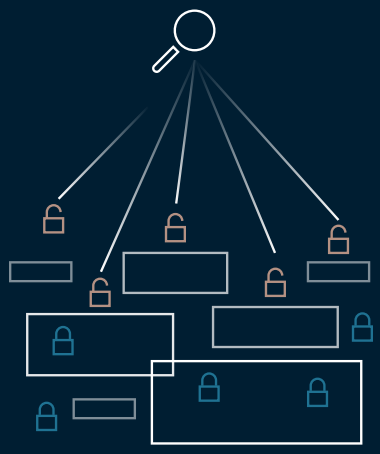
Comparing vulnerability and security configuration assessment coverage of leading VM vendors

Tenable covers more CVEs and CIS Benchmarks than Qualys and Rapid7

Infrastructure and data center attacks can be debilitating and costly. In perhaps the most destructive example of an attack, a piece of malware called NotPetya took advantage of a vulnerability in 2017 that allowed hackers to run their own code on any unpatched endpoint. The attack rendered numerous endpoints around the world useless and caused more than $10 billion USD in total damages.[1] Your organization can help limit its risk of attack exposure with vulnerability management (VM) software.

At Principled Technologies, we examined three VM solutions: Tenable.io, Rapid7 InsightVM, and Qualys® Cloud Platform. We extracted the lists of vulnerabilities, specifically common vulnerabilities and exposures (CVEs®), programmed in each solution. In addition, we enumerated the Center for Internet Security® security-configuration benchmarks (CIS Benchmarks™) as a measure of their ability to detect important security issues. The first section on the following page highlights what we found.

Using Tenable.io could help your organization manage, monitor, and address more unique vulnerabilities and exposures in your infrastructure, which could better protect your organization and users, as well as help meet security and compliance requirements of service-level agreements (SLAs).



Look for more vulnerabilities

up to 21.89% more unique CVEs*

Scan for vulnerabilities for top vendors

37.05% more unique CVEs* from 2009–2019 YTD for Oracle products compared to Rapid7 InsightVM

*covered by Tenable.io

General analysis takeaways

Our CVE analysis, based on data acquired from each of the three products, shows that Tenable.io leads Rapid7 InsightVM and Qualys Cloud Platform in coverage of both overall CVEs and CVEs with high-severity Common Vulnerability Scoring System v2 (CVSSv2) scores. Looking at the data by vendor coverage, Tenable.io leads Rapid7 InsightVM and Qualys Cloud Platform for most specific enterprise technology vendors that we analyzed. We also found that Tenable had more CIS Benchmark certifications for its products than the other two. The following sections of this report provide data and detailed analysis of our findings. We found the following notable takeaways for Tenable.io from our analysis:

- **More CVEs**: Tenable.io covers 8,218 more CVEs than Rapid7 InsightVM, a margin of 19.59 percent. Tenable.io covers 9,009 more CVEs than Qualys Cloud Platform, a margin of 21.89 percent.
- **More CVEs by CVSSv2 score**: Tenable.io covers more high-severity CVEs than Rapid7 InsightVM for every vulnerability year from 1999 to 2018. Tenable.io also covers more high-severity CVEs than Qualys Cloud Platform from almost every year in that same period.
- **Advantages for CVE coverage of top vendors in the enterprise space for years 2009 to 2019**: For most of the vendors we analyzed, Tenable.io covers more CVEs than either competitor. Compared to Qualys Cloud Platform, Tenable.io covers more CVEs for 23 of the 24 vendors we analyzed and had greater than 5 percent more coverage on 15 of those. Tenable.io and Qualys Cloud Platform were nearly equal for one vendor (a difference of one CVE). Compared to Rapid7 InsightVM, Tenable.io covers more CVEs for 15 of the 24 vendors we analyzed and had greater than 5 percent more coverage on eight of those. Tenable.io and Rapid7 InsightVM were equal for three vendors. Rapid7 InsightVM covers more CVEs for six vendors we analyzed.
- **More CIS Benchmarks**: Tenable covers nearly three times as many CIS Benchmarks as Rapid7 (126 vs. 43) and 18.87 percent more than Qualys (126 vs. 106).

On the following pages, we present our findings and analysis for the four distinctions above. For more information about our findings and how we tested, see the sections Our results (p. 9) and How we tested (p. 13).

Why vulnerability coverage should matter to your organization

When it comes to data protection and security, organizations can leverage multiple tools and approaches. So why scan for vulnerabilities?

Vulnerabilities are attack vectors in an organization that can result in loss of confidentiality, integrity, or availability. The more vulnerabilities that VM software finds, the more opportunities an organization has to close those paths to hackers.

CVEs are standard, consistent ways to identify and measure vulnerabilities across vendors. They are standardized descriptions of vulnerabilities and the key metric of the National Vulnerability Database (NVD) project, which includes "databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics."[2]

Technology vendors and the National Institute of Standards and Technology (NIST) collaborate to make the NVD work, and NIST assigns, manages, and oversees CVEs. NIST is part of the US Department of Commerce and, as such, can be considered a clearinghouse at the US-government level.

