orca security

HEALTH CARE

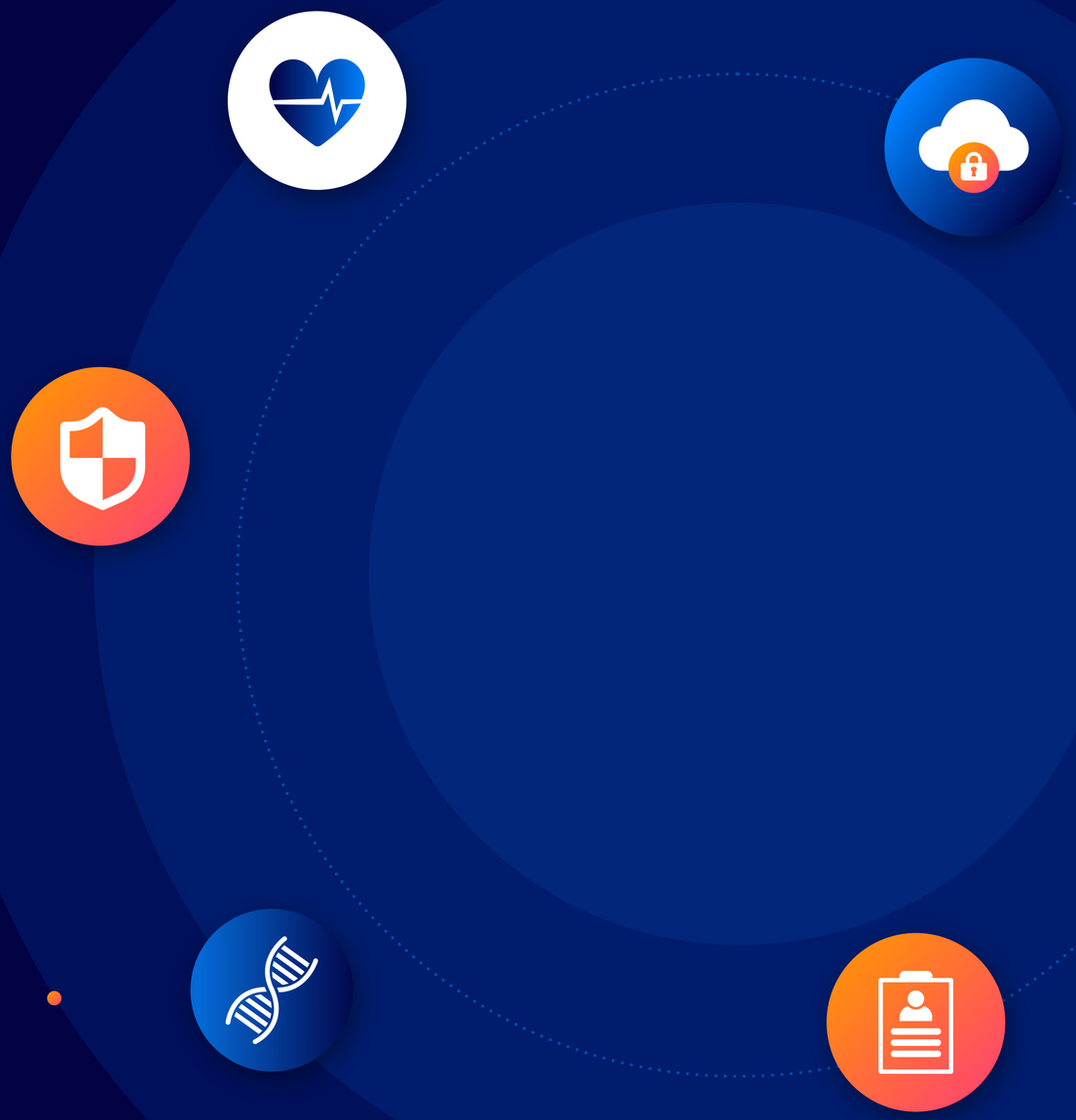
Cybersecurity for Healthcare Services and Technology



aws PARTNER

Cybersecurity for Healthcare Services and Technology

Cybersecurity in healthcare is vital to protecting electronic information and assets from unauthorized access, use, or disclosure, especially as organizations migrate sensitive data and critical applications to the cloud. Learn how comprehensive cloud security enables the delivery of cloud-driven care that is secure and compliant without impacting performance or patient confidentiality.



