



Vulnerability Management Buyer's Guide and Reviews October 2019

Get a custom version of this report...personalized for you!

Thanks for downloading this IT Central Station report.

Note that this is a generic report based on reviews and opinions from the entire IT Central Station community. We offer a [customized report](#) personalized for you based on:

- Your industry
- Company size
- Which solutions you're already considering

It includes recommendations for you based on what other people like you are researching and using.

It takes 2-3 minutes to get the report using our shortlist builder wizard. We recommend it!

[Get your personalized report here.](#)

Contents

Vendor Directory	4
Top Vendors	5 - 6
Top Solutions by Ranking Factor	7
Focus on Solutions	
Qualys VM	8 - 10
Skybox Security Suite	11 - 13
Tenable Nessus	14 - 16
Rapid7 InsightVM	17 - 19
Tenable SecurityCenter	20 - 22
Rapid7 Metasploit	23 - 24
Fortinet FortiDB	25 - 27
Qualys Virtual Scanner Appliance	28 - 29
Tripwire IP360	30 - 31
RiskSense	32
About This Report and IT Central Station	33

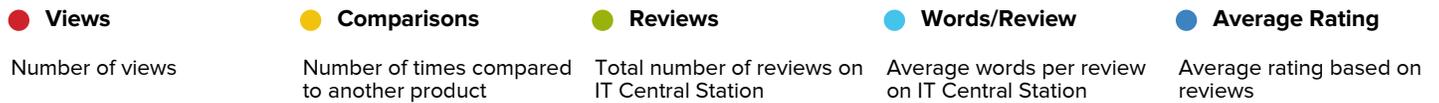
Vendor Directory

ARCON	ARCON ARSIM	Qualys	Qualys Virtual Scanner Appliance
Aruba Networks	Niara	Rapid7	Rapid7 InsightVM
Balbix	Balbix BreachControl	Rapid7	Rapid7 Metasploit
BMC	BMC TrueSight Vulnerability Management	Resolver	Resolver Threat and Vulnerability Management
Critical Watch	Critical Watch FusionVM	RiskSense	RiskSense
CyberGRX	CyberGRX	SecPoint	SecPoint Penetrator Vulnerability Scanner
DataVisor	DataVisor	Sixgill	Sixgill
Digital Defense	Frontline VM	Skybox Security	Skybox Security Suite
Flexera	Flexera Software Vulnerability Manager	SolarWinds	SolarWinds MSP Risk Intelligence
Fortinet	Fortinet FortiDB	Tenable Network Security	Tenable SecurityCenter
Hillstone Networks	Hillstone Security Audit Platform	Tenable Network Security	Tenable Nessus
Ivanti	Lumension Endpoint Management and Security	Tenable Network Security	Tenable.io Vulnerability Management
Kenna Security	Kenna Security Platform	Tintri	Tintri SecureVM
Qualys	Qualys VM	Tripwire	Tripwire IP360

Top Vulnerability Management Solutions

Over 369,366 professionals have used IT Central Station research. Here are the top Vulnerability Management vendors based on product reviews, ratings, and comparisons. All reviews and ratings are from real users, validated by our triple authentication process.

Chart Key



Bar length

The total ranking of a product, represented by the bar length, is based on a weighted aggregate score. The score is calculated as follows: The product with the highest count in each area gets the highest available score. (18 points for **Reviews, Words/Review, Views** and **Comparisons**.) Every other product gets assigned points based on its total in proportion to the #1 product in that area. For example, if a product has 80% of the number of reviews compared to the product with the most reviews then the product's points for reviews would be 18 (weighting factor) * 80% = 14.4. For **Average Rating**, the maximum score is 28 points awarded linearly between 6-10 (e.g. 6 or below=0 points; 7.5=10.5 points; 9.0=21 points; 10=28 points). If a product has fewer than ten reviews, the point contribution for Average Rating and Words/Review is reduced: 1/3 reduction in points for products with 5-9 reviews, two-thirds reduction for products with fewer than five reviews. Reviews that are more than 24 months old, as well as those written by resellers, are completely excluded from the ranking algorithm.

1 Qualys VM



2 Skybox Security Suite



3 Tenable Nessus



4 Rapid7 InsightVM



5 Tenable SecurityCenter



6 Rapid7 Metasploit



4,528 views

3,232 comparisons

2 reviews

314 Words/Review

7.0 average rating

7 Fortinet FortiDB



2,152 views

1,188 comparisons

4 reviews

570 Words/Review

8.0 average rating

8 Qualys Virtual Scanner Appliance



509 views

326 comparisons

2 reviews

322 Words/Review

8.5 average rating

9 Tripwire IP360



1,319 views

625 comparisons

1 reviews

449 Words/Review

8.0 average rating

10 RiskSense



1,136 views

789 comparisons

0 reviews

0 Words/Review

Top Solutions by Ranking Factor

 Views

	SOLUTION	VIEWS
1	Qualys VM	11,518
2	Rapid7 InsightVM	10,331
3	Skybox Security Suite	10,121
4	Tenable Nessus	7,995
5	Tenable SecurityCenter	5,064

 Reviews

	SOLUTION	REVIEWS
1	Qualys VM	8
2	Skybox Security Suite	8
3	Tenable SecurityCenter	6
4	Tenable Nessus	6
5	Rapid7 InsightVM	5

 Words / Review

	SOLUTION	WORDS / REVIEW
1	Tenable SecurityCenter	1,076
2	Skybox Security Suite	646
3	Fortinet FortiDB	570
4	Tripwire IP360	449
5	Qualys VM	355



Qualys VM

[See 8 reviews >>](#)

Overview

Qualys Vulnerability Management (VM) is a cloud-based service that gives you immediate, global visibility into where your IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps you to continuously identify threats and monitor unexpected changes in your network before they turn into breaches.