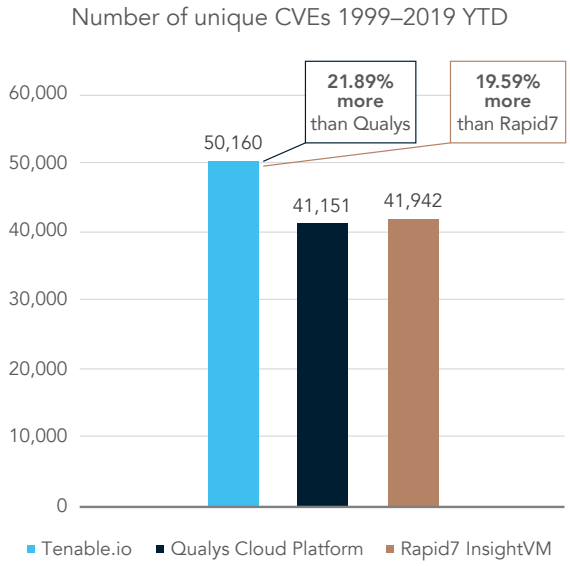
According to NIST, "[the data in the NVD] enables automation of vulnerability management, security measurement, and compliance."[3] Vulnerability management solutions such as Tenable.io use CVEs to document vulnerabilities that they claim to detect. Other vulnerability lists may lack centralization, standards, or metrics that enable automation.

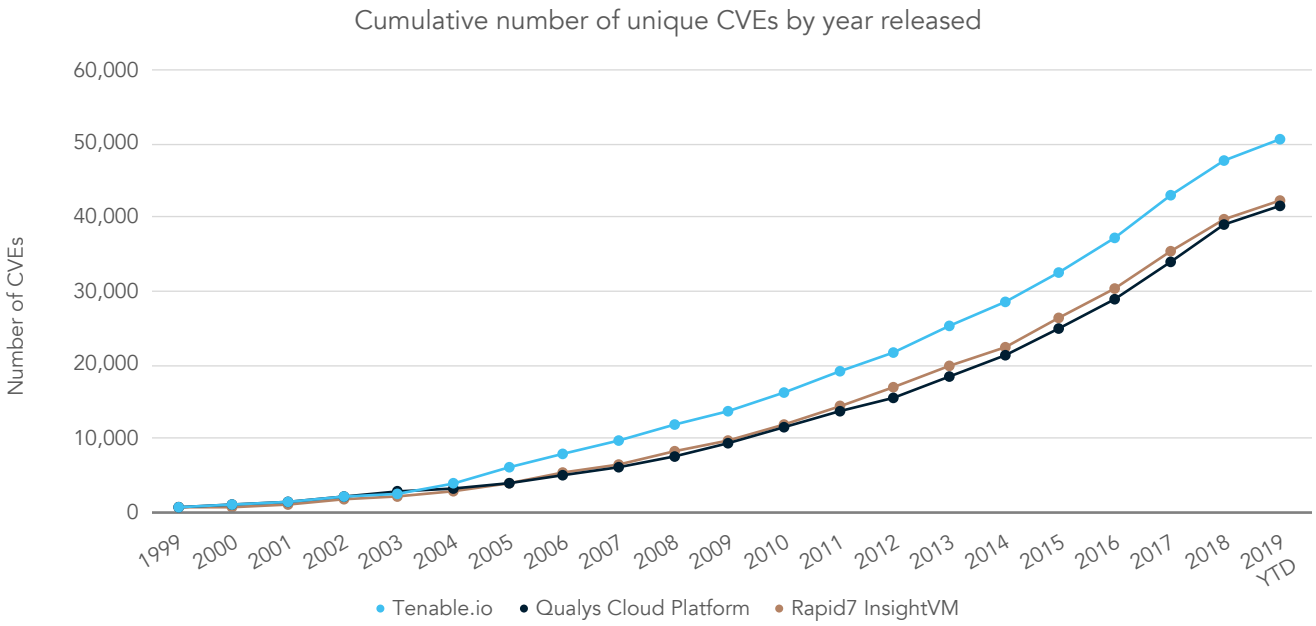
CVE analysis breakdown

CVE coverage data

We started our analysis by extracting lists of unique CVEs from the years 1999 to 2019 YTD from each of the three VM products. We then placed that information in databases, removed vulnerabilities not in the National Vulnerability Database (NVD), and totaled the number of unique CVEs each vendor claims to cover.

The chart to the right shows the number of unique CVEs each solution covers for vulnerability years 1999 to 2019 year to date (YTD). Tenable.io covers up to 21.89 percent more CVEs than Rapid7 InsightVM and Qualys Cloud Platform. As the chart below shows, Tenable.io is the clear leader of the three products for vulnerability years 2004 onward. For those vulnerability years, Tenable.io covers more CVEs than Rapid7 InsightVM and Qualys Cloud Platform. The trend of the graph below shows Tenable.io expanding its lead in CVE coverage even as all three solutions continue to increase their CVE coverage.