Digital Transformation in Healthcare and Healthtech

The future of healthcare organizations will rely on increasingly leveraging cloud technology to enhance personalized care. According to the BDO 2021 Healthcare Digital Transformation Survey, 78% of respondents said their organizations had deployed cloud technology, and 20% said they were planning to do so.[1]

The security of your health cloud environment needs to be a top priority. Continued migration of business-critical applications from on-site operations to cloud environments is impacting how teams collaborate and how decisions are made, enabling data-driven medicine while decreasing the cost of care.

The power of the cloud for healthcare and the explosion of health technology (health tech) platforms and applications that leverage the cloud promises to improve efficiency and quality of care within the healthcare system, as well as individual health outcomes.

[1]BDO Alliance USA, 2021 Healthcare Digital Transformation Survey, 2021

Healthtech is defined broadly as any IT tools or software designed to

- **Improve the quality of care** provided directly to consumers, in medical settings, and across the healthcare system
- **Boost operational excellence and productivity,** accelerating your organization's pace of innovation and clinical excellence
- **Uncover information** that leads to new insights for diagnoses and treatments
- **Enable healthcare at home** via wellness tracking with applications and wearables, as well as telehealth visits

While there are many benefits to embracing cloud technology, the transition to a cloud-based infrastructure can also present new security and compliance challenges. Healthcare and health tech companies should be aware of the following as they migrate and begin to operate in the cloud.

Areas of security concern in your cloud environment

Unprotected systems are at risk for exploits

A report from the US Department of Health and Human services states that 96% of small, medium, and large sized hospitals claim they were operating with end-of-life (EOL) operating systems or software with known vulnerabilities, which is inclusive of medical devices.[2] Healthcare also experienced the 3rd most number of global data breaches with confirmed data loss from November 2020 to October 2021.[3] Systems that incorporate many different tools alongside solutions nearing end of life have an increased number of vulnerabilities that threat actors can use attacks like malware to exploit. Gaps resulting from a lack of overlap in tool coverage pose a similar risk to EOL systems where software updates and security patches are no longer released.

Outdated approaches to security create risk

Organizations with a legacy approach to security have a limited view of their estate and can't fully understand their risk. This can lead to employing solutions that don't provide the "right" coverage for complete protection or to meet compliance. Legacy approaches may also lead to a homogenous threat response that does not recognize or prioritize the proper severity of a threat.

Legacy hardware presents risk

Legacy systems in hybrid environments or at organizations just starting their cloud migration may no longer receive security updates, and the organization may have limited budget or resources to upgrade systems to supported versions.

Operational inefficiencies limit risk reduction capacity

Sifting through thousands of alerts in different portals to manually prioritize issues can lead to alert fatigue, desensitization, and missed critical alerts. According to Orca Security's 2022 Alert Fatigue Report, 55% of security teams say they are missing critical alerts.[4] Time spent managing device security and correlating alerts from different tools leaves teams with little time to remove the risks that matter most.

[2] United States Department of Health and Human Services, Hospital Cyber Resiliency Initiative Landscape Analysis, April 2023

[3] Statista, Global number of data breaches with confirmed data loss from November 2020 to October 2021 Industrial security incidents with confirmed data loss, 2021

[4] Orca Security, 2022 Orca Security Alert Fatigue Report, 2022

Siloed tools impact efficient, secure care

When security functionality is spread across siloed tools, it can increase the difficulty for teams to secure complex cloud environments. Without a single cloud security tool that provides visibility into every cloud asset, and coverage for every cloud risk type — spanning misconfigurations, vulnerabilities, identity risks, API security, data security, and advanced threats — teams are operating without a holistic view and comprehension of their risk profiles to implement consistent security controls.

Without a single-pane of glass, and the unification of security data, security teams have been forced to sift through extremely long lists of alerts. Security practitioners have inherited these lengthy lists from siloed tools that have required them to collect and analyze the security data to better understand the risk, and prioritize which alert could potentially cause the most harm to the organization.

This operational inefficiency causes teams to spend valuable time correlating and prioritizing risks, instead of actually solving and removing the risk. With the speed and scalability that AWS provides its customers, any small operational inefficiencies within your organization's security teams can lead to quickly compounding challenges. Removing operational friction, alert fatigue, and having security teams focus on remediating risks — rather than the correlation of alerts — can be achieved by eliminating the approach of combining multiple siloed tools in an attempt to gain security visibility.

