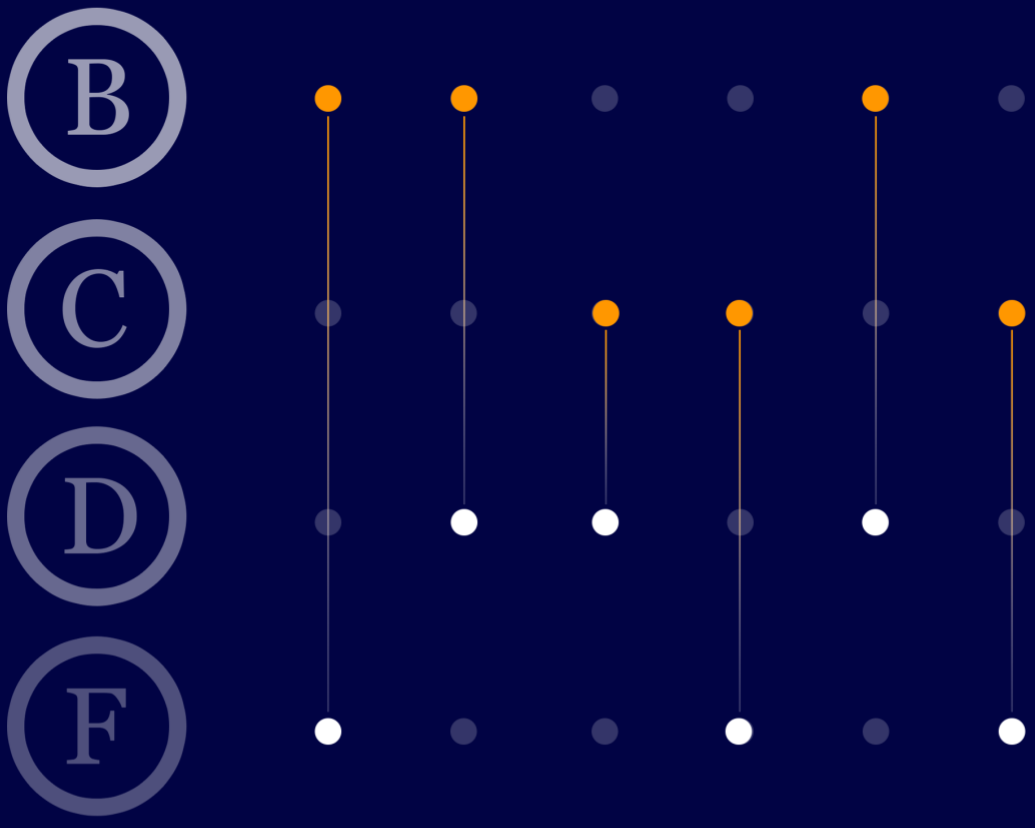
orca security

The Orca Security 2020 State of Virtual Appliance Security



How responsible are your software vendors?

Table of Contents

Executive Summary

Overview

To help move the cloud security industry forward and reduce risk for customers, Orca Security conducted a wide-reaching research and testing project to benchmark the current state of virtual appliance security.

Virtual appliances are cheap and easy for software vendors to distribute. Fully preconfigured with all requisite software, they're often delivered ready for customers to deploy to public and private cloud environments.

Customers assume that software vendors' virtual appliances are free from security risks such as known vulnerabilities and unsupported operating systems. The reality is a spectrum, from good to bad, with many virtual appliances being distributed with known and fixable security flaws.

Orca Security's research methodology

Between April 20th – May 20th, 2020, Orca Security's patent-pending SideScanning™ technology scanned over 2,000 virtual appliance images from 540 vendors for known vulnerabilities and other risks to provide an objective assessment score and ranking.

All are available in public marketplaces. Each tested product was given a security score—ranging from 0 for the worst to 100 for the best—and assigned a grade from A+ (exemplary) down to F (failure).

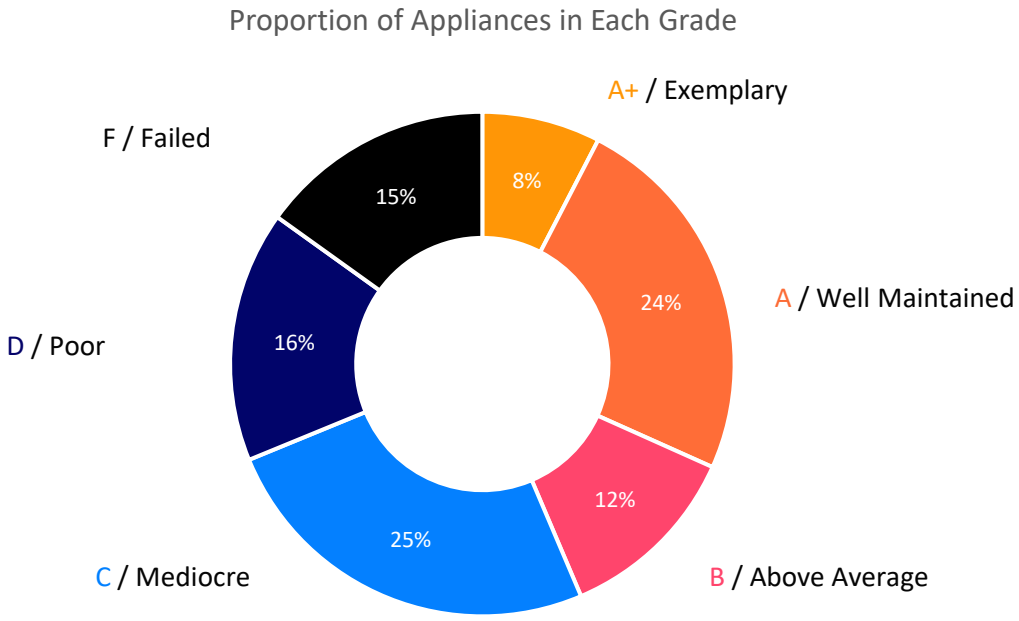
If a virtual appliance had no fixable vulnerabilities, and its operating system was currently maintained and supported, it would achieve a maximum score of 100. Of the 2,218 virtual appliances tested, only 4.6% (103) received this score.