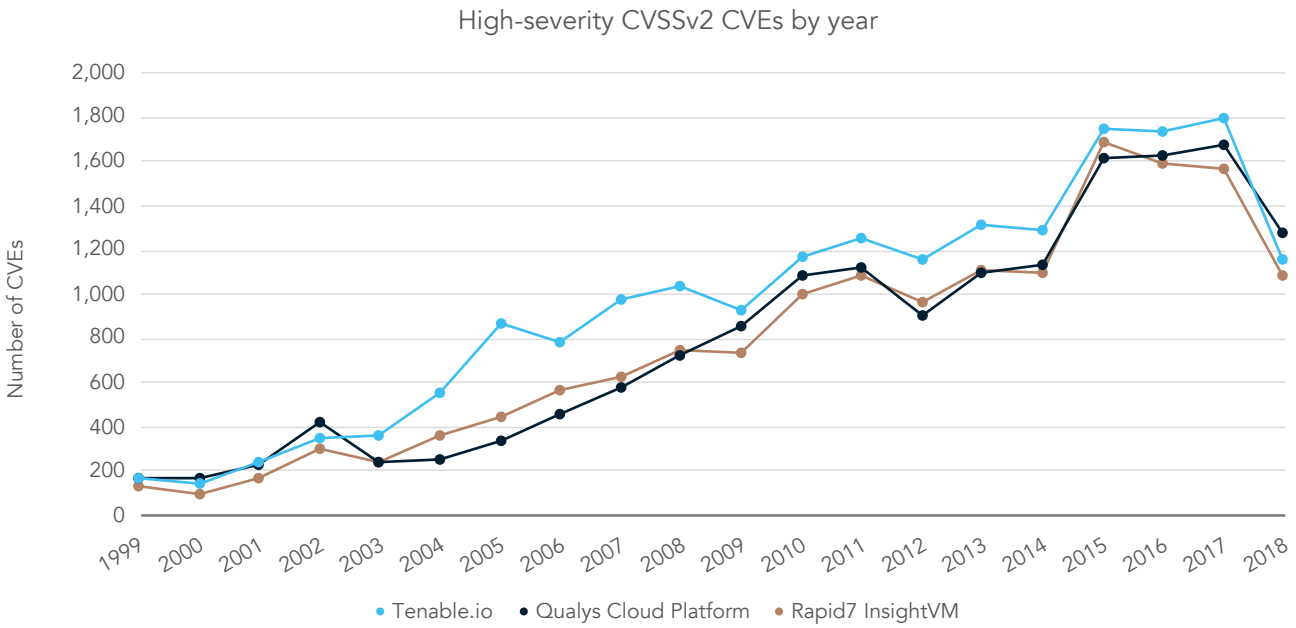


Notable takeaways:

- For every vulnerability year from 1999 to 2019 YTD, Tenable.io covers more CVEs than Rapid7 InsightVM.
- The largest coverage percentage advantage of Tenable.io over Rapid7 InsightVM was in 2005 (55.93 percent).
- The largest coverage percentage advantage of Tenable.io over Qualys Cloud Platform was in 2007 (59.72 percent).

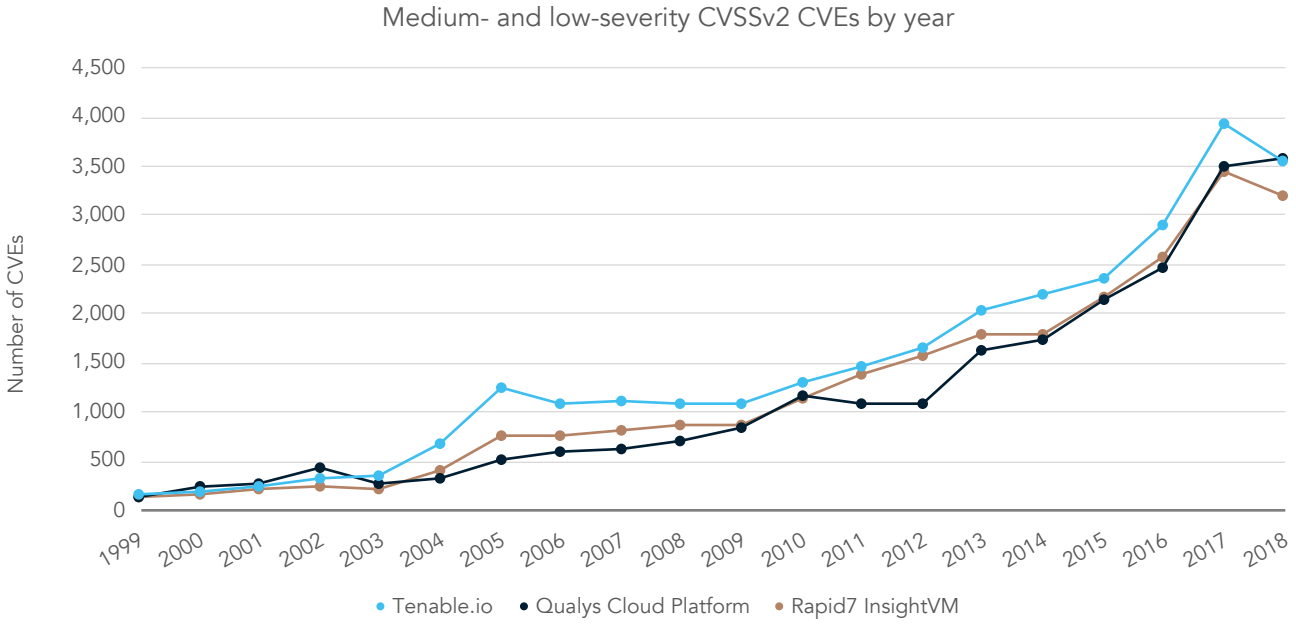
Common Vulnerability Scoring System v2 (CVSSv2) coverage data

