Orange
Cyberdefense

How can you protect what you can't see?

How to get single view, full visibility on your cloud estate

How can you protect what you can't see?

How to get single view, full visibility on your cloud estate

Table of contents

Author:
Marcus Hilmersson
Cloud Security Consultant
Orange Cyberdefense

Co-author:
Tim Lemmob
Principle Cloud Architect
Orange Cyberdefense

Introduction

Driven by a global health crisis and the most extensive remote working program the world has ever seen, the adoption of cloud-based services and platforms has surged during the pandemic. We've seen how cloud has served as a business enabler by allowing organizations worldwide to provide new and additional functionality to a remote workforce.

Unfortunately, this wave of often quickly implemented solutions has contributed to the exponential growth and changing nature of the threat landscape. How can you be confident that your cloud-based estate is sufficiently protected against these existing and emerging threats?

Our research shows an increase in pandemic-related business email compromises, phishing scams, and credential theft. We also saw escalating nation-state activity from persistent threat groups earmarking essential services to harvest personal data, intellectual property, and national intelligence. In addition, the number of exposed remote desktop protocol (RDP) and virtual private network (VPN) services has increased dramatically.

As a result, IT teams and associated project coordinators have been scrambling to patch and put solutions and policies in place to protect them. However, malevolent threat actors have been quick to exploit these opportunities and take advantage of the unexpected disruption that has ensued.

Dangers of cloud sprawl

For many enterprises, the move to the cloud has happened far faster than anticipated due to these unprecedented times. The instant elasticity that cloud provides has been of significant business benefit, especially in terms of scalability. As a result, enterprise have adopted and deployed cloud solutions and services without having a robust strategy in place. This has left them without any unified approach to manage, secure, and monitor legitimate cloud applications, let alone having any grasp on shadow IT.

Due to a lack of knowledge, we see enterprises waste energy and resources monitoring activity without knowing what they are looking for. Failure to manage and monitor cloud instances properly can in return spawn a significant and unpredicted spending on resources.

Establishing cloud security is a challenge

Some of the most beneficial elements of the cloud - its ability to be adopted, deployed, and scaled quickly – in return, also make it difficult to secure. Many enterprises try to superimpose their existing on-premises security framework and mindset on their cloud environment - only to sooner or later realize that this approach is like forcing a square brick into a round hole when a security breach happens.

A first step in the direction of improving the previously mentioned scenario, is a solid understanding of the shared responsibility model for securing a cloud environment.

Generally speaking, the cloud provider is responsible for protecting the physical data center, the core infrastructure network, and the virtual hosts deployed on that infrastructure. The enterprise's responsibility to provide the required level of security depends on services subscribed. It includes, however, at least all the company data hosted within the applicable cloud environment and can extend up to and including the operating systems deployed on the virtual machines. Protection of the intellectual property, access privileges provided to accounts, and ensuring identities are just some examples where the organization (or consumer of the cloud platform) remains responsible for its security, regardless of the service model.

Enter Cloud Security Posture Management (CSPM)

This is where Cloud Security Posture Management (CSPM) can help. It allows enterprises to continuously monitor their cloud infrastructure for holes in security enforcement policy and identify misconfiguration and compliance risks.

CSPM automates cloud security management across Infrastructure as a Service (IaaS), Software as a Service (SaaS), and platform as a service (PaaS). CSPM tools provide visibility into cloud infrastructure, comparing a cloud environment against a defined framework of regulatory compliance, best practices, and known security threats.

Rewiring security when you move to the cloud

Before embarking on a CSPM journey, it is vital to understand the cloud landscape. Cloud is transformational. It demands the creation of a cloud culture, and a rethink of the way technology is used. Silo mentality, for example, needs to be broken down and replaced with a unified vision of cross-team collaboration.

The technologies behind cloud are evolving so rapidly; the pressure to keep up can be relentless. As a result, some IT teams realize that their knowledge and skills do not cover the whole scope of the IT estate they suddenly need to cover.