A virtual appliance would receive an overall score of 0 if it had:

- an out-of-date (unsupported) operating system
- any four of 16 critical vulnerabilities as defined by Orca Security
- 20 or more vulnerabilities having a CVSS score of 9 or greater
- 100 or more vulnerabilities having a CVSS score between 7 – 9
- 400 or more unique vulnerabilities

The lowest recorded score was 6.

It would be impractical to report the results for all 2,218 virtual appliances tested within this document. For the full table of results, please visit https://orca.security/virtual-appliance-security-scores



An industry-wide wake-up call points to a safer future

Under the principle of Coordinated Vulnerability Disclosure, Orca Security researchers emailed each vendor directly, giving them the opportunity to fix their security issues.

This report has prompted the industry to move forward to a safer future. Of the 540 vendors contacted, 80 responded, with many confirming remedial action had been taken. 287 products have now been updated and 53 removed from distribution, leading to 36,938 discovered vulnerabilities being addressed (out of 401,571 total discovered vulnerabilities). The average score increase for updated products is 11, with the average grade rising from a B to an A. Here are a few examples of remedial actions taken as a result of this research:

- Dell EMC issued a critical security advisory for its CloudBoost Virtual Edition
- IBM updated or removed three of its virtual appliances within a week
- Zoho has updated half of its most vulnerable products
- Symantec removed three poorly scoring products
- Splunk, Oracle, IBM, and Cloudflare removed products
- Redis Labs had a product that scored an F due to an out-of-date operating system and many vulnerabilities; after an update it now scores an A+
- Cisco published 15 fixes to vulnerabilities found in Cisco vEdge Cloud Router

Some software vendors have yet to take responsibility for their virtual appliance vulnerabilities

Vendors in 32 cases said it was up to customers to patch virtual appliances. In 24 of them they claimed their virtual appliance vulnerabilities weren't exploitable and no action was needed. (We disagree; failure to remediate is bad practice as there may be future scenarios where a vulnerability becomes dangerous.) Some vendors threatened legal action. Many products remain in a neglected state.

Only 8% of software vendors achieved exemplary scores

Less than 8% of the virtual appliances were free of known vulnerabilities. High-scoring vendors with well-maintained products graded A+ or A included VMware's Bitnami, NVIDIA, HashiCorp, along with a handful of security vendors including BeyondTrust, Pulse Secure, Trend Micro, Barracuda Networks, and Versasec.

Both niche players and established brands had products with vulnerabilities

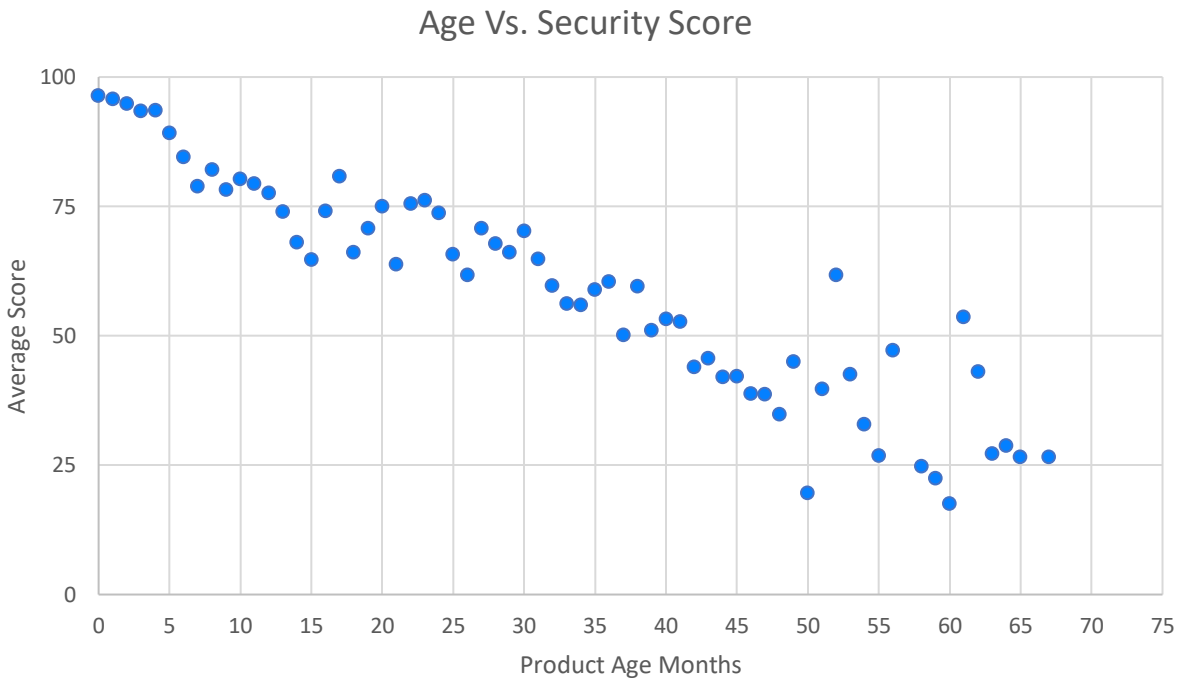
15% of the products were graded F, deemed to have failed the test. Not all were supplied by little-known vendors, although there were plenty of those. High-profile failures included products from CA Technologies, FireMon, A10 Networks, Cloudflare, Micro Focus, and Software AG.

For software vendors with multiple products, some vendors had products at both ends of the spectrum

We tested multiple images for 36% of the vendors; the grade varied for the majority.
Of all vendors, 4.8% had products at both ends of the spectrum, where disparate products were graded both A+/A and F. These included Intel, Symantec, Tibco, Zoho, and Cognosys.

