Orca Security 2020 State of Virtual Appliance Security

How responsible are your software vendors?

orca security

BREADTH OF ANALYSIS

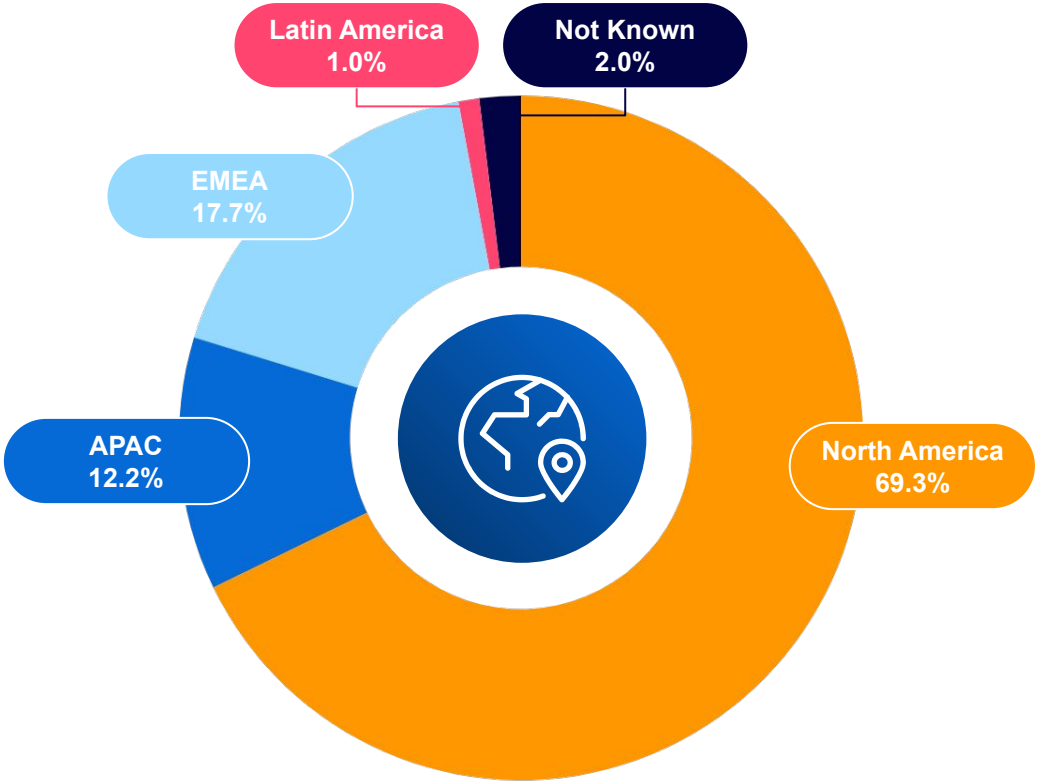
Software vendors are often distributing their wares on virtual appliances with exploitable and fixable vulnerabilities. The study analyzed:

2,218 virtual appliance images

from **540** software vendors

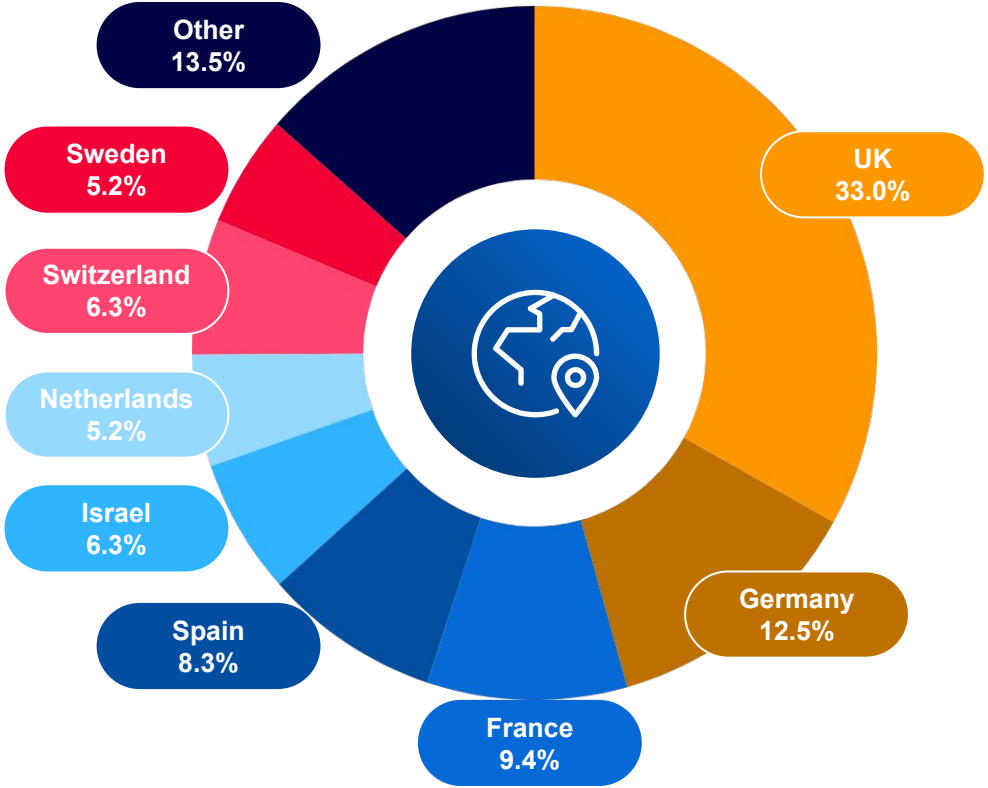
Finding **401,571** vulnerabilities

SOFTWARE VENDORS BY GLOBAL HQ



EMEA

Europe Middle East & African Countries



SECURITY PRACTICES VARIED AMONG GERMAN SOFTWARE VENDORS

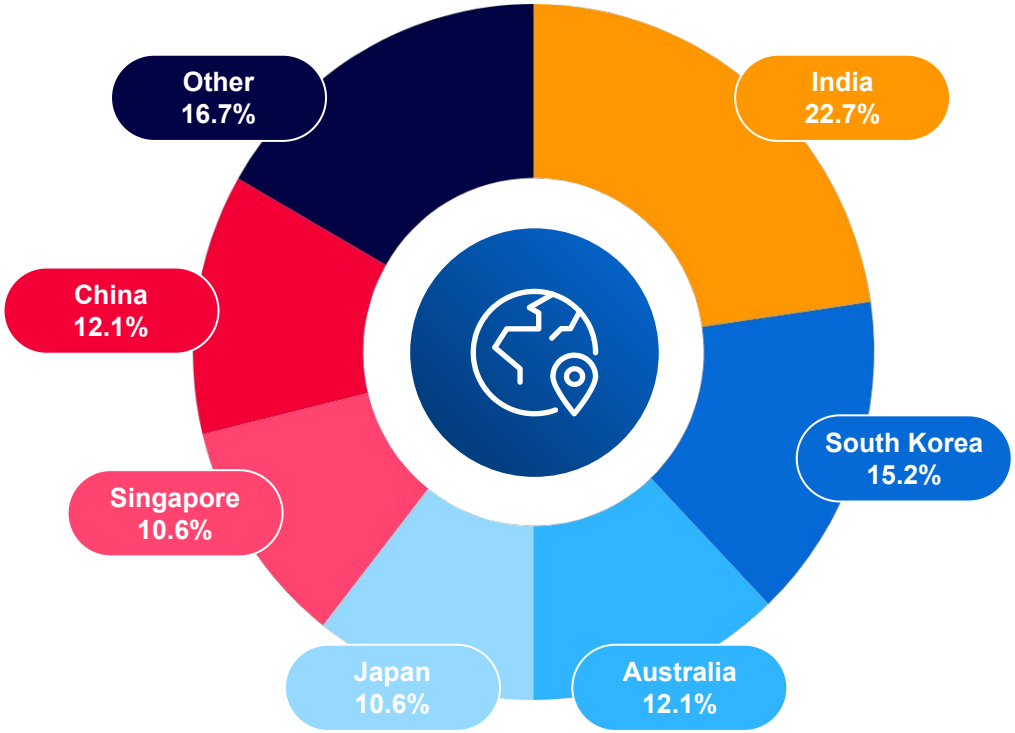
TE-SYSTEMS Inc. and metaphacts GmbH earned 'A+' grades. They routinely publish product updates in accordance with best practices.