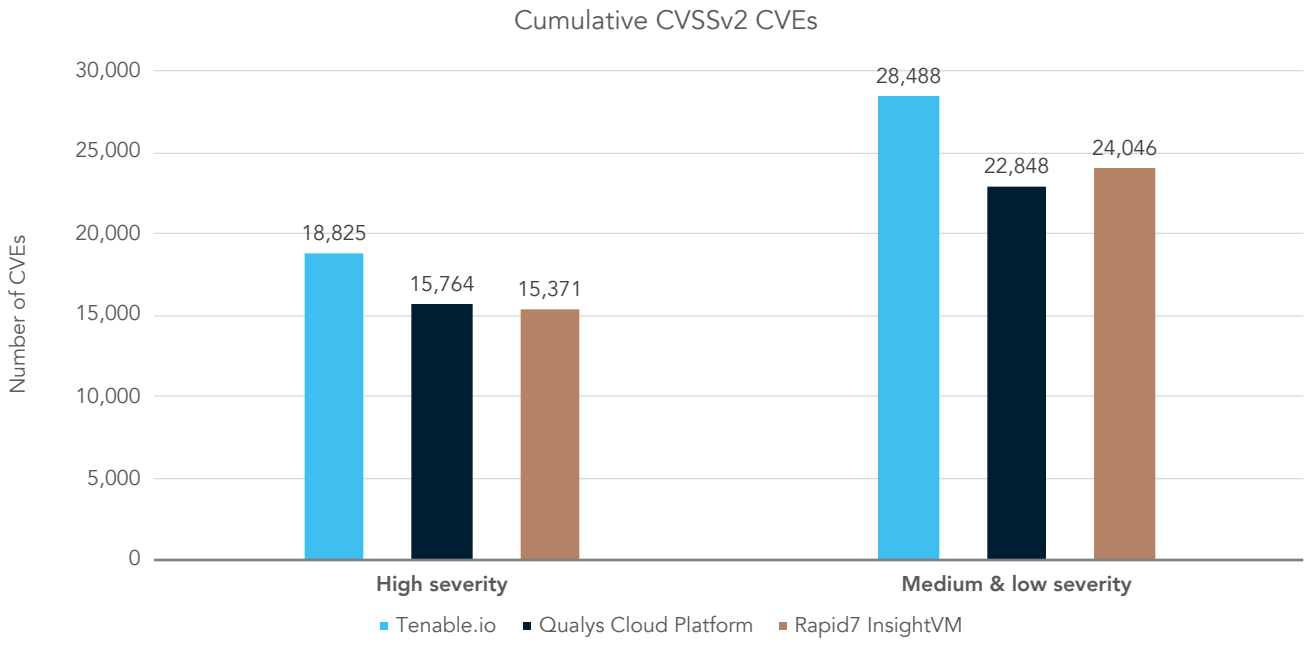
According to the Forum of Incident Response and Security Teams (FIRST), CVSS "provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes."[4] We chose to use CVSSv2 because it covers the entire CVE history and many organizations use it.



As the chart above shows, Tenable.io maintained a healthy lead in high-severity CVSSv2 CVE coverage over the two competitors for many years—in most years, the lead was in the hundreds. We varied the vertical scale in the charts to make the differences between solutions easier to see.

For vulnerability years 2003 to 2017, Tenable.io covers more medium- and low-severity CVSSv2 CVEs than Rapid7 InsightVM and Qualys Cloud Platform. Tenable.io covers more of those CVEs from 2018 than Rapid7 InsightVM, and the difference in 2018 between Tenable.io and Qualys Cloud Platform was 11 medium- and low-severity CVSSv2 CVEs.





Notable takeaways:

- Tenable.io covers more high-severity CVSSv2 CVEs than Rapid7 InsightVM each vulnerability year from 1999 to 2018. Tenable.io covers more high-severity CVSSv2 CVEs than Qualys Cloud Platform in all but three of those vulnerability years.
- For vulnerability years 2003 to 2018, Tenable.io covers more high-severity CVSSv2 CVEs than both competitors: 3,454 more than Rapid7 InsightVM (22.47 percent) and 3,061 more than Qualys Cloud Platform (19.42 percent).
- Compared to Rapid7 InsightVM, Tenable.io covers more high-severity CVSSv2 CVEs and medium- and low-severity CVSSv2 CVEs every vulnerability year in that period.
- For vulnerability years 2003 to 2018, Tenable.io covers more medium- and low-severity CVSSv2 CVEs than both competitors: 4,442 more than Rapid7 InsightVM (18.47 percent) and 5,640 more than Qualys Cloud Platform (24.68 percent).