Vulnerabilities accumulate as products age

Only 14% (312) of the tested virtual appliance images had been updated within the last three months, including ones from Barracuda Networks, InterSystems, NVIDIA, and Radware. 47% (1,049) hadn't been updated in the last year, including products from Oracle, Qualys, Symantec, CA Technologies, Cloudflare, and New Relic. 5% (110) had been neglected for at least three years, including products from Tufin and Unisys. The chart below shows that security scores fall as products age. Most vendors are not updating or discontinuing their outdated or end-of-life products.



More expensive doesn't mean more secure

Vendors charged an average of $0.3/hour for 67% (1,489) of the products, while 23% (510) were free to access—including many that are open source. About 10% (219) had a bring-your-own- license (BYOL) model. The average security score for free products was 77.58—slightly higher than fee-based products at 77.38. Those with a price higher than the median cost ($0.11/hour) had an average security score of 74.94; those below the median had 79.80 as their average.

Security vendors should know better

Virtual appliances are a common way to provide IT security functions such as firewalls and network encryption. Security products scored four points higher than the average at 83.0. However, failures still existed in the category, including products from A10 Networks, Symantec, FireMon, Cloudflare, and Tufin. Ironically, one vendor, Qualys (getting a grade of C)—itself a vulnerability scanning service provider—was shipping a 26-month-old appliance with a user enumeration vulnerability the vendor had discovered and reported to the industry in 2018. Qualys updated its solution following our security notice.

The Best and Worst Security Virtual Appliances		
Vendor	Product	Grade
Barracuda Networks	Barracuda Firewall Control Center (BYOL)	A+
BeyondTrust	BeyondInsight	
Trend Micro	Cloud Network Protection, protected by TippingPoint	
Versasec	vSec:CMS C-Series	
39 Products In-Between		
A10 Networks	A10 Lightning Application Delivery Controller	F
Cloudflare	Railgun™ WAN Optimizer	
FireMon	40Cloud Network Firewall (both BYOL and enterprise)	

What actions can IT security teams take to mitigate risk hiding inside software vendors' virtual appliances?

Simply because a vendor scores top marks doesn't mean all its virtual appliances are guaranteed to be risk-free. The data presented serves only as a guide, providing an idea as to how vendors approach the support and maintenance of their virtual appliances. Some scored well and deserve a measure of trust. Others have done badly, and their products should be approached with caution.

Your organization may use a specific virtual appliance tested in this report, but most of those in use aren't covered here—at least not every specific version you have installed.

Here are four steps your organization can take to reduce future risk from virtual appliances:

- Asset management can provide you with an understanding of the virtual appliances deployed across your organization's IT estate. This must include both internal platforms and the public cloud. Don't overlook informal deployments (shadow IT), as it's too easy for end users to access and deploy their own virtual appliances.

- Vulnerability management tools can discover virtual appliances and scan for known vulnerabilities and other security issues. Make sure the vulnerability management process in your organization scans all virtual appliances; you cannot assume they're safe to use as supplied by vendors.

- The vulnerability management process should prioritize actions to be taken by identifying the most severe vulnerabilities. In the short-term there are two choices: fix a product or immediately stop using it.

- In the longer-term for those appliances kept running, approach the respective vendors, understand their support process and how arising vulnerabilities are fixed—if at all. Seek an alternative if a given vendor's support processes are not satisfactory.

Orca Security is one vendor that can help your organization find and manage security problems for software deployed in AWS, Azure, and GCP—including virtual appliances.

The reason Orca Security was able to test the 2,218 virtual appliances covered in this report is that its SideScanning™ technology is able to scan stored images for problems with read-only access; it does not require any installation or maintenance of agents. If you would like to learn more about Orca Security and discover just how safe the virtual appliances installed across your public cloud really are, please https://info.orca.security/demo.

Background and Research Methodology

The ubiquitous virtual appliance

A computing appliance is a discrete combination of a single application and operating software. IT systems have long depended on appliances to carry out specific functions, for example network routing and security screening. In the past these were mostly sold as physical devices having their own dedicated hardware to be installed in data center racks alongside servers. Their numbers were limited by cost. The main motivator for this approach was to make use of specialized hardware or ensure a tight coupling of hardware, operating systems, and supported application software, rather than a mish-mash of these three components across deployments.

Virtualization enables this approach to be continued while improving economies of scale and dispensing with the need for dedicated hardware. This has led to a proliferation of inexpensive virtual appliances that are easily deployed within private or public cloud platforms. Virtual appliances eliminate the costs and complexities associated with configuring, tuning, securing, running, and maintaining complex stacks of software, as this should all be done by the vendor. As their customer, your either uses the images as provided or set a few parameters via some sort of user interface.

Virtualization means the barrier to entry for supplying appliances has been dramatically reduced, such that many small vendors have entered the market. This, along with poor processes by some well-established vendors, has led to most virtual appliances in use having significant security risks.

At the same time, customer cost for deploying appliances has plummeted, where you're often charged by the hour. Many are free to use, especially those that are open source. Other products have a bring-your-own-license (BYOL) model, where you might already have an in-house license that can be extended to off-premises use on public cloud platforms.

Appliances can be purchased directly from vendors or from their resellers. However, many are also available via marketplaces associated with major cloud platforms such as VMware, Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). It was from such marketplaces that Orca Security sourced the virtual appliances tested in this report, although in many cases they're the same products supplied directly by vendors.

Vulnerabilities as a proxy for virtual appliance hygiene

Vulnerabilities are errors discovered after software has been released. In a worst-case scenario, exploit code might be created that targets a vulnerability and enables attacks. Software suppliers provide patches for known vulnerabilities and emergency patches when necessary. However, the window for hackers is often left open for longer than it needs to be because, even when fixes are available, those responsible for applying them fail to do so.

Counting known vulnerabilities and their severity is a good proxy in assessing the overall hygiene of a virtual appliance. While most vulnerabilities are not exploitable, the best practice is to apply patches as soon as they're available to minimize risk in some future context. Failure to do so is indicative of poor practice. All of this equates to a virtual appliance bundled with hundreds of known vulnerabilities being a greater risk than one that ships with a few; it represents an ongoing risk to associated virtual machines (VMs) and other IT assets.

