The Ultimate Guide to:

Gaining Full Stack Visibility into Your Cloud Assets

November 2019

Orca Security Ltd.
Exhibit 2066
Wiz v. Orca
IPR2024-00863, -00864, -00865, -01109, -01190, -01191
Ex. 2066-001

Synopsis

It’s no secret that cloud deployments are sky-rocketing globally, with organizations of all sizes and industries transitioning at least some of their infrastructure and assets to the cloud. Are visibility and security of these cloud resources managing to keep up? The answer is: no. Conventional visibility tools all have 'blind spots' and either don't see all cloud assets or can't analyze assets in-depth. There is however, a new -generation cloud asset visibility and security solution that delivers in-depth, full stack visibility. This ultimate guide covers the pros and cons of current solutions and includes a comprehensive solutions comparison table. It concludes with what 2019 and beyond holds for full stack visibility.

Ex. 2066-002

Introduction

According to the 2018 IDG Cloud Computing Study, 77% of organizations have deployed at least a portion of their computing infrastructure in the cloud. First seen as a cost saving strategy, the cloud is now leveraged to accelerate IT service delivery, improve business continuity, and provide greater flexibility, resulting in competitive advantages in dynamic market conditions.

However, as cloud environments continue to expand at an unprecedented rate, new security risks arise for the organization. While building an agile culture, and in an effort to improve market responsiveness, security teams are sometimes in the dark as they are routinely left out of the loop when it comes to new assets being deployed. This is of course, not some sort of calculated plan to sabotage company security, but the ease, pace and value of cloud adoption simply leads to this rapid deployment and consumption. Speed is of the essence, thus amplifying the challenge of finding a solution that can see and manage all assets and their associated risks for the company.

Given the very nature of the cloud however, increasing the speed of innovation has made organizations feel they need to choose between slowing down innovation or accepting the risks.

The basic foundation of securing a cloud environment is “full-stack visibility” into your cloud assets. Achieving full stack visibility has become even more crucial, because what you can’t see carries the risk of unforeseen and unmanageable risks.

Full stack visibility entails a complete understanding of what goes on inside the comprehensive cloud environment: the infrastructure level, operating systems, applications and data.

Ex. 2066-003

The OS and application layers are the most critical, as they are the most commonly targeted attack surfaces today.

Full stack visibility into four layers:

Cloud Infrastructure level: All assets run on top of this layer. Clear visibility here provides answers to the following questions: Which assets are running on which networks? Who is allowed to access them? etc.

Operating System level: Common issues like remote code execution vulnerabilities (e.g. CVE-2019-0708, which was published recently) exist in this layer. It is vital to see which OS is in use, and when it was last updated or patched; is it secured sufficiently or wide open? And, what is the configuration setup (i.e. user privileges in compliance and patches that need to be applied)?

Application level: This layer is where the vast majority of the vulnerabilities reside. The Equifax breach provides one concrete example. It is vital to see; which applications are installed, what are their configurations, and whether they are patched appropriately.

Ex. 2066-004

Data Stack level: This layer includes all data inventory and where it is housed. Clear visibility is critical in order to determine where the organization's crown jewels are, and which servers include sensitive data such as PII or payment info.

Full stack visibility of the cloud environment is even more challenging when attempting to combine legacy agent-based systems with network scanners or first-generation cloud security posture managers. This patchwork of non-cloud-born solutions and their required workflows have proven to be operationally cumbersome and simply does not provide complete coverage of assets, leaving organizations with potentially unseen and unmitigated risks in cloud environments.

According to Gartner, "Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement, and mistakes." Gaining visibility into cloud services is therefore crucial in order to maintain a secure cloud environment.

Full stack visibility entails a complete understanding of what goes on inside the cloud environment: the cloud infrastructure level, operating systems, applications and data.