Vendor coverage data

As previously cited, Tenable.io covers more CVEs for many specific enterprise technology vendors than Rapid7 InsightVM and Qualys Cloud Platform.

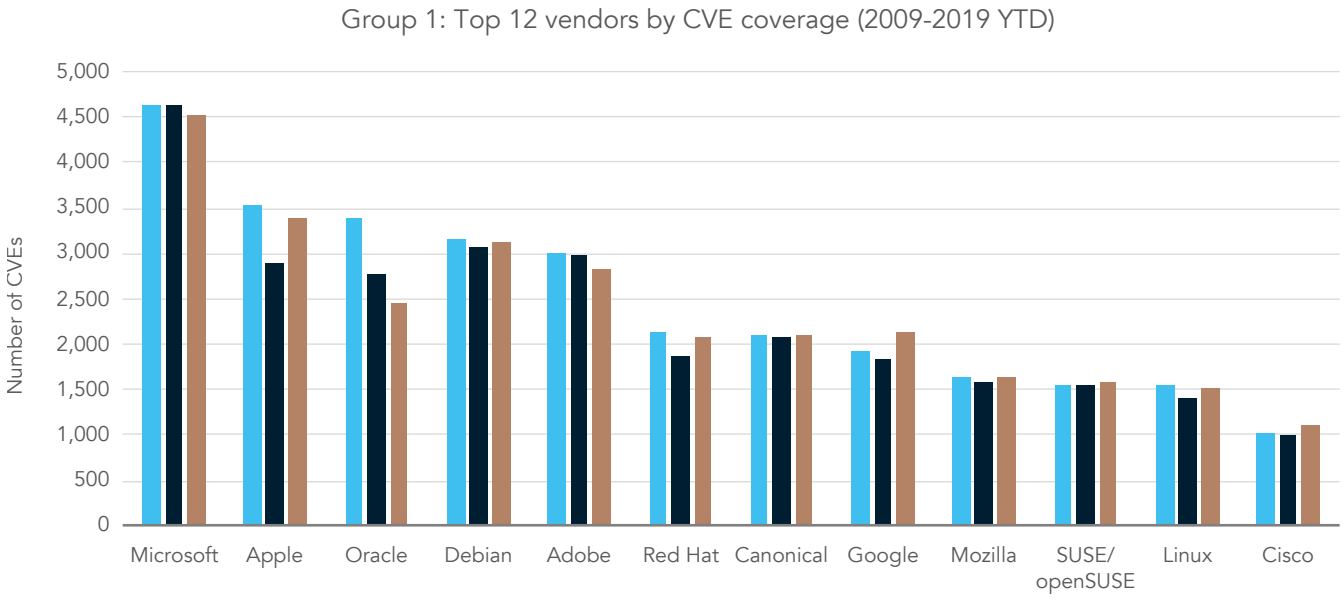
Compared to Rapid7 InsightVM for vulnerability years 2003 to 2019 YTD, Tenable.io covers:

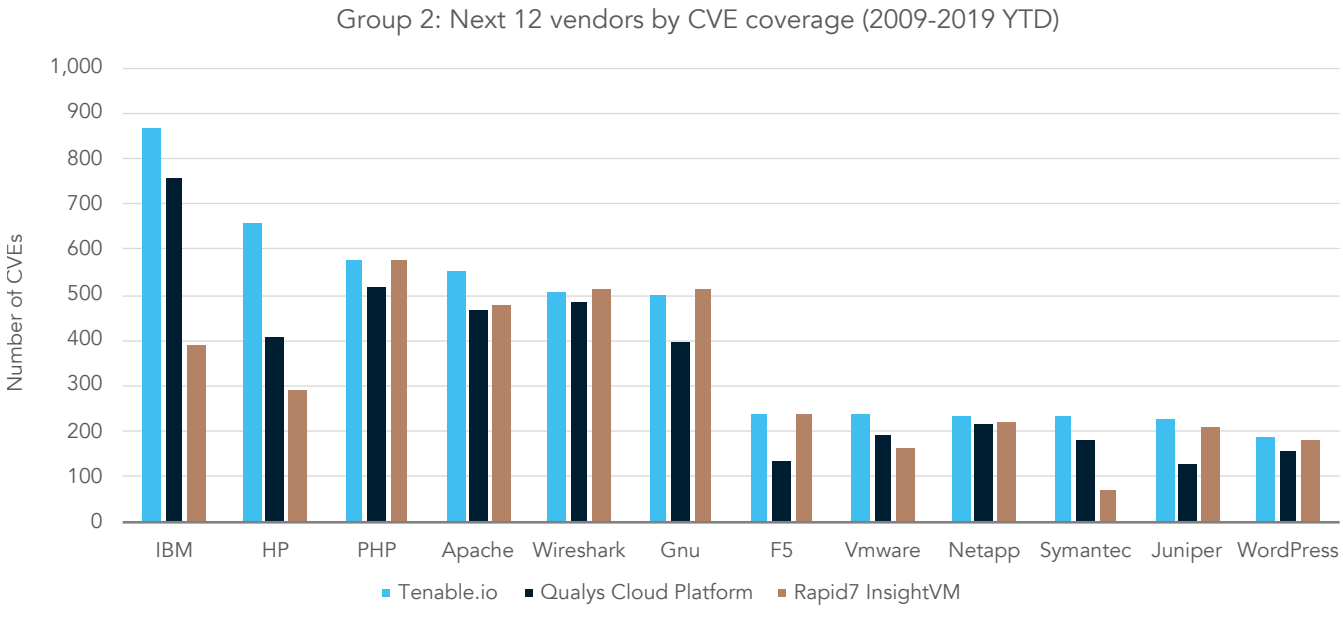
- More CVEs for 15 of the 24 vendors we analyzed
- At least 20 percent more CVEs for five of the vendors we analyzed
- 37.05 percent more CVEs for Oracle products (3,381 vs. 2,467)