SAMPLE CUSTOMERS

Agrokor Group, American Specialty Health, American State Bank, Arval, Life.), Axway, Bank of the West, Blueport Commerce, BSKyB, Brinks, CaixaBank, Cartagena, Catholic Health System, CEC Bank, Cegedim, CIGNA, Clickability, Colby-Sawyer College, Commercial Bank of Dubai, University of Utah, eBay Inc., ING Singapore, National Theatre, OTP Bank, Sodexo, WebEx

TOP COMPARISONS

Rapid7 InsightVM vs. Qualys VM ... Compared 29% of the time [\[See comparison\]](#)

Tenable SecurityCenter vs. Qualys VM ... Compared 23% of the time [\[See comparison\]](#)

Tenable Nessus vs. Qualys VM ... Compared 13% of the time [\[See comparison\]](#)

REVIEWERS *

TOP INDUSTRIES

Software R&D Company ... 25%
Financial Services Firm ... 13%
Comms Service Provider ... 9%
Retailer ... 6%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Comms Service Provider ... 29%
Healthcare Company ... 21%
Manufacturing Company ... 14%
Financial Services Firm ... 14%

COMPANY SIZE

1-200 Employees ... 11%
201-1000 Employees ... 25%
1001+ Employees ... 64%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.



Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES [See more Valuable Features >>](#)



Sujit Sharma

The most valuable features are that it is a simple solution that makes scanning easy. You just give it a scheduled task, and it will do everything for you. The reporting is fine, too. And, the knowledge base is pretty good, too. [\[Full Review\]](#)

Dr. Suresh Hung
enahally

The way we can maintain a current actual registry of all the IP assets within it is very good. The scanning of software assets on the endpoint machine is also useful. I've tried the scanning of similar asset vulnerabilities throughout different servers, including Unix and Windows. Qualys maintains a good intervention database. We have a service line that updates to the newest software, or whenever you set it up. The second service line has denominated my nodes across the globe. It's easy to deploy the solution. [\[Full Review\]](#)

SecuritySpe
c783

I find most valuable to achieve a channel system and we can also use it to track when we actually close the ticketing of the sites. In addition, it is quite easy to implement. We found it quite convenient. [\[Full Review\]](#)

IMPROVEMENTS TO MY ORGANIZATION [See more Improvements To My Organization >>](#)



Sujit Sharma

Before using Qualys, we had other security tools. And, the main purpose was to remove the granularity. We had so many attacks every day. Qualys really helped us manage the security for our operations. [\[Full Review\]](#)

Raghunanda
nRaju

If any anomalies are there, we can easily detect with our agent based solutions, and we can isolate them quickly, and response time or any incident is much quicker than previous. Before we were taking eight hours, now we're taking around 30 minutes to respond to any incident, security and such. [\[Full Review\]](#)

Florin
Alexandru
Pitruila

* Tracks workstations and servers. * Monitors workstations and servers for vulnerabilities and creates reports. * Performs automated, regular scans in the network. * Detects new hosts along with vulnerabilities. [\[Full Review\]](#)

**ROOM FOR IMPROVEMENT**[See more Room For Improvement >>](#)

Sujit Sharma

The only improvement I can think of is on the implementation side, otherwise the operation is fine. At times it is a bit slow. Qualys is really nice, but people only use Qualys for the VM and web scan. They just file the report, and send the report to the customer or client. They don't do anything with the reports. They will get the report, and there are usually 30 to 40 vulnerabilities, not in the web servers. And, of those 30 vulnerabilities, 10 or 15 were usually the first cases. In case of those vulnerabilities are around 50, in which around 50-... [\[Full Review\]](#)

Dr.
Suresh Hung
enahally

The server application scanning has room for improvement. It's quite complex on the way it is set up, so it takes a fair bit of time in order to get your head around it in order to deploy it. Once you've deployed it, then you're never confident on the versions of the browsers and the SSL certificates, etc. You have to always go back into Qualys and check. They do talk about an agent-based scanning for non-IP machines. It sort of sits between server scanning and endpoint scanning. That's not very clear. If they can improve that and deploy, then it'll... [\[Full Review\]](#)

Raghunanda
nRaju

When tested on Zero day, there were errors. In addition, they have integrated with other third parties, but it is still not viable. They are using their own Q id's. This sometimes leads to a false positive. And, even the updating of signatures into Qualys is not that much quicker. Maybe for Windows and Linux, it is a little quicker or networks and other devices. The signature updating is not quicker. [\[Full Review\]](#)



Reviewer214

One note for room for improvement is that all of the data is stored on the cloud. I think it would be better if they came up with a big box that could store the data and collect data from, it would be a huge improvement. [\[Full Review\]](#)

 **Skybox Security Suite** [See 10 reviews >>](#)

Overview

The Skybox Security Suite platform combines firewall and network device data with vulnerability and threat intelligence, prioritizing security issues in the context of your unique environment. Powerful attack vector analytics reduce response times and risks, bringing firewall, vulnerability and threat management processes for complex networks under control.