Ex. 2066-005

Security Risks of Sprawling Cloud Deployments

One of the first issues that arises is **determining administration of cloud resources; i.e. who is in charge around here?** The traditional network model no longer exists and cloud adoption has commonly created some friction among security teams and other departments in the organization. Defining roles and responsibilities within the cloud between DevOps, Sys Admins, outsourced staff, and any subsidiary organizations may not only create dysfunction, but also security weaknesses from rogue deployments and assets, forgotten assets, and misconfigured or forgotten user accounts. DevOps teams should be able to innovate without waiting for security tools to be integrated to assets deployed in the cloud.

Cloud assets can be very dynamic as they are spun-up and torn-down on demand, which makes them difficult to track and manage. **Due to the tremendous efforts required to deploy them**, traditional non-cloud-born visibility solutions don't provide complete visibility. As a result, they cannot be relied upon to answer basic questions such as, "Do I have servers vulnerable to XYZ?, "How many servers running ABC do I have?", "Do I have sensitive data stored insecurely?", "How many databases of this version exist"?

Below are the cloud layers and a breakdown of their specific security concerns.

Cloud Infrastructure level

- Defines who can access the machine (its IAM roles), the networks it is connected to, logging policies, and disk level encryption
- Visibility needs: Who has access to the machine (avoiding possible misconfigurations), connections to the wrong or dangerous networks
- Example: An internal server which is also mistakenly connected directly to an external network

Ex. 2066-006

Operating System level

- Manages, operates and executes processes
- Visibility needs: Into inventory and OS services, as well as vulnerabilities, including updates and patch status, configurations and misconfigurations
- Example: Weak authentication configuration that puts the machine in jeopardy or open ports; vulnerabilities residing in operating system services, like Eternal Blue or CVE-2019-0708 (recent vulnerability in the RDP service)

Application level

- Applications installed on the machine, like web servers, CRMs, Database
- Visibility needs: Into application inventory, as well as vulnerabilities within all versions of the apps, configuration or security misconfigurations on the apps, and the existence of malicious apps, which would leave you with a compromised machine
- Example: Vulnerable web server, database, or even malware such as Cryptominer installed on a machine

Data Stack

- The data that resides on top of the apps, like database content
- Visibility needs: Ability to answer, ‘ Where is my PII stored?’ ‘What critical data exists on these assets?”
- Example: Stored credit card information or other PII

Ex. 2066-007

Conventional Cloud Asset Visibility Solutions

The most common methods of visibility into the cloud include: **agent-based solutions, network scanners, and cloud security posture solutions (CSPMs)**, each armed with their pros and cons.The following chart breaks down each type of solution and its capabilities:

Type of Scanner / Capabilities	Agents	Unauthenticated Network Scanner	Authenticated Scanner	Cloud Security Posture Manager	orca security
Risk to scanned assets	Medium	Very High	Medium	None	None
Operating cost	High	Low	High	None	None
Security Visibility- Depth	High	Low	High	Very Low	High
Security Visibility-Breadth	Low	Moderate	Low	High	High
System Support	Low	Moderate	Low	N/A	High
Can be circumvented by malware	Yes	Yes	Yes	N/A	No
Performance Impact	Moderate	High	High	None	None
Vulnerability Detection	Yes	Moderate	Yes	No	Yes
Malware Detection	Yes	No	No	No	Yes
Full stack Asset Inventory	Yes	No	No	No	Yes
Cloud Level Misconfiguration Detection	No	No	No	Yes	Yes
Physical System Support	Yes	Yes	Yes	No	No
Scan stopped machines	No	No	No	N/A	Yes

Ex. 2066-008

Due to cumbersome and partial deployment, agent based solutions can't be relied upon to provide full visibility

1. Agent-based Solutions

Qualys Cloud agent, Rapid7 Insight agents, and Tenable Nessus agents are some of the more popular agent-based solutions available.
How: Agent-based solutions are installed on each host system either manually or using another tool. The agent scans the host and sends results back to the management server.
Maintenance: Need to ensure that the agent can communicate with the management server which requires constant monitoring as well as software updates from time to time.