Vulnerabilities are classified using the industry-standard Common Vulnerability Scoring System (CVSS). CVSS assigns a severity score based on several metrics that include ease of use and possible impact, with scores ranging from 0 (no risk) to 10 (highest risk). Such scoring facilitates the prioritization of responses. The current CVSS v3.1 was released in June 2019.

A new vulnerability is also given a common vulnerabilities and exposures (CVE) number. For example, the Heartbleed exploit first seen in 2014 targets a vulnerability in the OpenSSL secure network socket and is known as CVE-2014-0160.

Research Methodology

This research was carried out using Orca Security's SideScanning™ technology—a SaaS tool—usually used to scan an organization's VM deployment en masse, including servers and virtual appliances. There is no need to install agents on the VMs or authenticate to them—neither of which are allowed by most virtual appliances. All that's required is read-only access to the stored images.

Orca SideScanning™ uncovers a wide range of risks, including vulnerabilities, misconfigurations, weak authentication, the risk of lateral movement, active infections, and insecure data. Thousands of risks might be listed, which are then prioritized for the IT security team's attention based on their deployment context.

For this research, Orca Security used SideScanning™ in a limited way to evaluate virtual appliances for only two things: vulnerabilities and to check if operating systems were up to date. No pre-configuration of virtual appliances was involved and there was no real operational context. The inherent limitations of using SideScanning™ in this way meant the product's ability to detect operational weaknesses wasn't used. Nevertheless, it let Orca Security quantify the security state of a wide range of virtual appliances and the diligence of the respective vendors.

Vendors had no prior knowledge of our research, and they ranged in size from the small and esoteric to the large and well-known. In each case Orca Security accessed the latest available revision of the virtual appliances and paid the least practical rate to do so. Where multiple versions existed, we tested each one.

Inclusion Criteria

During April and May Orca Security scanned 2,218 virtual appliances from 540 vendors, all products available for download from public marketplaces. The research was not selective, all source images were scanned. 63% (343) of the vendors had but one product, while 90% (490) had five or fewer. About 1% had more than 100, the most scanned images for a single vendor (Cognosys) being 293. These represented 13% of all the scans.

There were two grounds for not including a virtual appliance in the research. One was a prohibitively high cost, as a few vendors charge $100s per hour for access. The other was that a small number of products included unusual or highly customized operating systems, to a degree that general vulnerability databases do not apply.

Scoring Methodology

To quantify the results, each virtual appliance was assigned an overall security score between 0 – 100 based on five weighted parameters as seen in Table 1.The higher the CVSS scores of the vulnerabilities discovered the worst a virtual appliance was rated. Appendix-A lists 17 critical vulnerabilities selected for this research, the presence of which meant compromise was considered just a matter of time. All were high profile with well-known exploits such as Heartbleed, EternalBlue, and DirtyCOW.

Table 1: Scoring Method for SideScanning™ Vulnerability Results

Criterion	Weight	Criteria Scoring (out of 100)	Summary Results (2,218 appliances)
Operating System in/out-of-date	20%	100 pts. If currently supported and maintained, 0 if unsupported	11.4% (252) had an out-of-date operating system
17 Orca-defined critical vulnerabilities	30%	25 pts. Deducted for each discovered; 4 or more = 0	46% (1,022) had at least one; 1.1% (24) scored 0
Vulnerability having CVSS score of 9 or more	15%	5 pts. Deducted for each discovered; 20 or more = 0	61% (1,350) had such vulnerabilities; 1.6% (36) scored 0
Vulnerability having CVSS score between 7-9	5%	1 pts. Deducted for each discovered; 100 or more = 0	92% (2,043) had such vulnerabilities; 10.5% (232) scored 0
Overall unique vulnerabilities	30%	0.25 pts. Deducted for each discovered; 400 or more = 0 (all vulnerabilities from above also counted here)	95.3% (2,114) had such vulnerabilities; 9.5% (212) scored 0

In summary, and as previously noted in the executive summary:

If a virtual appliance had no fixable vulnerabilities, and its operating system was currently maintained and supported, it would achieve a maximum score of 100. Of the 2,218 virtual appliances tested, only 4.6% (103) received this score.

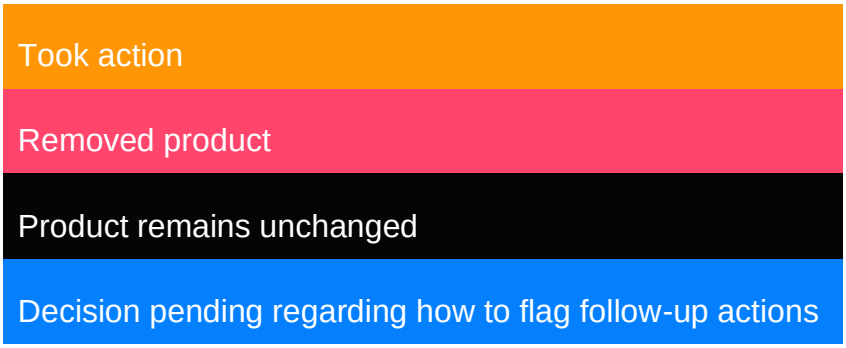
A virtual appliance would receive an overall score of 0 if it had:

- an out-of-date (unsupported) operating system
- any four of 16 critical vulnerabilities as defined by Orca Security
- 20 or more vulnerabilities having a CVSS score of 9 or greater
- 100 or more vulnerabilities having a CVSS score between 7 – 9
- 400 or more unique vulnerabilities

The lowest recorded score was 6.

Results and Analysis

Introduction



The Orca Security research team analyzed 2,218 virtual appliances using Orca's patent-pending SideScanning™ technology. Less than 8% of vendors had appliances that passed all the tests. This exemplary group includes Trend Micro, BeyondTrust, Pulse Secure, and Versasec.