Firewall Assurance brings all firewalls into one normalized view, continuously monitoring policy compliance, optimizing firewall rulesets and finding attack vectors that others miss. Skybox covers the most comprehensive list of firewall vendors, complex rulesets, even virtual and cloud-based firewalls. With proven scalability in 1,500+ firewall deployments, Firewall Assurance keeps rule... [\[Read More\]](#)

SAMPLE CUSTOMERS

ADP, Blue Cross Blue Shield, BT, USAID, Delta Dental, EDF Energy, EMC, HSBC, Johnson & Johnson

TOP COMPARISONS

AlgoSec vs. Skybox Security Suite ... Compared 27% of the time [\[See comparison\]](#)

Tufin vs. Skybox Security Suite ... Compared 26% of the time [\[See comparison\]](#)

RedSeal vs. Skybox Security Suite ... Compared 16% of the time [\[See comparison\]](#)

REVIEWERS *

TOP INDUSTRIES

Software R&D Company ... 23%
Financial Services Firm ... 17%
Manufacturing Company ... 12%
Comms Service Provider ... 11%

VISITORS READING REVIEWS *

COMPANY SIZE

1-200 Employees ... 44%
201-1000 Employees ... 13%
1001+ Employees ... 44%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

Top Reviews by Topic



VALUABLE FEATURES

[See more Valuable Features >>](#)


Randy
Watkins

The Vulnerability Management module is among the ones we talk about the most and the one that customers are biting off on quite a bit. Skybox, in general, has quite a few features that are particularly useful to large clients, but their scalability is unparalleled in the space. They have massive scalability, thousands of devices that they can pull from, hundreds of thousands of IP addresses for the vulnerability results and casting; that in itself is very unique. The way they do vulnerabilities, providing the additional context of the network mitiga... [\[Full Review\]](#)



Sharath K

For us, it's more important for our firewalls, to maintain the configuration compliance, to look at duplication of rules; clean up functionalities on the firewall and compliance of the firewall. That's where it's most important. We're still looking at making use of this tool for other purposes, but it's still a work in progress at this moment. We are using Network Assurance, primarily for our devices like routers and switches. Change Manager is still a work in progress for us. While we have that module, we're still working on customizing it. It's un... [\[Full Review\]](#)



Informat54af

The most valuable feature is the compliance, whether it's access compliance or the configuration compliance, to make sure that all of our devices are configured as they're supposed to be, to limit access as much possible, to follow least-access guidelines. [\[Full Review\]](#)



Informatb8c
7

It's the firewall change audit every week. Also, being able to track firewall ACL usage, so that we can produce semiannual reports on ACL usage and on shadowed and redundant rules on the firewall. [\[Full Review\]](#)



IMPROVEMENTS TO MY ORGANIZATION

[See more Improvements To My Organization >>](#)


Randy
Watkins

Specifically, in the Vulnerability Management piece, vulnerability management products are very noisy and they provide this arbitrary score called the CVSS that rates the criticality of the vulnerability. How bad would it be if somebody were to exploit this vulnerability? That doesn't matter if I have something on the network that prevents that vulnerability from being exploited. What Skybox does is to allow organizations, including three of my largest customers, to reprioritize the vulnerability they attempt to patch and mitigate, based on the cont... [\[Full Review\]](#)



Sharath K

It's given us more visibility in terms of what are the kinds of configurations that are on these devices, and how many of these are stale rules. So it's helped greatly in terms of cleaning up of rules, for sure. And it has definitely given a more secure way of backing up the configuration on these devices. [\[Full Review\]](#)



Informat54af

What we have done is found a lot of misconfigured stuff on firewalls. Our company, Verisk, is a company that buys other companies. We have 70 or so companies at last count and most of them are founder-based companies we bought. They had little to no idea of how to actually secure a firewall correctly. Using Skybox, when we bring them on we take a look at how their firewalls are configured and then make recommendations as far as what they need to do to tighten it up. That is the main function we've been using it for and that is where we have gotten t... [\[Full Review\]](#)



Skybox Security Suite

Continued from previous page



ROOM FOR IMPROVEMENT

[See more Room For Improvement >>](#)Randy
Watkins

The only place where Skybox has room for improvement, and they're working on releasing this, it's just a slow-go, is the UI. The user interface has historically been via a locally installed thick client. They are moving to a web-based console and it's slowly coming out. It looks really good right now. I've seen the previews. I've seen what's going GA. Really, it's just building in that feature parody, to take all the features that are currently in the thick client and move them into the thin client of Web-based GUI. [\[Full Review\]](#)



Sharath K

The primary room for improvement would be to enable a web interface, which is not something which is there in the product. This is supposed to have come a year, a year and a half ago, but still has failed to come out. It still needs a client application to be installed on a workstation to be able to access that server and then run these reports. So I cannot extend that access to anybody. It has to be one administrator all the time. So unlike a web interface, where you can give multiple users simultaneous access and generate the various reports, that... [\[Full Review\]](#)



Informat54af

Reporting. A lot of the reports, out of the box, are limited to a certain number of either configuration violations or access rule violations. So when you first set up a new firewall to be monitored by Skybox, you don't get a real full report. You have to really tweak it to get everything. In our business, our company buys a lot of other companies and a lot of them manage themselves. Unfortunately, for Firewall Assurance in particular, if you need a group of people to be able to manage their firewalls and only theirs, it's almost impossible because ... [\[Full Review\]](#)

Informatb8c
7

It's tough to say, because the areas of improvement, I understand the difficulty. For example, they pull configs from thousands of types of devices, and it's difficult for them to stay on top of when vendors change the way their commands work. If anything, it would be staying on top of the collector scripts, but I understand that's a very tough challenge. [\[Full Review\]](#)