Pros:

- Delivers in-depth visibility into issues within the OS, applications and data status by looking into files, process, and registry data
- Able to detect malware and vulnerabilities in the host
- Ongoing visibility

Ex. 2066-009

Cons:

- Very high TCO due to the necessity of administering continuous updates, individually installing agents on new machines, and maintaining communication within the management server
- Impact on machine performance as they consume CPU, memory, and disks
- Incompatible with some assets like native cloud storage, cloud databases and certain endpoint types
- Can't detect cloud-level misconfigurations. Agents cover 3 of the 4 cloud layers - OS, applications, and data, but they don't scan the Cloud I/S. For example, agent scanners

2. Network Scanners

Similar to agent-based solutions, network scanning tools assess security posture but do not attempt to identify possible vulnerabilities on the host. Products in this category include solutions from Qualys, Rapid7, and Tenable.

Agentless network scanners fall into two basic types; authenticated and unauthenticated.

Unauthenticated Network Scanners:

How: An unauthenticated scanner will scan each host for open ports and installed applications and will try to determine if the host is susceptible to vulnerabilities by actively trying to use the attack against itself.

Maintenance: Need to ensure that all networks are scanned. This is problematic when working in the cloud and new networks are frequently added.

Ex. 2066-010

Pros:

- Initial costs are low for partial visibility, but grow significantly when trying to cover a larger percentage
- Ability to gain data on vulnerabilities without on-asset installation or authentication
- Broad security visibility when given suitable access to each network

Cons:

- The scanner can inadvertently create outages on the services when trying to exploit the vulnerabilities. There is a fine balance between the detection level and a tolerable risk level.
- Due to the fact they're scanning from the outside, unauthenticated scanners use heuristic techniques in order to detect which applications are configured on the server. False negatives are thus a common side effect. These heuristics can be augmented by the administrator explicitly providing the details, something which is frequently overlooked due to the operational overhead.
- As unauthenticated network scanners rely on trying to exploit the environment, they're often blocked by firewalls and IPSs. Making sure the scans are completed correctly requires a lot of manual work and due to the large number of networks within the cloud, is impractical.

Ex. 2066-011

Authenticated Network Scanners

How: An authenticated scanner, also known as a credentialed scanner, uses privileged credentials to log in to each host and is able to detect vulnerabilities and security misconfigurations.

Maintenance: Like unauthenticated scanners, it is necessary to ensure that all networks are scanned, which can be problematic when working in the cloud as new networks are frequently added. The need for credentialed access takes up a lot of time as well for organizations.

Pros:

- Provide in-depth security visibility without requiring an agent on each machine
- Ability to detect vulnerabilities for issues on the OS, apps and data layers

Cons:

- The requisite to deploy a scanner on each network and the overall integration of the credential management system can lead to high operating costs and/or partial deployment and hence visibility
- Firewall modifications are required to allow remote authentication creating a potential security risk
- Security visibility is limited as you cannot see into the machines that can not be integrated with, i.e. agents

Ex. 2066-012

3. Cloud Security Posture Management Solutions (CSPMs)

How: These solutions are designed to connect to the cloud infrastructure and analyze data about the cloud assets, the networks they belong to, user permissions, and tags. Products in this category include solutions from Redlock, Evident.io, and Cloudchecker.

Maintenance: A continuous check of cloud platform account compliance can be used to scan for misconfigurations, such as assets with inappropriate IAM roles or publicly open data stores.