Implement a comprehensive security governance strategy

Maintaining security and compliance in a highly regulated and rapidly evolving industry can be challenging. Changing standards and escalating risks to an organization's reputation can make teams feel they have to choose between managing compliance and driving innovation.

Keeping patient data secure in this new era of personalized care is simple with the Orca Security platform on Amazon Web Services (AWS). By bringing cybersecurity data concerning posture, risk, workload needs, identity and access management, and more into one place, teams can efficiently manage risk related to device and patient data at scale. This results in HIPAA compliant healthcare reporting and fosters a more collaborative approach to care by ensuring that patient information stays secure while also being accessible to the different members across a care team.



Understand your greatest cloud risks

Within minutes (and with zero downtime), Orca's patented SideScanning™ technology collects data and retrieves cloud configuration metadata with read-only access.

This allows Orca to detect the following without any performance impact:

- VULNERABILITIES
- MALWARE
- MISCONFIGURATIONS
- LATERAL MOVEMENT RISK
- API RISK
- IDENTITY AND ACCESS MANAGEMENT RISK
- UNSECURED PHI/PII

Orca then surfaces the most significant cloud security risks for your connected devices to be remediated. This single tool replaces legacy vulnerability assessment tools, cloud security posture management, cloud workload protection platform solutions, and more while detecting important security risks at every layer of the cloud.

IMPLEMENT A COMPREHENSIVE SECURITY GOVERNANCE STRATEGY



Prioritize risk accurately and close the loop on alerts faster

Orca considers the environmental context when surfacing alerts that are most critical to your security posture, providing alert prioritization. Packaged with the alert, is a precise path to remediation that can integrate with third-party issue-tracking software for streamlined remediation efforts.



Unify cloud security in a single platform

Combining all intelligence in a central repository allows Orca to see the bigger picture and understand the connections between your different assets to create a **unified data model**. This lets Orca fully understand where your crown jewels are and effectively prioritize those risks that endanger the organization's most critical assets.

Additionally, Orca Security supports 100 out-of-the-box compliance frameworks, CIS Benchmarks, and custom compliance checks. This includes vital health industry frameworks including the HITRUST security framework, HIPAA, PCI-DDS, GDPR, SOC2 and more. It can also detect the presence of sensitive data and any potential exploitation paths, enabling fast, effective compliance and reporting.



Increase speed and agility

In a cloud computing environment, new IT resources are only a click away, resulting in a dramatic increase in agility for the organization. With Orca's agentless security, organizations are easily scalable and ready for environments where new workloads are spinning up and down. Time spent manually configuring, monitoring, and managing security can be put towards modernizing applications and infrastructure instead.

The Orca Cloud Security Platform for AWS

The Orca Cloud Security Platform delivers comprehensive coverage and visibility across your entire AWS cloud estate, empowering security teams to identify and remediate risks quickly. With its implementation, your healthcare organization experiences higher visibility leading to more robust data governance, defined security protocols for compliance reporting and audit logs, and a secure business without impacting performance or the patient experience.

Orca's comprehensive cloud security platform provides:

- **CLOUD SECURITY POSTURE MANAGEMENT**
  Identify and remediate misconfigurations across clouds.
- **CLOUD WORKLOAD PROTECTION**
  Protect cloud VMs, containers, and serverless.
- **CONTAINER AND KUBERNETES SECURITY**
  Secure cloud-native applications across Build, Deploy, and Run.
- **SERVERLESS SECURITY**
  Monitor vulnerabilities and compliance issues for serverless functions.
- **INFRASTRUCTURE AS CODE (IAC) SECURITY**
  Scan IaC templates and integrate security pre-deployment.
- **CLOUD DETECTION AND RESPONSE**
  Automatically identify and remediate cloud threats across clouds.
- **API SECURITY**
  Continuously monitor, audit, and secure APIs across multi-cloud environments.
- **VULNERABILITY MANAGEMENT**
  Identify, prioritize, and remediate vulnerabilities spanning libraries, packages, and operating systems.