Visibility is challenging

At the same time, typical cloud infrastructures are huge, and visibility is challenging. It also incorporates innovative technologies such as identity and access management (IAM) that traditional security solutions may not pick up.

Gartner[1] predicts that 95% of cloud security failures will be the enterprise's fault. Much of this will be down to misconfigurations. Exposing a cloud storage data bucket to the internet, for example, can lead to a significant data breach – especially if that data is highly sensitive. A big issue is that cloud infrastructure is easy to scale up and alter, potentially multiplying the number of misconfigurations in an instant and exposing the cloud estate even further.

CSPM has been designed to address the dynamic, constantly fluid nature of cloud. CSPM automates cloud security management across Infrastructure as a Service (IaaS), Software as a Service (SaaS), and platform as a service (PaaS). At a basic level, CSPM tools alert the enterprise if it is necessary to address a security risk. More advanced CSPM tools use robotic process automation (RPA) to correct issues automatically.

> "Cloud account compromises cost organizations over $6 million annually.[2]

Starting, but not finishing

Enterprises have great intentions when it comes to cloud security. IT teams start initiatives to heighten their security posture, but their efforts end up stalling as they have no end goal and are unable to understand the core problems.

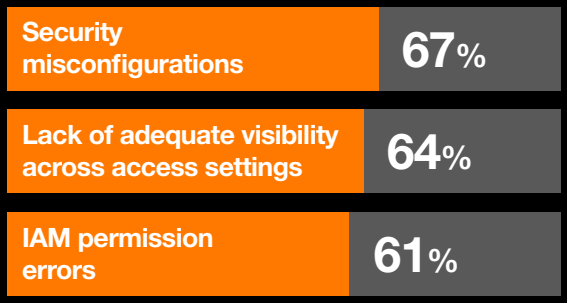
When migrating a portion of their IT infrastructure to the cloud, enterprises are, in addition to usual threats, exposed to new types of threats. It can be difficult, for example, to secure a multi-cloud estate because of a lack of visibility between the hosts and services, which could allow malicious actors to exploit this potential weakness.

You are responsible for security in the cloud

Enterprises that move to the cloud often wrongly assume that their cloud hosting provider is solely responsible for security. Unfortunately, many don't realize they are responsible for the data they put into the cloud. This includes data sharing, configuring applications, and putting role-based access controls in place. The result is avoidable misconfigurations and breaches to their data that are easily preventable.

A recent IDC study affirmed that misconfigurations continue to be a significant issue in keeping cloud data safe. The analyst firm found that Chief Information Security Officers (CISOs) list security misconfigurations (67%) as a primary worry, followed by lack of adequate visibility across access settings and activities (64%) and identity and access management (IAM) permission errors (61%).

Cloud can also be vulnerable to insider threats due to weak access management, insecure interfaces/APIs, improperly configured security, compromised credentials, and account hijacking.



Source: IDC

Don't trust anyone or anything – always verify

There is also the issue of insecure access points. This is where the concept of Zero Trust comes in. It eliminates the concept of trust in protecting infrastructures, applications, and data. Zero Trust does not trust anything by default – inside or outside the network. Access is only given via strict verification controls.