15% of vendors had products so riddled with vulnerabilities that they were deemed to have failed. Companies in this group included tech stalwarts such as Intel, CA Technologies, Symantec, FireMon, A10 Networks, and Cloudflare. Qualys, itself a provider of a vulnerability scanning service, was distributing a 26-month-old appliance that included a severe user enumeration vulnerability it had itself discovered and reported in 2018.

The good news is that the report itself has started the process of moving the industry forward to a safer future. As a direct result of this research, the vendors responsible have reported back to Orca Security that 36,259 vulnerabilities have been removed from their appliances by patching or removing the product from distribution. Overall, 534 products have now been updated and 39 products removed from distribution (table 2).

However, there is much more to be done, many products remain in a neglected state.

Table 2: Vendors That Deleted Products	Number Removed
Actian	4
Alfresco Software	1
Axiomatics	
Buckhill	
CA Technologies	
Cloudflare	
Cloudify	2
Dataguise	1
Electric Cloud	
Encore Analytics	
Helpy.io	2
IBM	1
JSCAPE	
Loadbalancer.org	
Mapbox	
Mendix	3
MidVision Limited	2
NVIDIA	1
Opmantek	1
Oracle	
PYDIO	
SearchBlox Software	
South River Technologies	
Splunk	
Symantec	3
Tech Info Systems	1
Virtuozzo	3

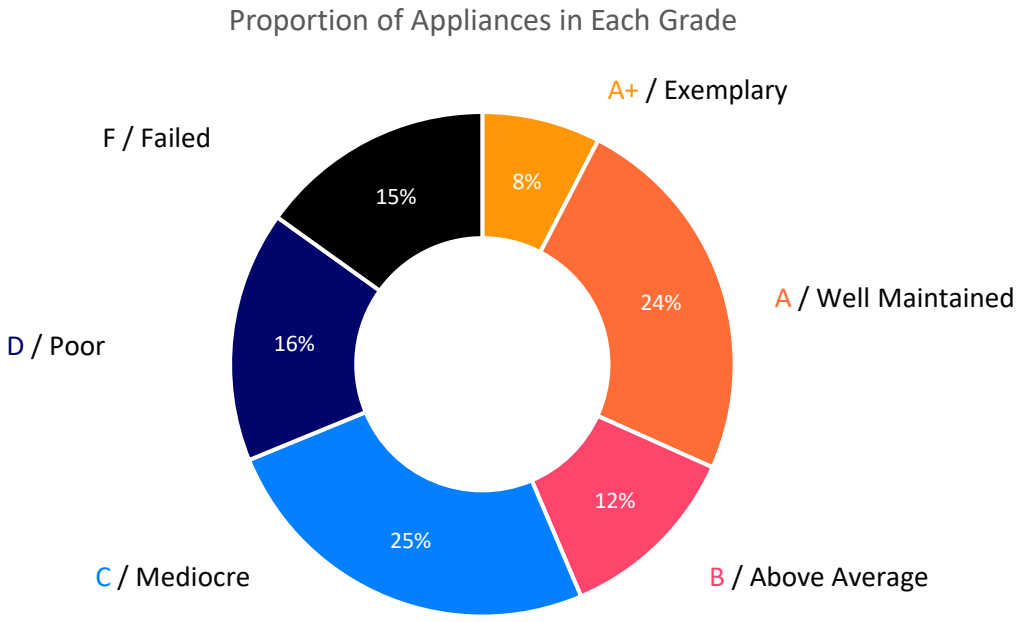
Scoring the security risk from virtual appliances

Software suppliers should make sure their products are well maintained and patches are provided as vulnerabilities are identified. This is not happening with many virtual appliances.

Each appliance tested was given a score between 0 and 100, based on criteria laid out earlier in table 1, the average overall score was 77.5. Based on its score each virtual appliance tested was given a grade as laid out in table 3.

Table 3: Grades Applied for Given Security Scores

Grade	Min. Grade Score	Description	No. of Virtual Appliances in Grade	Avg. Image Age (months)
A+	99.75	Exemplary	169	1.7
A	92	Well Maintained	534	5.6
B	85	Above Average	264	10.6
C	70	Mediocre	559	13.7
D	55	Poor	357	19.0
F	Below 55	Failed	335	32.5
Overall			**2,218**	**13.7**



Scoring the security risk from virtual appliances

Less than 8% of the tested virtual appliances were found to be free from known vulnerabilities. High-scoring vendors having well-maintained products included VMware's Bitnami, NVIDIA, HashiCorp, and a handful of security vendors including BeyondTrust, Pulse Secure, Trend Micro, Barracuda Networks, and Versasec. At the other end of the spectrum, around 15% of the virtual appliances were full of known vulnerabilities and failed the test. This set wasn't all furnished by little known vendors, although there were plenty of those. Failures included CA Technologies, Intel, Micro Focus, Software AG, and Zoho. Some, including Intel, Symantec, and Tibco Software had products at both ends of the spectrum. Full results are available here: https://orca.security/virtual-appliance-security-scores

The following are examples of virtual appliances tested in each of the defined grades:

Scoring A+ (exemplary)

BeyondInsight by BeyondTrust, version 3.2 UVM 3.2.0 BI 6.9.0, supported operating system, no known vulnerabilities found.

TensorFlow from NVIDIA AMI, version 20.03.1, running on Ubuntu 18.04; operating system has years of support left; one fixable vulnerability found

Scoring A (well maintained)

HashiCorp Vault OSS, version vault-1.3.2-20200129.01; supported operating system, 41 known vulnerabilities (six with a CVSS score of 7 – 9. HashiCorp issued a fixed version following Orca's notification.

Scoring B (above average)

OpenVPN Access Server (500 connected devices) version 2.7.5; supported operating system, 113 known vulnerabilities (28 with a CVSS of 7 – 9. OpenVPN issued an updated version following Orca notification, subsequently resulting in an 'A' score.

Scoring C (mediocre)

Qualys Virtual Firewall Appliance HVM version Qualys-WAF-AWS-1.4.0 running Centos 6.9; supported operating system, 99 known vulnerabilities (33 graded CVSS 7 – 9, with one over 9). These included CVE-2018-15473, an exploitable vulnerability discovered by Qualys as early as April 2018, but with no update since March of that same year. Qualys did update its solution following our notification.