Pros:

- Low maintenance and low operational costs
- Low risk; no agents or proxies are required
- Sees all of the cloud assets

Cons:

- Limited security visibility depth within each asset, covering the lowest level of the stack. It cannot provide visibility into the OS, apps or data layers
- Cannot detect vulnerabilities, compromised assets, and the vast majority of security risks
- While it provides a full list of assets, the data provided on them is limited

Ex. 2066-013

CSPMs don't penetrate the layers above the cloud I/S, failing to provide visibility to OS and application level vulnerabilities and breaches

Ex. 2066-014

Conventional Cloud Visibility Solutions:

Cons Outweigh the Pros

When comparing conventional solutions, the cons outweigh the pros. Integrating multiple tools can eliminate some of the deficiencies, but the more integration that's required means that more time, management, and manpower will also be needed. Furthermore, deploying and maintaining multiple solutions is not a cost effective way to spend the IT budget. Many businesses know all too well that even if all three solutions are implemented, it doesn't mean there will be full visibility or bullet proof security. Full stack visibility into the cloud, OS, applications, and data will still be lacking on one or more of the many assets on the layers. It's also highly likely that the assets lacking visibility are the most prone to risks. For example, a department or subcontractor that hasn't followed guidelines to install agents on their assets or integrate them with a credential management system has probably ignored other security measures and guidelines.

Integrating multiple tools can eliminate some of the deficiencies, but the more integration that's required means that more time, management, and manpower will also be needed.

Ex. 2066-015

The Orca Security Full Stack Cloud Visibility Platform

Attempts to implement visibility solutions constrained by pre-cloud limitations, are futile. No combination of these aforementioned visibility solutions will provide full visibility into an enterprise's resources on the cloud. While some solutions provide either broad or in-depth visibility, they don't provide both. Cloud security visibility solutions should provide full stack visibility for all assets, with no risk or per-asset integration cost. For this, a cloud-born visibility solution is a must-have. **This is precisely why Orca Security was established.**

How it works: The platform utilizes the patent pending SideScanning™ technology. After a one-time, essentially instantaneous, impact free integration into the cloud infrastructure; it scans the configuration, network layout, security configuration, while reading into virtual machines disks, databases, and datastores, as well as cloud logs for all of the cloud assets. It then analyzes the data, building a full-stack inventory and automatically assessing the security state of every discovered asset throughout the entire technology stack - including all four cloud layers: I/S, OS, apps and data. It undertakes a comprehensive assessment of the security state of every discovered asset, with complete visibility into compromised resources, vulnerable software, and misconfigurations without impacting performance or availability.

Maintenance: Orca's platform is integrated once **in a matter of minutes to get full stack visibility** into the security posture of all assets in the entire cloud footprint. There is no need to constantly monitor or integrate new systems. As it leverages read only integration, there is absolutely no risk involved.

Pros:

- Full stack visibility into all of your assets in minutes. As it doesn't rely on the OS, it can even scan stopped machines
- Deep security visibility on vulnerable software, non-secure configuration, exploitation attempts and compromised assets
- Utilizes read only access, so there is no performance or availability impact
- Provides full stack asset inventory for your entire cloud deployment
- Enables security teams to do their job without the enormous costs and organizational friction involved in deploying agents or network scanners
- One time integration to the I/S level covers all assets, no matter how many exist
- Since it doesn't rely on the scanned machine, Orca's side scanning solution can detect rootkits and malware which circumvent security agents

Cons:

- Does not currently cover IoT devices
- Does not support bare metal environments

Ex. 2066-017

SideScanning provides full stack visibility to all of the assets.

The Next Generation of Cloud Environment Visibility

While each of the conventional solutions have their strengths, when it comes to cloud visibility, it's clear that no matter which one is implemented, there will always be something missing in cloud coverage. Even when deploying a combination of agents, scanners, and CSPMs, there will still only be partial visibility. In most cases, organizations manage to reach less than 50% coverage when using these methods.

Orca's cloud visibility platform is the next generation, comprehensive solution for providing full-stack visibility into cloud assets.

> "Solutions like Orca's that offer comprehensive in-depth visibility with no integration headaches are exactly what's needed to empower teams to secure and scale the high velocity growth of cloud deployments,"
>
> Justin Somaini, former Chief Security Officer at SAP.

For more information on the Orca Security Platform, **Contact: info@orca.security.**

Ex. 2066-019