Compared to Qualys Cloud Platform for vulnerability years 2003 to 2019 YTD, Tenable.io covers:

- More CVEs for 23 of the 24 vendors we analyzed
- At least 20 percent more CVEs for eight of the vendors we analyzed
- 13.05 percent more CVEs for Red Hat products (2,123 vs. 1,878)

We varied the vertical scale in the charts below to make the differences between solutions easier to see.

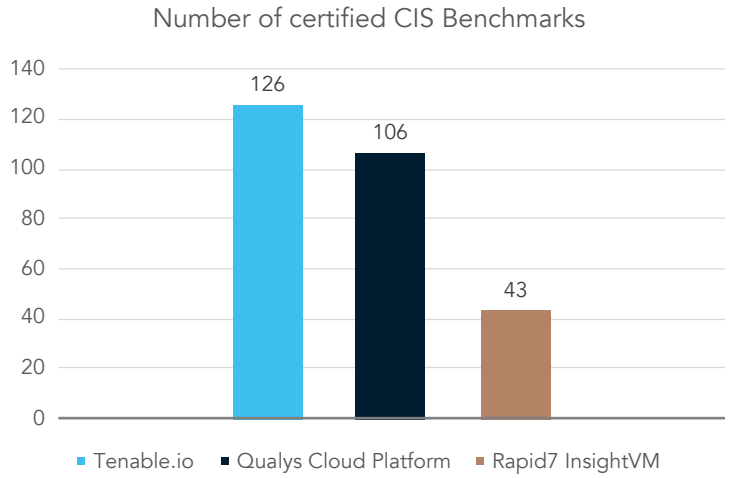




CIS analysis breakdown

We found that Tenable.io covers more CIS Benchmarks than Rapid7 InsightVM and Qualys Cloud Platform—nearly three times as many as Rapid7 InsightVM and 18.87 percent more than Qualys Cloud Platform. While it's critical to scan your infrastructure for vulnerabilities, it's also important to audit your organization's use of proper hardware and software settings.

According to CIS, "CIS Benchmarks are best practices for the secure configuration of a target system."[5] By covering more CIS benchmarks, Tenable.io can provide more visibility into potential risks due to misconfiguration in your organization's infrastructure.



We pulled the CIS Benchmarks data for the three solutions from the CIS website, which lists the CIS Benchmarks that have been certified for use by each vendor. The CIS Benchmarks that appear in each vendor's security configuration assessment (SCA) tool could include scans that they have not added to the CIS certification website. We did not include those CIS Benchmarks as part of this assessment.

Conclusion

Vulnerability management software can help your organization better protect itself by scanning for potential exposure to attacks. Tenable.io lists more unique CVEs than Rapid7 InsightVM and Qualys Cloud Platform list. Vulnerability management could aid your organization's data-protection efforts, and choosing Tenable.io could allow you to find more vulnerabilities across your environment.

---

1. Greenberg, Andy, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," accessed September 12, 2019, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
2. "Information Technology Laboratory: National Vulnerability Database," accessed September 17, 2019, https://nvd.nist.gov/.
3. "Information Technology Laboratory: National Vulnerability Database."
4. "Common Vulnerability Scoring System SIG," accessed September 21, 2019, https://www.first.org/cvss/.
5. "CIS Benchmarks™ FAQ," accessed September 22, 2019, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/#targetText=CIS%20Benchmarks%20are%20best%20practices,matter%20experts%20around%20the%20world.

Appendix

We concluded our hands-on analysis on September 16, 2019. The results in this report reflect software versions as well as software and cloud data that we obtained on September 16, 2019 or earlier. Unavoidably, they may not represent the latest versions available when this report appears.

Our results

The tables below present our findings in detail. Note: We did not include deprecated detections in our analysis. In addition, we discarded common vulnerabilities and exposures (CVEs) that did not appear in the National Vulnerability Database (NVD) CVE feeds. We could not use them for the Common Vulnerability Scoring System (CVSS) and vendor portions of the analysis.

The year 2019 had not ended when we published this report. We included 2019 data in cumulative metrics, and refer to that data as 2019 year to date (YTD). For yearly totals, we omitted 2019 and used 2018 as the last year in that sequence.