PRICING, SETUP COST AND LICENSING

[See more Pricing, Setup Cost And Licensing >>](#)Randy
Watkins

In terms of licensing, it's about defining use cases. If somebody were to say, "Hey, how should I go about the licensing?" I would say, "Define what use cases you're looking for. Look at Skybox's entire portfolio and decide what is important, or what would improve your organization and then just license accordingly." I have some customers who only purchased Firewall Assurance. That was all they're interested in, and they eventually grew into the Vulnerability Management. Then I had the exact opposite where they started off with Vulnerability Management... [\[Full Review\]](#)



Sharath K

I think for the cost, what we got definitely is worth it. We're looking to expand it come next financial year, that will start from April of 2018. We'll need to look at how we will get better pricing this time around. So we're looking to expand the scope four-fold or five-fold, beyond what we have actually done initially. The only caution I would give is that whenever you license for Firewall Assurance at the same time, for some weird reason, you have to get one Network Assurance license, just to manage one firewall. That's a little bit of overkill.... [\[Full Review\]](#)



Informat54af

As with anything else, I would love it to be less expensive, but do I think pricing is a good value? Sure. I've had issues with licensing where, when they were expiring and I asked for the updated licenses, I would the wrong ones. I think their process needs to be straightened out a little bit - I don't know if they fixed it already, it has been awhile. It wasn't as straightforward as it could have been. When you get the licenses you just put in the license numbers so it's working. That part is easy. It's getting the correct licenses that can be a l... [\[Full Review\]](#)



Tenable Nessus

[See 6 reviews >>](#)

Overview

Nessus Professional is the industry's most widely deployed assessment solution for identifying the vulnerabilities, configuration issues, and malware that attackers use to penetrate your, or your customer's network. With the broadest coverage, the latest intelligence, rapid updates, and an easy-to-use interface, Nessus offers an effective and comprehensive vulnerability scanning package for one low cost.

SAMPLE CUSTOMERS

Bitbrains, Tesla, Just Eat, Crosskey Banking Solutions, Covenant Health, Youngstown State University

TOP COMPARISONS

Qualys VM vs. Tenable Nessus ... Compared 27% of the time [\[See comparison\]](#)

Rapid7 InsightVM vs. Tenable Nessus ... Compared 26% of the time [\[See comparison\]](#)

Rapid7 Metasploit vs. Tenable Nessus ... Compared 25% of the time [\[See comparison\]](#)

REVIEWERS *

TOP INDUSTRIES

Software R&D Company ... 30%

Comms Service Provider ... 14%

Media Company ... 6%

Healthcare Company ... 5%

VISITORS READING REVIEWS *

COMPANY SIZE

1-200 Employees ... 36%

201-1000 Employees ... 36%

1001+ Employees ... 27%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.



Top Reviews by Topic



VALUABLE FEATURES

[See more Valuable Features >>](#)



Miguel
Angel
Hernández
Armas

The comprehensive coverage offered by Nessus has been the most remarkable; it really does everything that has been asked of the software. It's great, the possibility of automating implementations and really your database is immense for all the compliances and vulnerabilities. Tenable University is great and allows to train all the personnel in charge of making the scans in an optimal and effective way. [\[Full Review\]](#)



Thomas
Kung

We wanted to do a lot of Hardening and we have to make sure that all endpoints are up to the certain Hardening standard and we propose the CIS benchmark to do this. That's why we use Tenable to do scanning frequency and to ensure the quality of the endpoints. [\[Full Review\]](#)



KalaiarasuSa
nthirasekera
n

I find the features that are most valuable are the policies that help us identify the vulnerabilities. These policies are then used for scanning and identifying instabilities. [\[Full Review\]](#)



Angus Konig

I have found the remedy recommendation feature helpful, as it: * Provides multiple recommendations towards the remedy of vulnerabilities. * Allows me to prioritize efforts and utilize effective technical resources. [\[Full Review\]](#)



IMPROVEMENTS TO MY ORGANIZATION

[See more Improvements To My Organization >>](#)



Miguel
Angel
Hernández
Armas

Nessus has greatly improved the security of our clients' networks. The comfortable management of their systems makes it easier for engineers to use the codes for each vulnerability or compliance. Deploying the server to launch the scans is very easy, and only the necessary prerequisites for scanning should be fulfilled. Nessus has been very valuable to the company. [\[Full Review\]](#)



Thomas
Kung

We use Tenable Nessus for scanning. We find lots of vulnerabilities and then we reduce the time spent on finding inbox vulnerabilities. Of course, Tenable streamlines the process. It has been a positive experience overall. Tenable can scan for missing patches for the endpoints. We can scan it and then, once we can support any endpoint without patching, we inform our users. [\[Full Review\]](#)



Ladislav
Solc

This is something that allows us to quickly get a really important information context. We can now deliver highly professional consulting using the product. [\[Full Review\]](#)



Tenable Nessus

Continued from previous page



ROOM FOR IMPROVEMENT

[See more Room For Improvement >>](#)



Miguel
Angel
Hernández
Armas

* I think that the next versions could improve the graphical interface to make more intuitive the management of the reports. * Additionally, it could include better features in the vulnerability scan at the language level. [\[Full Review\]](#)



Thomas
Kung

This is still a maturing product. Tenable is only a scanner for one ability, while other solutions like Rapid7 have more tools for verification. We still have to manually verify to see if the vulnerability is a false positive or not. [\[Full Review\]](#)



Ladislav
Solc

From my point of view, the solution basically is not for large enterprises. I also think there should be built-in plugins for the public cloud vendors. [\[Full Review\]](#)



Angus König

* They should improve the I/O reporting and the customized spreadsheet export feature. * Multiple steps to create an actionable plan will be a great addition to Nessus. [\[Full Review\]](#)



Overview

Rapid7 InsightVM is the vulnerability assessment tool built for the modern web. InsightVM combines complete ecosystem visibility, an unparalleled understanding of the attacker mindset, and the agility of SecOps so you can act before impact.