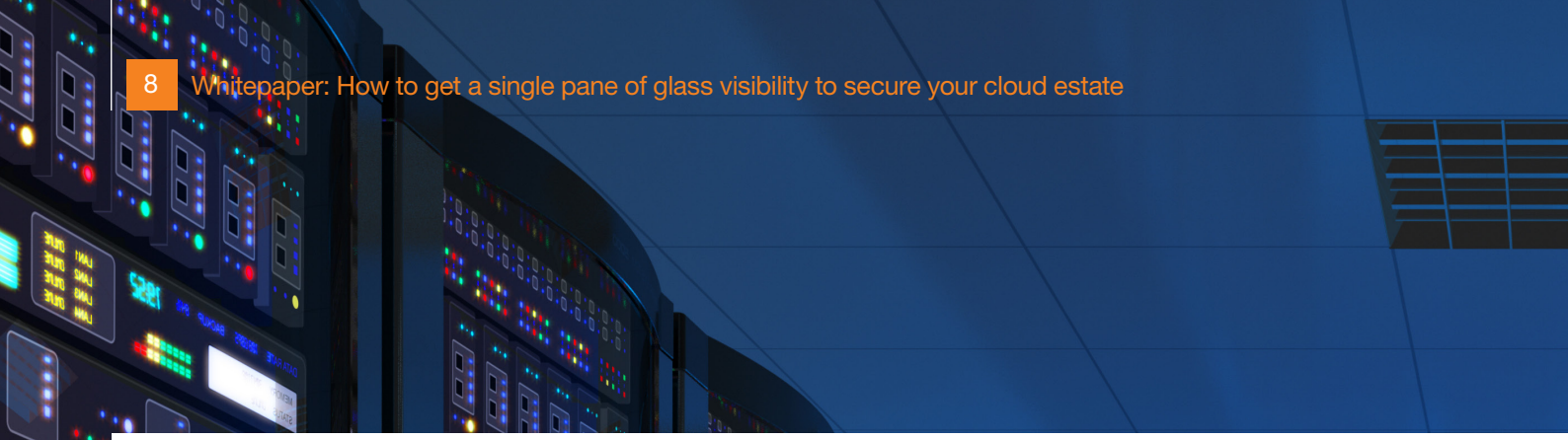
Don't ignore the issue of shadow IT

Enterprises not knowing where their assets are makes management extremely difficult and isn't limited to the cloud. But cloud's easy and fast self-service capabilities have made shadow IT a major issue. In some cases, sensitive corporate data is being uploaded to services without the knowledge of the IT department. Moving data to ungoverned data services means that the enterprise loses control and visibility, risking data leaks, security breaches, and regulatory non-compliance.

Moving forward

It is essential to tackle all these points to move forward. Secure cloud adoption necessitates a robust cloud security posture through cloud development, migration, and beyond. Cloud infrastructure security is not a tick box exercise; it is a continuous and committed process. CSPM is an essential component of this program.

> **"Through 2024, most enterprises will continue to struggle with appropriately measuring cloud security risks.[4]**



CSPM identifies errors that are often overlooked

It has never been more of a challenge to protect critical assets in the cloud. Multicloud is creating complex estates that are difficult to have visibility over. New cloud services are being added exponentially, which is making the task of managing risk burdensome. CSPM is a holistic approach that allows enterprises to quickly and easily identify cloud resource vulnerabilities, ensure compliance and respond promptly to any threats found.

A CSPM tool is the best way of securing your cloud configurations and keeping all your data safe. It provides a single pane of glass for seeing your cloud vulnerabilities and security posture in real-time.

The benefits of CSPM include:

- Continuous real-time visibility into cloud usage and events
- Cloud asset inventory
- Configuration assessment to prevent configuration vulnerabilities
- Regulatory and compliance management
- Automated remediation in many cases