Number of unique CVEs by year

	PT analysis			Per year difference for Tenable.io™ vs. competing solution		Per year Tenable.io advantage vs. competing solution	
Year	Tenable.io	Rapid7 InsightVM	Qualys® Cloud Platform	Rapid7 InsightVM	Qualys Cloud Platform	Rapid7 InsightVM (%)	Qualys Cloud Platform (%)
1999	301	225	253	76	48	33.78	18.97
2000	302	236	380	66	-78	27.97	-20.53
2001	456	348	473	108	-17	31.03	-3.59
2002	646	498	833	148	-187	29.72	-22.45
2003	669	419	472	250	197	59.67	41.74
2004	1,207	738	544	469	663	63.55	121.88
2005	2,084	1,169	829	915	1,255	78.27	151.39
2006	1,833	1,290	1,009	543	824	42.09	81.67
2007	2,037	1,418	1,177	619	860	43.65	73.07
2008	2,070	1,580	1,382	490	688	31.01	49.78
2009	1,982	1,564	1,656	418	326	26.73	19.69
2010	2,452	2,104	2,227	348	225	16.54	10.10
2011	2,685	2,431	2,155	254	530	10.45	24.59
2012	2,787	2,496	1,953	291	834	11.66	42.70
2013	3,310	2,871	2,685	439	625	15.29	23.28
2014	3,446	2,868	2,833	578	613	20.15	21.64
2015	4,063	3,822	3,732	241	331	6.31	8.87
2016	4,601	4,119	4,053	482	548	11.70	13.52
2017	5,693	4,976	5,143	717	550	14.41	10.69
2018	4,689	4,245	4,823	444	-134	10.46	-2.78
Totals	**47,313**	**39,417**	**38,612**	**7,896**	**8,701**	**20.03**	**22.53**

Cumulative unique CVEs by year

	CVE count			Amount more for Tenable.io vs. competing solution		Tenable.io advantage vs. competing solution	
Year	Tenable.io	Rapid7 InsightVM	Qualys Cloud Platform	Rapid7 InsightVM	Qualys Cloud Platform	Rapid7 InsightVM (%)	Qualys Cloud Platform (%)
1999	301	225	253	76	48	33.78	18.97
2000	603	461	633	142	-30	30.80	-4.74
2001	1,059	809	1,106	250	-47	30.90	-4.25
2002	1,705	1,307	1,939	398	-234	30.45	-12.07
2003	2,374	1,726	2,411	648	-37	37.54	-1.53
2004	3,581	2,464	2,955	1,117	626	45.33	21.18
2005	5,665	3,633	3,784	2,032	1,881	55.93	49.71
2006	7,498	4,923	4,793	2,575	2,705	52.31	56.44
2007	9,535	6,341	5,970	3,194	3,565	50.37	59.72
2008	11,605	7,921	7,352	3,684	4,253	46.51	57.85
2009	13,587	9,485	9,008	4,102	4,579	43.25	50.83
2010	16,039	11,589	11,235	4,450	4,804	38.40	42.76
2011	18,724	14,020	13,390	4,704	5,334	33.55	39.84
2012	21,511	16,516	15,343	4,995	6,168	30.24	40.20
2013	24,821	19,387	18,028	5,434	6,793	28.03	37.68
2014	28,267	22,255	20,861	6,012	7,406	27.01	35.50
2015	32,330	26,077	24,593	6,253	7,737	23.98	31.46
2016	36,931	30,196	28,646	6,735	8,285	22.30	28.92
2017	42,624	35,172	33,789	7,452	8,835	21.19	26.15
2018	47,313	39,417	38,612	7,896	8,701	20.03	22.53
2019 YTD	50,160	41,942	41,151	8,218	9,009	19.59	21.89

Number of CVEs by year and CVSSv2 severity level

According to the National Institute for Standards and Technology (NIST), CVSS "is an open framework for communicating the characteristics and severity of software vulnerabilities."[1]

	High			Medium and low		
Year	Tenable.io	Qualys Cloud Platform	Rapid7 InsightVM	Tenable.io	Qualys Cloud Platform	Rapid7 InsightVM
1999	161	152	118	140	101	107
2000	137	160	90	165	220	146
2001	235	220	152	221	253	196
2002	343	416	288	303	417	210
2003	345	234	228	324	238	191
2004	543	243	354	664	301	384
2005	856	325	437	1,228	504	732
2006	777	448	554	1,056	561	736
2007	961	567	620	1,076	610	798
2008	1,020	714	739	1,050	668	841
2009	913	840	721	1,069	816	843
2010	1,162	1,074	986	1,290	1,153	1,118
2011	1,241	1,108	1,071	1,444	1,047	1,360
2012	1,151	894	949	1,636	1,059	1,547
2013	1,303	1,089	1,098	2,007	1,596	1,773
2014	1,281	1,117	1,090	2,165	1,716	1,778
2015	1,731	1,608	1,671	2,332	2,124	2,151
2016	1,730	1,614	1,577	2,871	2,439	2,542
2017	1,787	1,670	1,556	3,906	3,473	3,420
2018	1,148	1,271	1,072	3,541	3,552	3,173
Totals	**18,825**	**15,764**	**15,371**	**28,488**	**22,848**	**24,046**

1. "Information Technology Library: National Vulnerability Database - Vulnerability Metrics," accessed September 17, 2019, https://nvd.nist.gov/vuln-metrics/cvss.