SAMPLE CUSTOMERS

ACS, Acosta, AllianceData, amazon.com, biogen idec, CBRE, CATERPILLAR, Deloitte, COACH, GameStop, IBM

TOP COMPARISONS

Qualys VM vs. Rapid7 InsightVM ... Compared 43% of the time [\[See comparison\]](#)

Tenable Nessus vs. Rapid7 InsightVM ... Compared 18% of the time [\[See comparison\]](#)

Tenable SecurityCenter vs. Rapid7 InsightVM ... Compared 14% of the time [\[See comparison\]](#)

REVIEWERS *

TOP INDUSTRIES

Software R&D Company ... 29%

Financial Services Firm ... 16%

Comms Service Provider ... 9%

Manufacturing Company ... 8%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

Top Reviews by Topic

VALUABLE FEATURES

[See more Valuable Features >>](#)


Birzu
Alexandru-
Adrian

Rapid 7 offers the community edition, a free of charge edition(32 IP's) that helps small companies to secure their IT environment. Also with this edition it helps the students to learn about Vulnerability Management. The report from Nexpose is very big, and gives you a description of the problems you have on your servers, and the solution for remediation. Other valuable feature is the ability to check the vulnerability with Metasploit with only one click. [\[Full Review\]](#)



Jim
Gallagher

The feature that we find most valuable is the granularity. You can view your assets however makes the most sense to your business. We found that we could isolate systems easily via tagging and site setup. [\[Full Review\]](#)



IMPROVEMENTS TO MY ORGANIZATION

[See more Improvements To My Organization >>](#)


Birzu
Alexandru-
Adrian

I use Nexpose to scan my production servers, check the patching level on those servers, and use the reports to show the evolution of security on my servers. [\[Full Review\]](#)



Nanda-
Kumar

When it comes to the automation, we use the plug-ins that are compatible with the dimensions. Once the builder is done, we run the test cases. Then it is installed onto the server and we run the test cases on the server after the installation. [\[Full Review\]](#)



Jim
Gallagher

Rapid7 InsightVM has given us a practical view of the vulnerabilities present in our organization. Not only does it verify the vulnerability, but scores it against the skill level of an attacker. [\[Full Review\]](#)



ROOM FOR IMPROVEMENT

[See more Room For Improvement >>](#)


reviewer613
356

We could always have a cheaper price, but other than that it's pretty good stuff. Also, if they'd expand their product line, that would be good, and they are doing so, but they're not done yet. [\[Full Review\]](#)



Birzu
Alexandru-
Adrian

For the community edition one of the big issues is with the registration. Rapid 7 only supports paid domains for registration, so no .gmail.com , .yahoo.com domains (once it was possible) . Also the resources needed by the scans can be an issue. [\[Full Review\]](#)



Nanda-
Kumar

It gives false positives at times, and this a problem. It causes problems with reporting. In addition, I did not find plug-ins for a Rapid7 InsightVM. It would be much more informational to run it through directly, so once the app is installed, once the software is installed on that particular server, it would find what exactly that application is open for. This would make things easier for us. [\[Full Review\]](#)



reviewer606
432

There are not enough templates, and the reporting is weak with this solution. It would be great if there were more templates for the analytical reports, such as patch management reports. At present, these do not exist. In addition, there are false positives. [\[Full Review\]](#)



PRICING, SETUP COST AND LICENSING

[See more Pricing, Setup Cost And Licensing >>](#)



Birzu
Alexandru-
Adrian

When you buy a vulnerability management tool, always count your IP's. If you miss one IP, and that server is compromised, you have left the door open for attackers into your environment. [\[Full Review\]](#)



Tenable SecurityCenter

[See 7 reviews >>](#)

Overview

SecurityCenter consolidates and evaluates vulnerability data across the enterprise, prioritizing security risks and providing a clear view of your security posture. With SecurityCenter, get the visibility and context you need to effectively prioritize and remediate vulnerabilities, ensure compliance with IT security frameworks, standards and regulations, and take decisive action to ensure the effectiveness of your IT security program and reduce business risk.

SAMPLE CUSTOMERS

IBM, Sempra Energy, Microsoft, Apple, Adidas, Union Pacific

TOP COMPARISONS

Qualys VM vs. Tenable SecurityCenter ... Compared 53% of the time [\[See comparison\]](#)

Rapid7 InsightVM vs. Tenable SecurityCenter ... Compared 23% of the time [\[See comparison\]](#)

ForeScout CounterACT vs. Tenable SecurityCenter ... Compared 6% of the time [\[See comparison\]](#)

REVIEWERS *

TOP INDUSTRIES

Software R&D Company ... 30%

Comms Service Provider ... 20%

Healthcare Company ... 10%

Financial Services Firm ... 8%

VISITORS READING REVIEWS *

COMPANY SIZE

1-200 Employees ... 22%

201-1000 Employees ... 11%

1001+ Employees ... 67%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.



Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES [See more Valuable Features >>](#)



Joey Smith

What is useful to me is being able to fulfill very customized scanning policies. In the clinical environment, because of vendor control, we can't perform credential-vulnerability scanning. And network scans, which I've done before, can cause a lot of impact. Being able to create very customized policies to be able to routinely scan and audit our clinical networks, while simultaneously not causing impact, is important to us. That requires a lot of flexibility in how we create the policies, so flexibility in policy-creation is a big feature. For me, a... [\[Full Review\]](#)



Justin Kolker

One of the most valuable features is their distributed scan model for allotting engines to work together as a pool and handle multiple scans at once, across multiple environments. Automatic scanning distribution is a distinguishing feature of their toolset. Also, the ability to trend data back as far back as we have disk space for, is helpful. Finally, the ability to write custom audit files is a really helpful and useful feature. That's something that not a lot of assessment companies have gotten right. There's room for improvement, but literally b... [\[Full Review\]](#)



Beej

We really love the Security Center dashboard. It performs vulnerability scanning and then outputs vulnerability data. When you are working with one, two, three, up to 10 IT pieces of equipment, managing the vulnerability data would just be fine, but when you are managing assets across an organization of 10,000+ employees, you have a really hard time normalizing those vulnerability data. The dashboard helps us out to map what things need to be prioritized, what is our current threat landscape and what would be the latest threats that we have in our n... [\[Full Review\]](#)



Abill Nerry

One valuable feature is the Assurance Report Card. with the Assurance Report Card, we are able to give our overview about security posters in just a glance. And with a report to cut this we can quickly, our executives can quickly consume that without going into the difficulties of the vulnerability issue. [\[Full Review\]](#)

IMPROVEMENTS TO MY ORGANIZATION [See more Improvements To My Organization >>](#)



Joey Smith

My department is not enterprise-managed. We don't use like tools like SCCM to push out patches. Everything is manual updating. I need to be able to track and audit against our devices and know what exactly what Microsoft hotfixes I need to see. I need to identify what specific patches are missing on devices. Or, for example, there was a Microsoft CVE alert that was put out a couple of weeks ago for RDP, Remote Desktop Protocol. I'm using the scanner now to try to identify what devices we actually need to look at to address risk on. Including IP came... [\[Full Review\]](#)



Justin Kolker

The ability to view the plug-ins, the way that the plug-in library works, is really good. It's not an individual list of 80 million different CVEs. We can actually just say, "Hey, here's a plug-in," and it really helps us to boil things down. Instead of having a million CVEs, here's the specific plug-ins that are actually tying the CVE families together. That helps our platform owners, if there is an issue, to see what it is and understand better how to fix it. Also, the fact that they display the very specific plug-in output in their details area h... [\[Full Review\]](#)



Beej

Before, we did manual management of our assets. We have an EXO file that has all our assets in it. They have the IP address and all the details of each equipment. We manually enrolled those assets to our vulnerability scanning tool for them to be scanned on a monthly basis and check what new vulnerabilities they may have. With the Security Center, we are able to automate. We were able to automate how we enroll our assets in the Security Center, and the scheduling of when we scan each asset, and how we report them to respective system owners. We are ... [\[Full Review\]](#)



ROOM FOR IMPROVEMENT

[See more Room For Improvement >>](#)



Joey Smith

In terms of the reporting, it's good for IT tools, but it doesn't give me contextual insight into what device, what kind of medical equipment it is. And in my world, that's a big deal. That's a con, given what my needs are. We can't integrate it with our biomed database to correlate data. So I can know what vulnerabilities are on it by IP address, but it doesn't tell me what device it is. Is it an MRI or a workstation? Is it the workstation which is running MRI's or is it the one that's just pulling patient images? Things like that are things that I... [\[Full Review\]](#)



Justin Kolker

It's good at creating information, it's good creating dashboards, it's good at creating reports, but if you want to take that reporting metadata and put it into another tool, that is a little bit lacking. It does great for things for the API. For instance, if we say, "What vulnerabilities do we have?" or "How many things have we scanned?" those things are great. But if we want to know more trending stuff over time, it can create a chart, but that's in a format which is really difficult to get into another program. Integration into other reporting pl... [\[Full Review\]](#)



Beej

One of the challenges that we may have experienced with that platform would be the flexibility of how to modify or create. They have this configuration compliance audit function, so if ever an organization has their own configuration standards that should be set on their servers, you have to modify those plugins in Tenable for it to match the specific values that you are looking for when you perform the configuration assessment on your equipment. It is a small challenge because it uses regular expressions on their plugins and so we are having a hard... [\[Full Review\]](#)



Abill Nerry

In terms of the configuration of the reports, there's some level of flexibility that we are not able to achieve. In terms of configuring the reports to achieve certain percentages and all of that. So, that's really the main thing I've noticed. But, apart from that, I think it's one of the best vulnerability management tools I've used, in terms of giving us the full visibility into the environment. [\[Full Review\]](#)



PRICING, SETUP COST AND LICENSING

[See more Pricing, Setup Cost And Licensing >>](#)



Joey Smith

The pricing is more than Rapid7 Nexpose. PVS and the agents, etc., are all part of that agreement. So it's pretty comprehensive, but I don't know how much it is. [\[Full Review\]](#)



Overview

Attackers are always developing new exploits and attack methods—Metasploit penetration testing software helps you use their own weapons against them. Utilizing an ever-growing database of exploits, you can safely simulate real-world attacks on your network to train your security team to spot and stop the real thing.