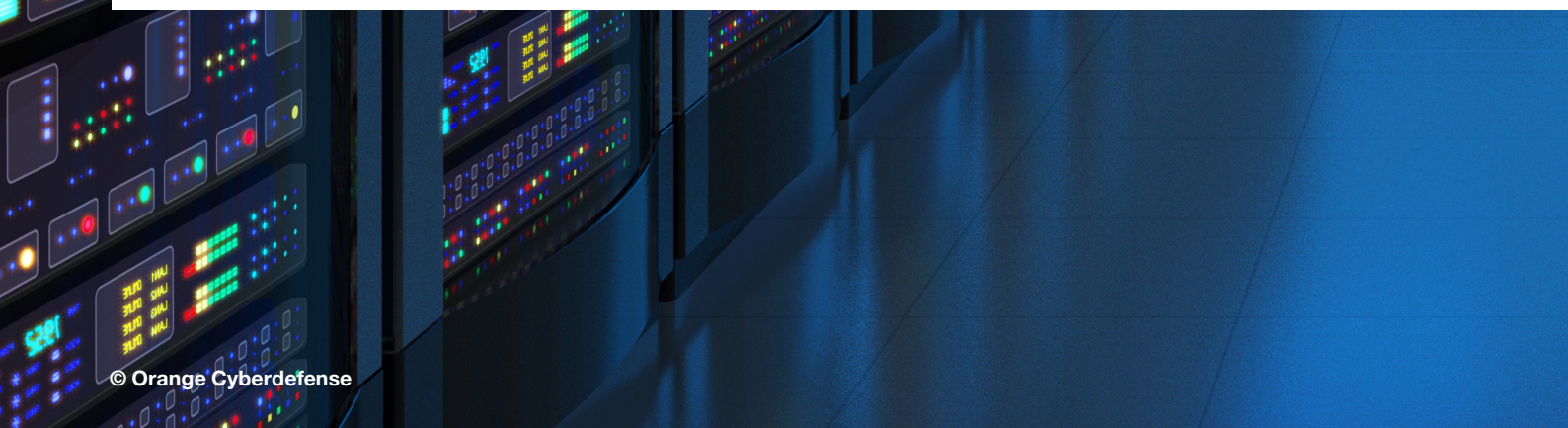
CSPM education is essential

If you are planning to deploy CSPM yourself, you can't simply rely on the technology. The IT team will need upskilling and continuous training in cloud best practices and fundamentals to ensure the tool provides the depth of visibility you need into your cloud estate and performs to its optimum.

CSPM: the continuous process of improving cloud security

No one size fits all when it comes to CSPM tools; they are not self-playing and can be challenging to orchestrate. A good security posture comes from having a robust strategy and framework, which is why many enterprises are turning to CSPM as a managed service to put best practices into place—allowing the CSPM to grow with your cloud presence.

Orange Cyberdefense offers Managed Cloud Security Infrastructure, a solution built with best-of-breed technology combined with security experts to monitor your cloud assets, 24 hours a day, seven days a week, to prevent misconfigurations, maintain compliance and detect known and unknown threats.