Dell EMC CloudBoost Virtual Edition, version 19.2, included 276 vulnerabilities (48 with a CVSS score of 7 – 9 and 5 scoring over 9). These included Apache PE vulnerability CVE-2019-0211 and SQLite RCE vulnerability CVE-2017-2520. Dell acted on Orca Security's report by issuing a critical security advisory DSA-2020-180.

Scoring D (poor)

Symantec Protection Engine for Cloud Services on Linux (BYOL), version 8.0.0; 323 vulnerabilities (79 with a CVSS score between 7 – 9, four with a score over 9). These include CVE-2018-15473, an unauthenticated user enumeration vulnerability in OpenSSH. Symantec removed the product from distribution following Orca Security's notification.

Scoring F (failed)

Redis Enterprise Software (RS) versions 5.4.6-18 suffered from 299 unique vulnerabilities. Three scored over 9 and included critical vulnerabilities such as DirtyCOW, all the while running an out-of-support OS. Following our notification Redis has updated the image; its new version runs on the more modern Red Hat 7.8 OS and has no critical vulnerabilities, thereby earning it an A+.

Symantec Control Compliance Suite – BYOL 11.1 included 700 vulnerabilities, of which 11 had a CVSS score over 9. These included critical ones with exploits such as DejaBlue. It allows remote code execution and CVE-2019-1388, a simple-to-execute privilege escalation in the Windows Certificate Dialog. The image had last been updated in January 2016. Symantec removed the product from the marketplace following Orca Security's notification.

Vendors with virtual appliances at both ends of the spectrum

For 37% (197) of vendors for which multiple scans were undertaken, 84 had a consistent grade across their products, while grades varied for 113. 5% (28) of vendors had products graded both A+/A and F (see table 5).

Table 5: Inconsistent practices - vendors with both high and low grades

Vendor name	Max grade	Min grade	# of virtual appliances tested
Aurora	A	F	17
BL King Consulting LLC	A	F	4
clckwrk Ltd	A	F	94
Code Creator	A	F	19
Cognosys Inc.	A+	F	293
CubeBackup Inc.	A	F	3
ESRI	A	F	11
Installatron LLC	A+	F	14
Intel	A	F	2
Intuz	A	F	86
Jetware	A	F	131
Kurian	A	F	8
Loadbalancer.org, Inc.	A	F	2
MidVision Limited	A+	F	8
Miri Infotech	A	F	133
Pragmatic Techsoft Pvt Ltd	A	F	5
Rogue Wave Software	A	F	12
SmartAMI	A	F	7
StarWind	A	F	7
Symantec Corporation	A	F	4
Technology Innovation Lab of Texas	A	F	6
Technology Leadership Corporation	A	F	12
The Globalsolutions	A	F	45
TIBCO Software Inc.	A+	F	5
TurnKey GNU/Linux	A	F	104
Xilinx	A	F	3
zCost Management	A	F	4
ZOHO Corporation Private Limited	A	F	18

IT Security Vendors

Virtual appliances are a common way to provide IT security functions such as firewalls, secure gateways, and encryption. Overall, it was somewhat reassuring that security products scored four points higher than the average at 83.0. However, there were still failures in this category, including products from A10 Networks, Symantec, FireMon, Cloudflare, and Tufin.

Table 3 lists 27 security vendors whose products were tested, along with grades achieved by each.

Table 3: Security vendors - summary results

Vendor	# of products tested	Min grade	Max grade	Avg product age
A10 Networks	1	F	F	21
Barracuda Networks, Inc.	1	A+	A+	1
BeyondTrust	1	A+	A+	4
CloudFlare Inc.	1	F	F	51
Cohesive Networks	1	B	B	2
Device42	2	D	D	6
Firemon	2	D	F	29
Fortinet Inc.	1	C	C	1
GuardiCore	1	A	A	7
HailBytes	1	B	B	7
HyTrust, Inc.	2	A	A	2
Juniper Networks	1	C	C	30
Kali Linux	1	A	A	3
Kaspersky Lab	1	C	C	11
Lastline, Inc.	2	A	C	4
McAfee	1	C	C	6
OpenVPN Inc	7	A	B	8
OPSWAT	1	A	A	0
Preempt Security, Inc.	1	C	C	3
Qualys, Inc.	1	C	C	26
Radware	4	C	D	1
SAS Institute, Inc.	1	D	D	16
Symantec Corporation	4	A	D	25
Trend Micro	1	A+	A+	4
Tufin	1	C	C	43
Versasec	1	A+	A+	0
Zscaler	1	C	C	9

Hardened Appliances

Hardened virtual appliances are those having stripped-down operating software that minimizes their attack surface. As might be expected, collectively these had a high average score of 94.2. Leading in this class were Nemu Corporation and the Center for Internet Security both averaging A grades, whilst Faro Source and Frontline trailed averaging C. These may not be well-known names, but they set an example for others to follow.

Application Stack Integrators

52% (1,171) of the tested products were provided by 18 application stack integrators (an average of 65 images per vendor). Their virtual appliances are self-sufficient software stacks running popular open source programs (e.g., WordPress packaged with Apache web server, MySQL database, and the OpenSSL secure network library). This group's average score was 77.6—close to the overall average. But as table 6 shows, all have product versions that scored A or A+ while most also had failures. The most consistently high-scoring vendors were VMware Bitnami, ProComputers.com, and AppXen.