In contrast, farfos and Software AG both ranked very low. Of the two frafos' products examined, both had not been updated in at least two years. Similarly, Software AG's product got an 'F' due to hundreds of known vulnerabilities detected, and the product has now been removed from distribution.

Seller Name	Product Name	Product Version	Solution age - Months	Unique CVEs Score	Critical CVE Score	CVSS 7-9 Score	CVSS Over 9 Score	OS Score	Final Score	Corrective Measure
Archiware Software GmbH	Archiware P5 Archive & Backup Free Trial & BYOL Edition	Archiware P5 Version 6.0.0	1	B	A+	B	A+	A+	A	Updated
Cloudplan	cloudplan Private Cloud Node Server	cloudplan PCN for Ubuntu 16.04	32	B	A+	B	A+	A+	A	
DW applications	nimbleBI AWS AMI	nbi_ami_1.0.0	31	D	C	C	A	A+	C	
flonatel	rmtoo	24.3.0	30	F	C	F	D	A+	F	
frafos	Monitor for ABC SBC (free AMI, required paid-AMI frafos ABC SBC)	4.0-002	30	F	C	F	D	A+	F	
frafos	VoIP Session Border Controller (SBC) with WebRTC Gateway (PAID AMI)	4.0-003	28	F	C	F	C	A+	F	
MainConcept	MainConcept 2GO AAC Audio Converter AMI	2.1	6	A	A+	B	B	A+	A	
metaphacts GmbH	MainConcept 2GO AAC Audio Converter AMI	2.1	6	A	A+	B	B	A+	A	
Michael Fleck	Puppeteer Browser Automation on Headless Ubuntu	Puppeteer on Headless Ubuntu v1	7	C	A+	C	A+	A+	A	Updated
Michael Fleck	Puppeteer Browser Automation on Windows	June 2020	0	B	A+	C	A+	A+	A	
Michael Fleck	Selenium Webdriver on Headless Ubuntu	v1.2	2	A	A+	A	A+	A+	A	Updated
Michael Fleck	Selenium Webdriver on Windows	June 2020	0	B	A+	C	A+	A+	A	
Michael Fleck	Ubuntu GUI (18.04 LTS)	Ubuntu GUI (18.04 LTS) v1	3	B	A+	A	A+	A+	A	Updated
Michael Fleck	Puppeteer Browser Automation on Graphical Ubuntu	Puppeteer on Graphical Ubuntu v1	7	F	A+	F	B	A+	C	Updated
netCubed	Ubuntu Linux Desktop	v1.3.2	1	A	A+	A	A	A+	A	Updated
netCubed	Ubuntu 19.10 Desktop and Analytics Workbench	v1.3.2	1	A+	A+	A+	A+	A+	A+	Updated
netCubed	ML Workbench for TensorFlow	v1.3.2	4	F	A+	F	D	A+	C	Updated
netCubed	Machine Learning Workbench	v1.2.2	9	F	A+	F	D	A+	D	Updated
RapidBusinessModeling	Detailed Business-Modeling Customer-Profitability-Analysis & Improvement	RBM4	0	A	A+	A	A+	A+	A	Updated
Software AG	ARIS Process Mining	10.4	9	F	F	D	B	A+	F	Removed
TE-SYSTEMS Inc.	anynode - The Software SBC (VM)	anynode (v3.16.16) - debian 9.6	1	A+	A+	A+	A+	A+	A+	Updated

APAC

Asian Pacific Countries



SECURITY PRACTICES VARIED AMONG AUSTRALIAN SOFTWARE VENDORS

We scanned four Schams.net products, which ranked from an 'A' grade to a 'D' grade. In response, they not only patched the vulnerabilities we mentioned but also included a new automatic updates mechanism to their new product. Inspired Corporation ranked an 'F' grade and removed their product, while openQRM Enterprise ranked an 'F' grade and their product remains available and unchanged.

