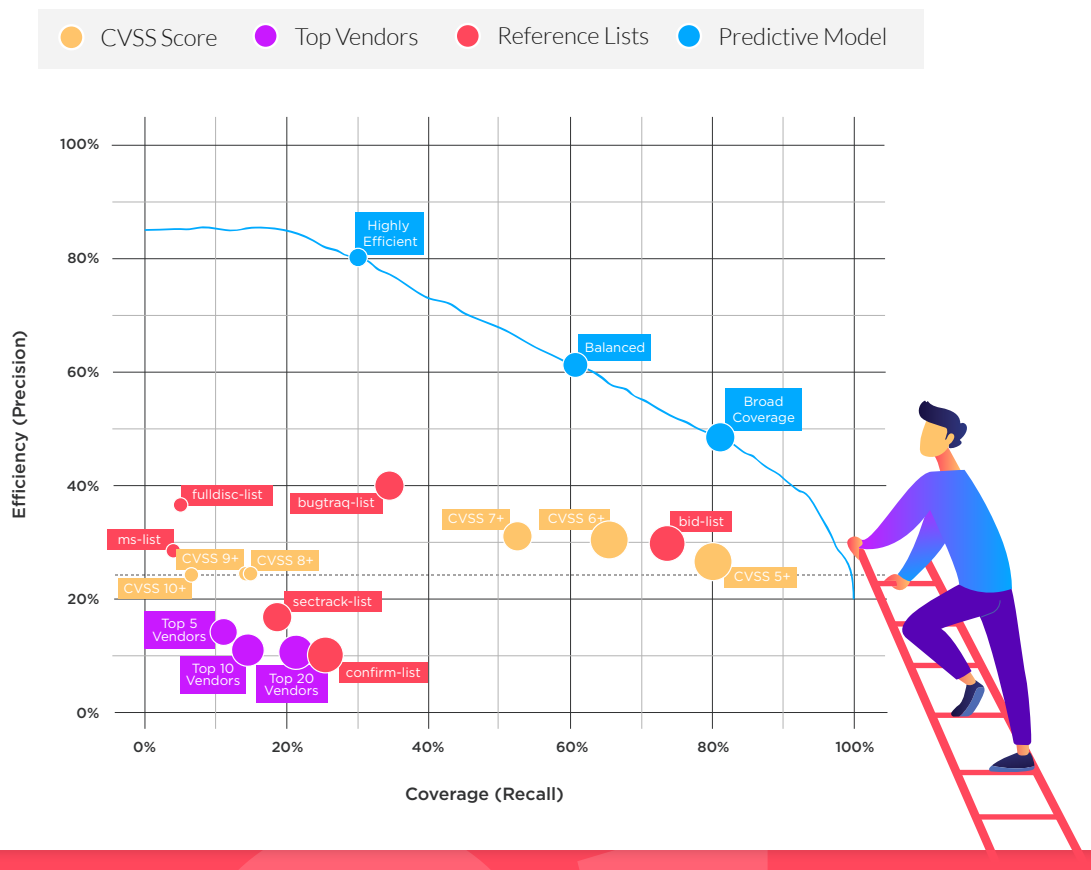
Not All Vulnerability Management Strategies Are Created Equal

Based on research by Kenna Security and the Cyentia Institute, here's a brief comparison of a few.

The Coverage/Efficiency Plot for Various Prioritization Strategies and Prediction Model Thresholds



CVSS Score

Based on a scale of 0 to 10, Common Vulnerability Scoring System (CVSS) scores reflect assessments about the underlying vulnerabilities. Organizations may remediate based on a certain CVSS score and/or higher.

CVSS 5 or Higher

26.1% efficiency
80.8% coverage

Needlessly fixing
~50,000 CVEs

CVSS 7 or Higher

31.5% efficiency
53.2% coverage

Needlessly fixing
~25,000 CVEs

Top Vendors

Remediation based on the vendors with the highest number of Common Vulnerabilities and Exposures (CVEs) from MITRE's list.