Number of unique CVEs associated with top vendors

Group	Technology vendor	Tenable.io	Qualys Cloud Platform	Rapid7 InsightVM
1	Microsoft	4,625	4,626	4,531
	Apple®	3,522	2,883	3,388
	Oracle®	3,381	2,771	2,467
	Debian	3,141	3,066	3,120
	Adobe®	2,993	2,986	2,834
	Red Hat	2,123	1,878	2,078
	Canonical	2,093	2,064	2,097
	Google	1,938	1,835	2,124
	Mozilla®	1,628	1,575	1,628
	SUSE/openSUSE	1,565	1,549	1,573
	Linux	1,538	1,415	1,529
	Cisco®	1,029	1,012	1,110
2	IBM®	868	754	389
	HP	657	406	289
	PHP	578	518	578
	Apache	551	466	479
	Wireshark	509	482	511
	Gnu	498	397	514
	F5®	238	135	238
	VMware	236	191	160
	NetApp	230	213	221
	Symantec™	230	180	71
	Juniper®	225	129	211
	WordPress®	183	154	182

How we tested

Tallying CVEs

We updated the VM software and detections for each vendor on September 16, 2019, and obtained the public NVD CVE feeds on September 16, 2019.

We obtained the vulnerability detection metadata for each vendor as follows:

1. **Tenable.io:** We logged into our account in the Tenable.io solution. We used a shell script and the Tenable.io API to enumerate and download descriptions and metadata for 109,378 plugins in JSON format. We converted the JSON data to CSV format via a jq script and sed.
2. **Qualys Cloud Platform:** In the QualysGuard console, we selected the KnowledgeBase tab, we clicked New→Download, and selected CSV.
3. **Rapid7 InsightVM:** We downloaded the metadata from the local VM by downloading in chunks of 500 entries and combining the resultant 299 JSON files. We converted the JSON data to CSV format via a jq script and sed.

In each case, we omitted detections that the vendor had marked "deprecated."

For the NVD CVE data, we used a jq script and sed to convert the JSON data to CSV format. We omitted CVEs that NVD marked as rejected. We also filtered the affected vendors to remove versioning information.

We extracted the unique CVEs from each of our vendor CSV files, and removed any CVEs that were not in our CSV file of NVD CVEs.

From each set of winnowed CVEs, we calculated the number of unique CVEs by year, by CVSSv2 base severities per year, and by 24 vendors per year. The year associated with any CVE in this report is the year encoded in the name of the CVE; e.g., YYYY is the year for CVE-YYYY-XXXX. This definition is similar to the methodology used in the NIST CVE assignment process.

Tallying CIS Benchmarks™

We obtained the raw lists of CIS Benchmarks for each solution from these CIS webpages:

- https://www.cisecurity.org/partner/tenable/
- https://www.cisecurity.org/partner/qualys/
- https://www.cisecurity.org/partner/rapid7/

First, to eliminate counting CIS Benchmarks twice and concentrate on the products covered by the CIS Benchmarks, we removed CIS Benchmark levels and CIS versioning information. For comparison purposes, we simplified the CIS Benchmark names by removing, in order, the strings 'CIS Benchmark for' and 'CIS', 'Profile', 'Level [12]', 'Level II', and 'Level I'. We removed the CIS Benchmark version number (of the form ' v#.#.#', 'v#.#.#.#.#', or '#.#.#'). After reducing the benchmark names, we eliminated duplicates.

Finally, we reduced the list using this rule:

- Identify and eliminate duplicates by identifying benchmarks that cover the same product. For example, these pairs represent the same benchmark:
  - 'CentOS 6' and 'CentOS Linux 6'
  - 'Microsoft Word 2016' and 'Microsoft Office Word 2016'
  - 'Oracle Database Server 11*g*' and 'Oracle Database 11*g*'

This project was commissioned by Tenable.

Principled Technologies®

Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc.
All other product names are the trademarks of their respective owners.

DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY:
Principled Technologies, Inc. has made reasonable efforts to ensure the accuracy and validity of its testing, however, Principled Technologies, Inc. specifically disclaims any warranty, expressed or implied, relating to the test results and analysis, their accuracy, completeness or quality, including any implied warranty of fitness for any particular purpose. All persons or entities relying on the results of any testing do so at their own risk, and agree that Principled Technologies, Inc., its employees and its subcontractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing procedure or result.

In no event shall Principled Technologies, Inc. be liable for indirect, special, incidental, or consequential damages in connection with its testing, even if advised of the possibility of such damages. In no event shall Principled Technologies, Inc.'s liability, including for direct damages, exceed the amounts paid in connection with Principled Technologies, Inc.'s testing. Customer's sole and exclusive remedies are as set forth herein.