Orca Security and AWS are better together

As the 2022 Global winner of the AWS Security Partner of the Year award, Orca Security is also making the cloud more secure through the Orca Cloud Security Platform and the Orca Security Research Pod. This research team discovers and analyzes cloud risks and vulnerabilities to strengthen the Orca Platform, promote cloud security best practices, and make the cloud a safer place for all organizations — customers and non-customers alike.

aws PARTNER

Security
AWS Partner of the Year

GLOBAL WINNER 2022



100% coverage

Never settle for partial deployment and visibility again. Orca's agentless platform sees it all (even idle, paused, or stopped machines). Within minutes, Orca surfaces the most critical security risks that threat actors exploit — all without agents, organizational friction, or impact on performance.



Multiple tools in one

Orca detects every important security risk at every layer of the cloud. There is no longer the need to cobble together disparate tools. Orca replaces legacy vulnerability assessment tools, CSPM, CWPP solutions, and more.



Alerts that matter

While other solutions only consider the severity of the security issue (e.g. CVSS score) and ignore the possible business impact, Orca considers the environmental context and surfaces those alerts that are most critical to your security posture along with their precise path to remediation.



Built-in compliance

Orca ensures regulatory compliance by alerting to threats ranging from vulnerabilities and malware, to file integrity and leaked passwords. Orca also detects the presence of sensitive data such as PII and any potential exploitation paths, helping you meet compliance mandates such as PCIDSS, SOC 2, CCPA, GDPR, and HIPAA.

CUSTOMER CASE STUDY

Flo Health deploys an automated defense

Business Challenge

Flo Health, a cloud-native provider of personalized cycle and ovulation tracking, health insights, expert recommendations, and a private community to share their questions and concerns for over 200 million people, was looking for ways to:

- Increase visibility into their cybersecurity posture across their entire technology stack.
- Adopt a data-driven, automated approach to security.
- Ease compliance efforts to achieve ISO certification.

Solution

After briefly evaluating security tools, Flo Health committed to Orca Security for a well-structured security product. “With Orca being agentless, our cloud security lead got it up and running, and we took our first snapshot within a few hours. After that, it was very easy to get a login and start adding integrations. It plugs in seamlessly with what we have,” explains Cunningham.

Impact

The Orca Security platform fits into the long-term strategy Flow Health has. By setting up integrations and automation into Jira, they’ve created a closed-loop process that has proven to be a time-saver for Flo Health, with Cunningham estimating it saves the time of about five full-time employees.

Results

- Orca consolidated alerting into one place to give a detailed view of the security posture for the entire cloud estate.
- Integration with Jira for automation reduced friction with software engineers and accelerated Flo Health’s time-to-remediation.
- Orca eased efforts needed for Flo Health to reach compliance with CIS, PCI DSS, ISO, and more.
- The return on investment has been strong and almost immediate.

> “Data security posture management provides visibility as to where sensitive data is, who has access to that data, how it has been used and what the security posture of the data store or application is.”

Leo Cunningham, Chief Information Security Officer, Flo Health

Why Orca Security and AWS

As an AWS Software Partner, we're committed to working closely with you to secure your AWS cloud estate. Orca Security's commitment and support on AWS includes:

- AWS Security Competency and AWS Service Ready for Amazon Linux 2.
- Support for 100+ AWS services and products, including Amazon Elastic Compute Cloud Image Builder, Amazon Elastic Kubernetes Service, Amazon Elastic Container Service, AWS Fargate, Amazon Linux2, AWS Lambda, Amazon GuardDuty, AWS CloudTrail, AWS PrivateLink, Amazon Security Lake and many more.
- Availability on the AWS Marketplace.

Ready to improve your cloud security posture? Understand and prioritize your greatest cloud risks with a free, no-obligation Cloud Security Risk Assessment from Orca Security on AWS. Receive an expert-guided experience, your own Key Risk Finding Report, and full access to the platform for 30 days access. Organizations can immediately get actionable insights and remediation recommendations for the most critical security risks.

Register for your Cloud Security Risk Assessment:
https://orca.security/lp/awws-cloud-security-risk-assessment/

Learn more about the complete and comprehensive cloud security platform that is Orca Security on AWS: **https://orca.security/partners/technology/amazon-web-services-aws/**



About the Orca Cloud Security Platform

Orca Security is a comprehensive cloud security platform that identifies, prioritizes, and remediates risks throughout your entire cloud estate. Orca connects to your environment in minutes with patented SideScanning technology to provide complete coverage across vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords, overly permissive identities and more. Founded in 2019, Orca is trusted by hundreds of customers globally.