Seller Name	Product Name	Product Version	Solution age - Months	Unique CVEs Score	Critical CVE Score	CVSS 7-9 Score	CVSS Over 9 Score	OS Score	Final Score	Corrective Measure
Bryte Systems	BryteFlow Enterprise Edition-Data Integration S3, Redshift, Snowflake	V 2.0.2	V 2.0.2	C	C	F	B	A+	C	
Buddy	Buddy - One-click delivery automation for Web Developers	v2.2.11	v2.2.11	B	A+	A	A+	A+	A	
Inspired Corporation	S3 Parallel Data Migration Tool	1	1	F	F	F	B	A+	F	Removed
Last Bastion Network Pty Ltd	Grafana Monitoring	6.5.3	6.5.3	A	A+	A	A+	A+	A+	
Last Bastion Network Pty Ltd	Zenoss 4	4.2.5*	4.2.5*	A+	A+	A+	A+	F	C	
openQRM Enterprise	openQRM Enterprise Amazon Edition	5.2.15	5.2.15	F	C	F	F	A+	F	
schams.net	TYPO3 CMS 10.x	10.3.0a	10.3.0a	A+	A+	A+	A+	A+	A+	Updated
schams.net	TYPO3 CMS 7.x	7.6.32a LTS	7.6.32a LTS	F	A+	F	B	A+	C	Updated
schams.net	TYPO3 CMS 8.x	8.7.30a LTS	8.7.30a LTS	F	A+	F	C	A+	D	Updated
schams.net	TYPO3 CMS 9.x	9.5.13a LTS	9.5.13a LTS	F	A+	F	C	A+	D	Updated
SigmoData	Deep Learning Notebook (Python 3, Tensorflow 2, Pytorch 1.3)	4	4	A+	A+	A+	A+	A+	A+	Updated
Yellowfin	Yellowfin 8.0.3 for AWS (12 Month, 3 User Free then BYOL)	8.0.3	8.0.3	C	C	C	C	A+	C	Updated

SECURITY PRACTICES VARIED AMONG JAPANESE SOFTWARE VENDORS

All three DigitalCube Co. Ltd products ranked an 'A+'. Similarly, Trend Micro's product also earned an 'A+'. Of the two SIOS Technology Corp. products, both ranked a 'C' grade despite their relative newness, the solutions' age being merely 3 month old.

Seller Name	Product Name	Product Version	Solution age - Months	Unique CVEs Score	Critical CVE Score	CVSS 7-9 Score	CVSS Over 9 Score	OS Score	Final Score	Corrective Measure
DigitalCube Co. Ltd	WooCommerce powered by AMIMOTO	6.1	1	A	A+	A+	A+	A+	A+	Updated
DigitalCube Co. Ltd	WooCommerce powered by AMIMOTO (Apache)	6.1	1	A	A+	A+	A+	A+	A+	Updated
DigitalCube Co. Ltd	WordPress powered by AMIMOTO (Apache)	6.1	1	A	A+	A+	A+	A+	A+	Updated
N2SM	N2 Search	10.3.0	41	F	C	D	A	F	F	
NRI	mPLAT Suite - Multi-Cloud Conductor	2018.0.0	21	D	F	F	D	A+	D	
Passlogy, Co.,LTD	PassLogic Enterprise Edition for AWS (BYOL)	4.2.0	7	D	A+	D	A+	A+	B	
Prime Strategy Co.,Ltd.	KUSANAGI for AWS (WordPress)	8.0.7	34	F	C	F	D	A+	F	
SIOS Technology Corp.	SIOS Protection Suite for Linux on RHEL	SPS-L 9.4.1 on RHEL 7.7	3	F	A+	F	A	A+	C	
SIOS Technology Corp.	SIOS Protection Suite for Linux on RHEL - BYOL	SPS-L 9.4.1 on RHEL 7.7	3	F	A+	F	A	A+	C	
Trend Micro	Cloud Network Protection powered by TippingPoint (BYOL)	5.3.0.10254	4	A+	A+	A+	A+	A+	A+	