SAMPLE CUSTOMERS

City of Corpus Christi, Diebold, Lumenate, Nebraska Public Power District, Prairie North Regional Health, Apptio, Automation Direct, Bob's Stores, Cardinal Innovations Healthcare Solutions, Carnegie Mellon University

TOP COMPARISONS

Tenable Nessus vs. Rapid7 Metasploit ... Compared 39% of the time [\[See comparison\]](#)

Wireshark vs. Rapid7 Metasploit ... Compared 17% of the time [\[See comparison\]](#)

Darktrace vs. Rapid7 Metasploit ... Compared 12% of the time [\[See comparison\]](#)

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

Top Reviews by Topic

VALUABLE FEATURES [See more Valuable Features >>](#)



Informate5e
5

* The option to generate phishing emails has proven to be very valuable in understanding the behavior of users. * It contains almost all the available exploits and payloads. * The in-built Wireshark is valuable in performing packet analysis. * It has different installation files for different OSs. [\[Full Review\]](#)

IMPROVEMENTS TO MY ORGANIZATION [See more Improvements To My Organization >>](#)



it_user17223
9

The search engine is actually pretty cool. It actually allows you to search the vulnerability very fast, and the big difference is that the exploit you see on Metasploit has been tested and imported, it's going to work and it is not going to crash anything. That's a big thing. That's basically why I use it. [\[Full Review\]](#)

ROOM FOR IMPROVEMENT [See more Room For Improvement >>](#)



Informate5e
5

* The GUI version is not as effective as a command prompt. For general users, the PT using GUI could be improved. At the same, the track of a phishing emails were not accurate sometimes. Rapid7 could work on this further. * Metasploit cannot be installed on a machine with an antivirus. This could be improved. * There were times when it hung, then I had to restart the DB service. This leaves an area of improvement for them. * It is necessary to add some training materials and a tutorial for beginners. [\[Full Review\]](#)



Fortinet FortiDB

[See 4 reviews >>](#)

Overview

FortiDB software is a comprehensive database security and compliance platform that helps large enterprises and cloud-based service providers protect their databases and applications from internal and external threats. Its flexible policy framework allows you to quickly and easily implement internal IT control frameworks for database activity monitoring, IT audit and regulatory compliance.

SAMPLE CUSTOMERS

Chunghwa Telecom

TOP COMPARISONS

Imperva SecureSphere Database Security vs. Fortinet FortiDB ... Compared 41% of the time [\[See comparison\]](#)

IBM Guardium vs. Fortinet FortiDB ... Compared 33% of the time [\[See comparison\]](#)

Oracle Audit Vault vs. Fortinet FortiDB ... Compared 9% of the time [\[See comparison\]](#)

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.



Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES [See more Valuable Features >>](#)



Jason
Wetzel

It's great to get out, it's flexible. They have some good ramping up for performance between different devices. The biggest thing, for us lately, has been their cloud tools. They're like Intercept X from Sophos, where they'll test for ransomware. Fortinet has the same sort of set up with their cloud devices. So your firewall picks up something suspicious, it sends it up to the cloud for analysis. We also have their in-house antivirus. Having different antivirus checkpoints throughout the network is a good thing as well. [\[Full Review\]](#)



JoelSadomb
a

The most valuable feature is database security. This solution provides file-level protection. Automatic database discovery finds all databases on the network, including those across subnet and WAN boundaries. [\[Full Review\]](#)



ReviewerSE
399

It is critical to monitor the action in a database. This is the most important feature of FortiDB. You can create queries, delete data, block as a firewall and more. You can also reset the station user if you want to do a specific update. [\[Full Review\]](#)

IMPROVEMENTS TO MY ORGANIZATION [See more Improvements To My Organization >>](#)



JoelSadomb
a

24 x 7 database activity monitoring captures all forms of database activity to detect erroneous or malicious activity. Database auditing records all database activity for complete and accurate audit trails, with independent storage for additional security. [\[Full Review\]](#)



ReviewerSE
399

In most of my organization, I must disable SSL encryption in a database for monitoring by FortiDB. Once I do so, FortiDB can get to work and monitor the solution. [\[Full Review\]](#)

ROOM FOR IMPROVEMENT [See more Room For Improvement >>](#)



Jason
Wetzel

WatchGuard has a desktop-based admin tool, instead of doing everything through the web. I'm an old-school guy. I really don't like web GUI interfaces. They're always slow and laggy and their design is restricted, whereas a binary deployment for an admin tool is always faster, easier, more flexible. I would like that kind of functionality from Fortinet. In part, it's bias, because I'm familiar with it. But WatchGuard is a very flexible tool. It's very dated now, it needs to be worked on, but it is quite a good tool in that way. [\[Full Review\]](#)



Fortinet FortiDB

Continued from previous page



JoelSadomba

They need to improve the web filter to make it more user-friendly. The cost needs to be reduced. In the next release, I would like this solution to include some phishing detection, to detect phishing activity on the network. I would like a way to keep users away from my domain controller. If somebody wants access to the internet, it would have to be authenticated from the main controller, or if the user wants access for internal use. If the machine is not from the domain it is not granted access. [\[Full Review\]](#)



PRICING, SETUP COST AND LICENSING

[See more Pricing, Setup Cost And Licensing >>](#)



Jason
Wetzel

It's relatively inexpensive in comparison to everything else that has the same functionality. If you're looking at SonicWall or if you're looking at WatchGuard, their prices are about a third higher with relatively the same functionality. [\[Full Review\]](#)



Qualys Virtual Scanner Appliance

[See 2 reviews >>](#)

Overview

Qualys Virtual Scanner Appliance supports the same global scanning capabilities as our physical scanner appliance. The virtual scanner appliance is a stateless, disposable resource which acts as an extension of the Qualys Cloud Platform and is not a separately managed entity. This user guide describes how to get started with using a virtual scanner with your virtualization or cloud platform.