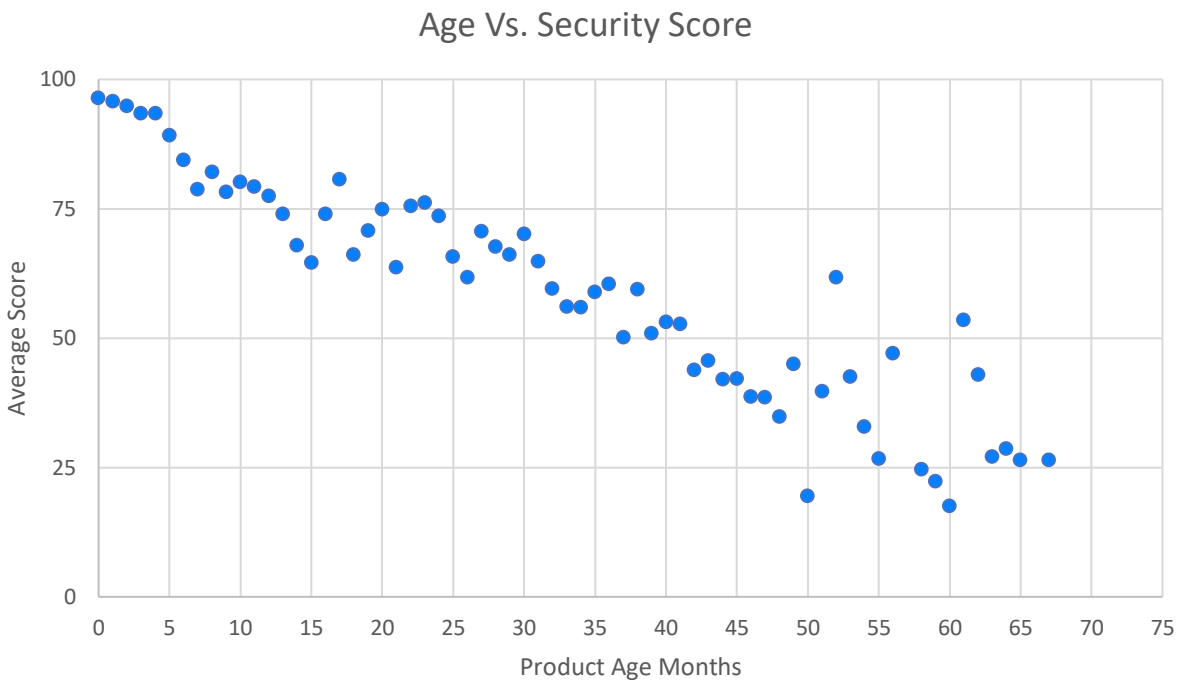
Table 4: Application stack vendors

Vendor	# of images scanned	Max grade	Min grade	Avg image age
AppXen	8	A	A	3
ProComputers.com	10	A+	A	2
Bitnami	115	A+	B	1
aMiSTACX	29	A	D	5
Websoft9	30	A	D	5
Cloudmint	36	A+	D	3
ZOHO Corporation Private Limited	18	A	F	13
Aurora	17	A	F	20
clckwrk Ltd	94	A	F	15
Code Creator	19	A	F	16
Intuz	86	A	F	14
Jetware	131	A	F	32
Kurian	8	A	F	25
Miri Infotech	133	A	F	24
Technology Leadership Corporation	12	A	F	24
TurnKey GNU/Linux	104	A	F	17
Cognosys Inc.	293	A+	F	7
The Globalsolutions	45	A+	F	6

The problem of out-of-date virtual appliances

Unsurprisingly, Graph 2 shows that known vulnerabilities accumulate as products age. When a virtual appliance is updated (to fix vulnerabilities, for example), its age is reset to the time of the update.

The average age of virtual appliances scanned for this report was 13.7 months. Only 2.8% (64) had been updated within the past month. 14% (312) had been updated within the last three months, including products from Barracuda Networks, InterSystems, NVIDIA, and Radware.



47% (1,049) had not been updated in the past year. These included products from Oracle, Symantec, CA Technologies, Cloudflare, and New Relic. Qualys, itself a provider of a vulnerability scanning service, was distributing a 26-month-old appliance, with a critical vulnerability (CVE-2018-15473) Qualys itself had discovered and reported in 2018. 5% (110) of virtual appliances had been neglected for at least three years, including offerings from Tufin and Unisys.

11% of products had out-of-date operating systems; on average, this set of virtual appliances were about three times older than those that were up-to-date. Astonishingly, Cognosys had 45 appliances running Windows Server 2008.

Poor processes account for the product age problem in many cases. Out-of-date products remain available after they've reached their end-of-life. The overall product is no longer supported, the operating systems may be unsupported, and/or updates and patches are no longer being applied. As a result of Orca Security's research, 39 products have been removed from distribution—including three by Symantec along with others from Splunk, Oracle, IBM, and Cloudflare.

What is your organization paying for with virtual appliances?

Charges for 67% (1,489) of the tested products were assessed by vendors at an average cost of $0.3/hour. The maximum for appliances tested in this report was $3.00/hour. 23% (510) of products were free, including most of the open source ones. Around 10% (219) used a BYOL model.

More expensive does not necessarily equate to more secure. The average overall security score for free products was 77.58, slightly higher than charged-for products at 77.38. BYOL products came in higher at 78.52.

The median cost of charged-for products was $0.11/hour: those with a price higher than the median had an average security score of 74.94, while those lower than the median price scored below 79.80. So it would seem that when it comes to security offered by virtual appliances, less expensive is better.

The vendor response

Each of the 540 vendors covered by this report was contacted by email for each of the 2,218 virtual appliances we tested. We received 80 responses that ranged from polite, professional, and grateful all the way down to derogatory.

There were many positive interactions. Larger vendors generally took the results seriously—Cisco, Intel, Dell, IBM, TrendMicro, and Qualys being among these. One smaller vendor, HailBytes, took the time to record a personalized thank you video.

Dell-EMC issued a critical security advisory for its CloudBoost Virtual Edition as part of its response. IBM updated or removed three of its virtual appliances within a week, and asked Orca Security to initiate further scans of Linux images its Red Hat subsidiary provides on public cloud marketplaces. Zoho requested a meeting to discuss recommendations for acting on its related findings; half of the products concerned had been updated within about a month. Four Symantec products were scanned for the test: one scored an A, a second a D, and two failed (scoring an F). Distribution of the three poor-scoring products was ended.