SECURITY PRACTICES VARIED AMONG SINGAPORE SOFTWARE VENDORS

5 out of 7 Singapore-based sellers ranked an 'A' grade, among them Qtum and Zilliqa Research Pte Ltd. However, Fabrix got a 'D' score for a virtual appliance image that was created in 2016, and appears to have not been updated since.

Seller Name	Product Name	Product Version	Solution age - Months	Unique CVEs Score	Critical CVE Score	CVSS 7-9 Score	CVSS Over 9 Score	OS Score	Final Score	Corrective Measure
Fabrix	Fabrix Data Visualization for Splunk	2.1.0	41	F	C	D	A+	F	D	
NKN.org	NKN Full Node	1.2	7	B	A+	B	A+	A+	A	
ontology	ONT_Dev_Platform	2	17	F	C	F	C	A+	D	
PCHAIN	pchain client	1.0.23	11	A	A+	A	A+	A+	A	
QTum	Qtum AMI	Qtum AMI 3.1	7	B	A+	B	A+	A+	A	Updated
The Oxchild Pte.Ltd.	APIS Preloaded AMI 2019-Mar-001	APIS Preloaded AMI 2019-Mar-001	14	B	A+	B	A+	A+	A	
Zilliqa Research Pte Ltd	Zilliqa blockchain consensus node	v5.0.1	8	B	A+	B	A+	A+	A	

KNOWN VULNERABILITIES RUN RAMPANT

8%

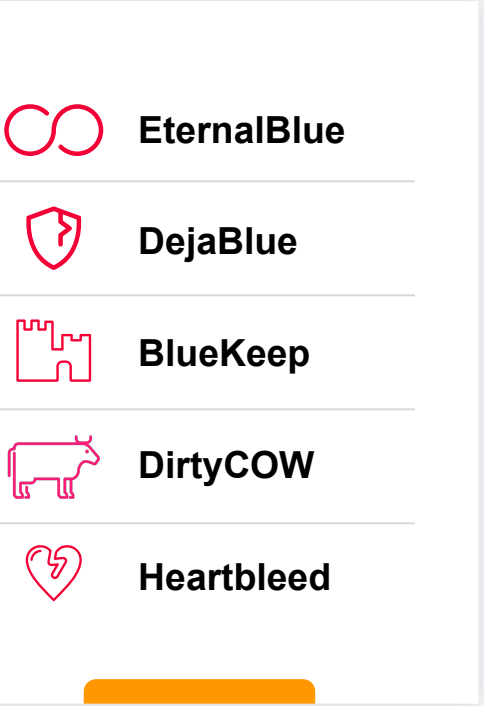
Only 8 percent of virtual appliances were free of known vulnerabilities