Top 5

12.3% efficiency
12% coverage

Needlessly fixing
~19,000 CVEs

Top 10

11.5% efficiency
16.5% coverage

Needlessly fixing
~28,000 CVEs

Top 20

12.1% efficiency
21.8% coverage

Needlessly fixing
~35,000 CVEs

Randomly choosing CVEs to remediate would achieve 23% efficiency and 42% coverage.

Reference Lists

These are advisory lists that are referenced in most CVE descriptions via a URL. They are used as sources of additional detailed information for the CVEs that reference them. Remediation based on those lists.

sectrack-list

16.1% efficiency
18.3% coverage

Needlessly fixing
~20,000 CVEs

confirm-list

10.9% efficiency
24.4% coverage

Needlessly fixing
~43,000 CVEs

ms-list

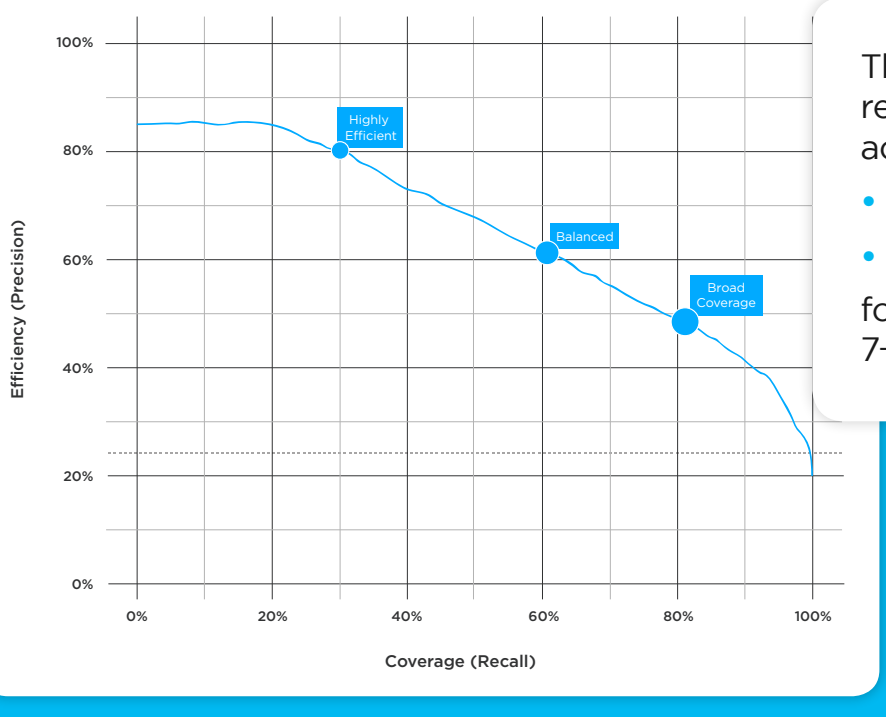
28% efficiency
4.9% coverage

Needlessly fixing
~2,700 CVEs

The above strategies cannot achieve what randomly choosing CVEs to remediate would achieve in terms of coverage and efficiency.

A Predictive Model

These remediation strategies are based on Kenna's predictive model that allows one to stay on an optimal coverage/efficiency curve. The predictive model then allows the use of different strategies based on how much effort one wants to expend by following the curve using Kenna's remediation intelligence. A small amount of effort yields the "Highly Efficient" model and as more effort is expended one moves on the curve to the right.



The "Balanced" remediation strategy achieves

- **61% efficiency,**
- **53% coverage,**

for half the effort of CVSS 7+! **(19K vs 37K CVEs)**

Highly Efficient

target the CVEs most likely to be exploited

79.3% efficiency
29.1% coverage

Needlessly fixing
~1,500 CVEs

Balanced

less efficient, but improves overall coverage

61.4% efficiency
61.7% coverage

Needlessly fixing
~7,400 CVEs

Broad Coverage

expanding the coverage at the cost of efficiency

47.9% efficiency
81.6% coverage

Needlessly fixing
~17,000 CVEs

A remediation strategy based on a predictive model can be:
8 X more efficient than remediating based on Top 20 vendors
2 X more efficient than remediating based on CVSS 7+

Want to find our more about these comparisons? Read the full report.

KENNA Security