On the negative side, in 24 cases vendors claimed their analysis showed that the vulnerabilities in their virtual appliances are not exploitable and no action is needed. (Along with many others, Orca Security maintains that failure to remediate is bad practice. While a vulnerability may not be directly exploitable today, it may be in the future as part of a new exploit.) 6% (32) of vendors said it was the customer's responsibility to patch vulnerabilities in their products. A few vendors threatened legal action.

The rescanning of virtual appliances

Many vendors acted on the information sent to them. To date, 53 products from 31 vendors have been deemed to have reached end-of-life and have been removed from distribution. A further 287 products have been updated, in many cases the vendor having informed Orca Security of the changes it made.

In the interest of fair reporting, a rescanning exercise was undertaken. In some cases, products that were initially marked as failures (F) are now scoring A or A+. Otherwise, the average score increase for updated products is 11 points, with the average grade rising from B to A. For example, Redis Labs had a product with an out-of-date operating system and many known vulnerabilities that originally received an F; after updating it now scores A+.

Critical vulnerabilities

For the purposes of this research, Orca Security identified 17 critical vulnerabilities deemed to have serious implications if found unaddressed in a virtual appliance. Easily obtainable and usable by the most amateur of hackers, exploits are available for all of these. 13 of them are associated with well-publicized and named exploits/attacks. A well-conducted vulnerability management process should not overlook any of them.

EternalBlue is a remote code execution exploit in Windows Remote Desktop Protocol (RDP). It was originally developed by the US National Security Agency and leaked in April of 2017 by the Shadow Brokers hacking group. It has been widely used in cyberattacks, including the infamous WannaCry ransomware and NotPetya encrypting ("disk-wiper") malware in 2017.

Four vulnerabilities are commonly exploited by EternalBlue:

CVE-2017-0144, CVSS score 8.1

CVE-2017-0143, CVSS score 8.1

CVE-2017-0146, CVSS score 8.1

CVE-2017-0147, CVSS score 5.9

Actian's DataConnect Studio IDE was an example of a virtual appliance vulnerable to EternalBlue. Once we contacted Actian, it promptly removed the product from distribution.

Like EternalBlue, **DejaBlue** and **BlueKeep** are remote code execution exploits targeting vulnerabilities in Windows RDP. Discovered in 2019, they can act as worms, multiplying and spreading across computer systems. Neither have yet been confirmed to have played a part in a major attack. In September of 2019, the penetration testing project Metasploit released a module for these exploits, making their use fairly simple.

Four vulnerabilities are commonly exploited by DejaBlue/BlueKeep:

CVE-2019-1181, CVSS score 9.8

CVE-2019-1182, CVSS score 9.8

CVE-2019-1222, CVSS score 9.8

CVE-2019-0708, CVSS score 9.8

Symantec's Symantec Control Compliance Suite – BYOL was vulnerable to CVE-2019-1181. After we alerted the company of the issue, Symantec chose to remove this offering from distribution.

DirtyCOW or Dirty Copy-On-Write is a privilege escalation exploit found in 2014 that affects all Linux kernel versions prior to V4.8.3. It allows any user having access to the operating system to gain root access. Versions of the exploit can be found on GitHub and Metasploit, thereby making it easy to access and use.

The vulnerability exploited by DirtyCow is:

CVE-2016-5195, CVSS score 7.8

Orca Security's scan shows the Unisys Stealth (cloud) Upgrade System is vulnerable to this exploit. The instructions do say the product should be terminated once an upgrade has been applied. But it's not uncommon for such virtual appliances to be forgotten and remain within a company's IT estate. The product remains available and unpatched.

Heartbleed is a buffer over-read exploit. It gained notoriety in 2014 for providing read access to any web server using the OpenSSL cryptography library.

Its vulnerability exploit is:

CVE-2014-0160, CVSS score 7.5

With Heartbleed being an old vulnerability, we didn't expect to find products vulnerable to it. But Datagres Technologies' PerfAccel Appliance is susceptible. The vendor didn't respond when contacted on Aug 17th and, when last checked, its website appeared to be down.

Apache Struts is an open source web application framework for Apache, one of the most popular web servers. Exploits for critical vulnerabilities in the framework are freely available and commonly used; one example is the 2017 Equifax breach and subsequent data leak.

Commonly used vulnerabilities are:

CVE-2017-5638, CVSS score 10.0

CVE-2018-11776, CVSS score 8.1

CVE-2019-0232, CVSS score 8.1

Not many vendors deployed Struts, but Jamcracker's Hybrid Cloud Management was found to be vulnerable to CVE-2017-5638. Most of Jamcracker's offerings are no longer available, but this one still is.

Additional vulnerabilities

Privilege escalation vulnerability in Windows Certificate Dialog:

CVE-2019-1388, CVSS score 7.8

User enumeration vulnerability in OpenSSH:

CVE-2018-15473, CVSS score 5.3

Privilege escalation vulnerabilities in the Linux kernel:

CVE-2016-0728, CVSS score 7.8

CVE-2013-2094, CVSS score not available, being reevaluated

About Orca Security

Orca Security is the cloud security innovation leader, providing instant-on, workload-level security and visibility for AWS, Azure, and GCP — without the gaps in coverage and operational costs of agents.

Delivered as SaaS, Orca Security's patent-pending SideScanning™ technology reads your cloud configuration and workloads' runtime block storage out-of-band, detecting vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords, and unsecured PII.

Orca Security deploys in minutes - not months - because no opcode runs within your cloud environment. With Orca, there are no overlooked assets, no DevOps headaches, and no performance hits on live environments.

And unlike legacy tools that operate in silos, Orca treats your cloud as an interconnected web of assets, prioritizing risk based on environmental context. This does away with thousands of meaningless security alerts to provide just the critical few that matter, along with their precise path to remediation.

Connect your first cloud account in minutes and see for yourself. Visit https://orca.security

Acknowledgments

Thank you to Anindya Chakraberti of Millennium Partners, who inspired this research.