56%

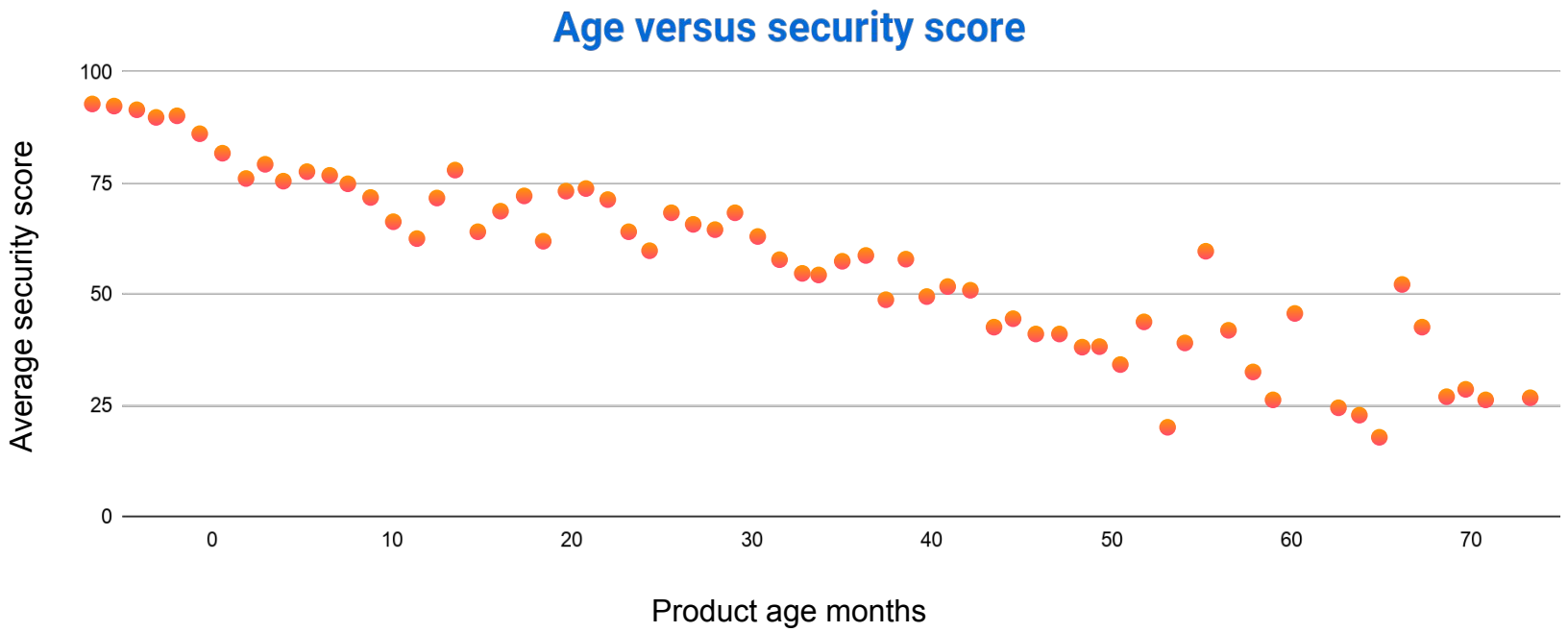
of products received a failed (F), mediocre (C), or poor (D) rating

17

critical vulnerabilities found



SECURITY SCORES FALL AS PRODUCTS AGE



LACK OF RECENT UPDATES AND OLD OPERATING SYSTEMS

of virtual appliances had not been updated within the last year

hadn’t been updated for at least three years, or were running on out of date or EOL (end of life) operating systems

SECURITY VENDORS SHOULD KNOW BETTER

Security products scored four points higher than the average at 83.0. However, failures still existed in the category.

The Best and Worst Security Virtual Appliances

Vendor	Product	Grade
Barracuda Networks	Barracuda Firewall Control Center (BYOL)	A+
BeyondTrust	BeyondInsight	
TrendMicro	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	30Cloud Network Firewall (both BYOL and enterprise)	

TOWARD A SAFER FUTURE

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

287
products have been updated

53
products removed from distribution

36,938
vulnerabilities have been addressed

Average increase in scores went from a B to an A

B → A

4 KEY
RECOMMENDATIONS

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

01

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.

02

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.

03

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.

04

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.

ABOUT THE REPORT

The Orca Security 2020 State of Virtual Appliance Security Report was a wide-reaching research and testing project to benchmark the current state of virtual appliance security. Between April 20 and May 20, 2020, Orca Security scanned 2,218 virtual appliance images from 540 security vendors for known vulnerabilities and other risks to provide an objective assessment score and ranking.

Report Resources

Read the blog post

Download the full report with detailed rankings and research findings

Register for the webinar with 451 Research or watch it on demand

See the full list of 2,218 products, scores, and actions taken by their suppliers

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