SAMPLE CUSTOMERS

TOP COMPARISONS

Rapid7 InsightVM vs. Qualys Virtual Scanner Appliance ... Compared 34% of the time [\[See comparison\]](#)

Kenna Security Platform vs. Qualys Virtual Scanner Appliance ... Compared 17% of the time [\[See comparison\]](#)

Microsoft Intune vs. Qualys Virtual Scanner Appliance ... Compared 11% of the time [\[See comparison\]](#)

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

Top Reviews by Topic

VALUABLE FEATURES [See more Valuable Features >>](#)



Sameer
Quraishi

The first thing we like is the scanner, the device which checks vulnerability management. They also have threat detection which maps threats. There is a feed that comes from Qualys when a new vulnerability is found. It tells us which machines are infected with that vulnerability. If there is a new attack, we definitely know that it is happening, what is happening in our environment. [\[Full Review\]](#)

IMPROVEMENTS TO MY ORGANIZATION [See more Improvements To My Organization >>](#)



Sundeep
Oberoi

The customer was manually testing asset health by point-in-time audits. Using the policy compliance module allowed this to be automated and saved time as well as generated more complete coverage of assets leading to greater assurance. [\[Full Review\]](#)

ROOM FOR IMPROVEMENT [See more Room For Improvement >>](#)



Sameer
Quraishi

What we have found is that the solution is not closely tied with the patch management. It is okay with newer ones, like Windows 10 machines; it gives the correct patch. But for Windows 7 or Windows Server 2008, it does not give us the correct patch so we have to manually identify the patches. This is a major problem. [\[Full Review\]](#)



Tripwire IP360

[See 2 reviews >>](#)

Overview

Tripwire IP360 delivers risk-based vulnerability assessment and asset discovery capabilities. With IP360, you get:

Comprehensive discovery and profiling of all network assets. Highly scalable architecture with low network impact. Advanced vulnerability scoring that identifies top risks. Prioritized change results when used with Tripwire Enterprise.

SAMPLE CUSTOMERS

State of Iowa, State of Minnesota, U.S. Cellular

TOP COMPARISONS

Qualys Web Application Scanning vs. Tripwire IP360 ... Compared 25% of the time [\[See comparison\]](#)

Tenable Nessus vs. Tripwire IP360 ... Compared 20% of the time [\[See comparison\]](#)

Acunetix Vulnerability Scanner vs. Tripwire IP360 ... Compared 8% of the time [\[See comparison\]](#)

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.



Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES [See more Valuable Features >>](#)



user9776

The most valuable feature would be the command app to control feature. It's not hugely utilized. It can go a lot further. It can be used a lot more because it can drift over into spaces from telephoning, where you have certificate expiry and it's easy with a couple of scripts to control expiry or certificates for everything else for outages with a call center solution. There are multiple areas where the product can quickly adapt by using upper command control to immediately solve a lot of issues where you don't need to look at other products. [\[Full Review\]](#)

IMPROVEMENTS TO MY ORGANIZATION [See more Improvements To My Organization >>](#)



user9776

It's become the pinnacle point for anything that enters the network or anything that's passing through to production to first be affected by IP360, hardened, and up to standard. For our integrity management, one was deployed in the bank about two years ago and that's still going to expand the usage and the product itself. That will go hand in hand with training and expanding the product as for where it's deployed. [\[Full Review\]](#)

ROOM FOR IMPROVEMENT [See more Room For Improvement >>](#)



user9776

The reporting functions can use improvement. There is room for growth because reporting functions differ a lot depending on what you're going to output. It depends on whether it's for technical or senior management and how it's interpreted. There could be growth within the reporting functionality side. [\[Full Review\]](#)

PRICING, SETUP COST AND LICENSING [See more Pricing, Setup Cost And Licensing >>](#)



user9776

It's more expensive but also more superior. I've had a lot of cases where I opted for something similar which they normally have and some other kind of products but they always fall short and it doesn't do so I know of a release of more than two different products have been deployed that have failed and are not being used anymore. [\[Full Review\]](#)



Overview

RiskSense empowers enterprises and governments to reveal cyber risk, quickly orchestrate remediation, and monitor the results. And not just for your network and end points, but for a growing attack surface!

SAMPLE CUSTOMERS

Care First, City of Albuquerque, Electric Company El Paso, State of Arizona, Washington Gas

TOP COMPARISONS

SecurityScorecard vs. RiskSense ... Compared 24% of the time [\[See comparison\]](#)

CyberGRX vs. RiskSense ... Compared 21% of the time [\[See comparison\]](#)

Kenna Security Platform vs. RiskSense ... Compared 17% of the time [\[See comparison\]](#)

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

About this report

This report is comprised of a list of enterprise level Vulnerability Management vendors. We have also included several real user reviews posted on ITCentralStation.com. The reviewers of these products have been validated as real users based on their LinkedIn profiles to ensure that they provide reliable opinions and not those of product vendors.

About IT Central Station

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors but what you really want is objective information from other users.

We created IT Central Station to provide technology professionals like you with a community platform to share information about enterprise software, applications, hardware and services.

We commit to offering user-contributed information that is valuable, objective and relevant. We protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

IT Central Station helps tech professionals by providing:

- A list of enterprise level Vulnerability Management vendors
- A sample of real user reviews from tech professionals
- Specific information to help you choose the best vendor for your needs

Use IT Central Station to:

- Read and post reviews of vendors and products
- Request or share information about functionality, quality, and pricing
- Contact real users with relevant product experience
- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendors

IT Central Station

244 5th Avenue, Suite R-230 • New York, NY 10001

www.ITCentralStation.com

reports@ITCentralStation.com

+1 646.328.1944