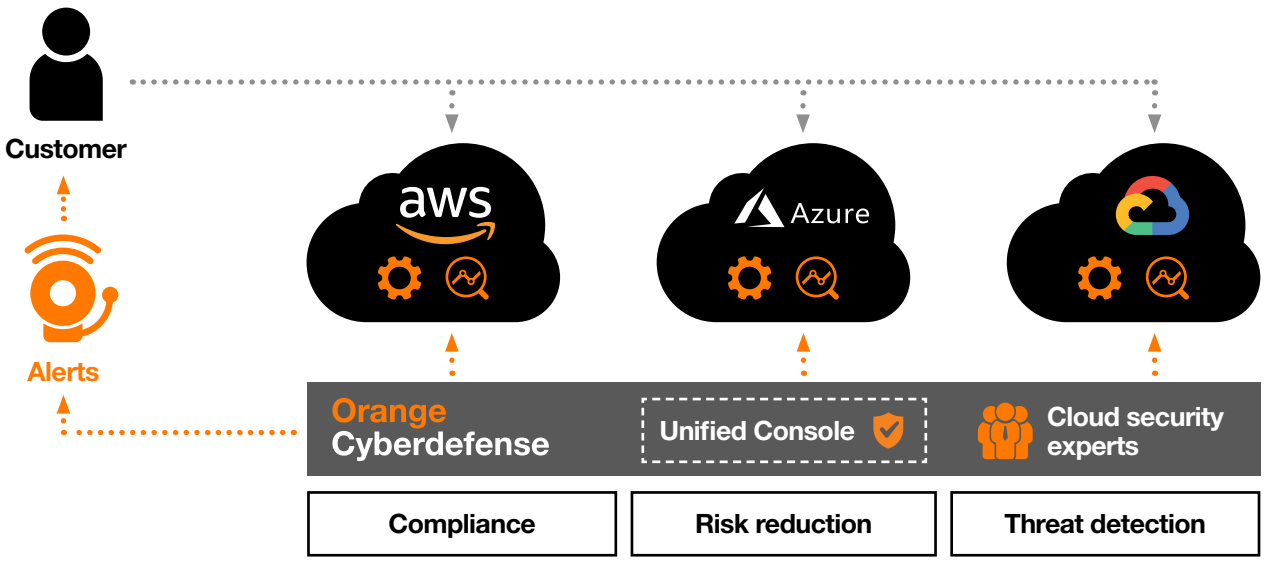


We also offer proprietary threat intelligence, which provides a unique value-add to these services, correlating and combining findings for actionable intelligence. We provide you with unified controls and a single pane of glass, providing a 360-degree view of your cloud assets and behaviors.

Continuous monitoring and assessment prevent compliance and cloud configuration risks while helping protect your data sovereignty. CSPM can highlight where you should and should not have data stored, for example.

CSPM requires a new set of skills, commitment, and a change in cultural mindset. But, CSPM provides a vital tool in the security kit to identify errors and eradicate risks that may otherwise have gone unnoticed.

Continous monitoring



CSPM: taking the first steps to manage cloud security risk

Cloud requires a rethink of traditional security concepts. To help manage the cloud's distributed and dynamic nature, many cloud management platforms and tools are available to monitor and control cloud computing resources. CSPM focuses on security assessment and compliance monitoring.

CSPM allows enterprises to constantly monitor the known and unknown in their IT estate and the cloud. Some CSPM solutions identify the problems; others have tools that can quickly remediate issues.

Continuous monitoring

Most enterprises today are aware of CSPM, but they often fail to understand that it is a continuous process of improvement and adaptation to reduce the possibility of a malevolent attack. As such, the key to the effectiveness of CSPM is continuous monitoring. By continuously looking out for security or policy violations, the solution can raise a red flag to issues such as misconfigurations before bad actors have a chance of exploiting them.

> **"Through 2025, 99% of cloud security failures will be the customer's fault.[5]**

6 points to consider in choosing a CSPM solution:

1. **Consultancy assessment**
   It is essential to have a consultancy assessment of an enterprise's current processes so that the right tool can be leveled for the task at hand.

2. **Support cloud environments**
   It is paramount that the enterprise verifies that the chosen CSPM supports its cloud environments.

3. **Customization**
   Look at how easily the CSPM tool can be customized to fit in with the enterprise's technical and regulatory environments.

4. **Integration**
   Check that the CSPM can easily integrate with the cloud infrastructure to run detailed security assessments and carry out remediations.

5. **Efficiency**
   Enterprises with hybrid and multicloud environments must ensure that the chosen CSPM will run efficiently and effectively across infrastructures.

6. **Visibilty**
   Make sure the CSPM platform provides end to end visibility of the cloud environment.

Sources

1. Gartner cloud computing insights 2019
2. Ponemon Institute: the cost of cloud compromise and shadow IT 2021
3. IDC Top identity and data access risks survey 2020
4. Gartner Is the cloud secure? 2019

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Our organization retains a 25+ year track record in information security, 250+ researchers and analysts 17 SOCs, 11 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Orange Cyberdefense has built close partnerships with numerous industry-leading technology vendors.

We wrap elite cybersecurity talent, unique technologies and robust processes into an easy-to-consume, end-to-end managed services portfolio.

At Orange Cyberdefense we embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. Their competence, passion and motivation to progress and develop in an industry that is evolving so rapidly.

We are proud of our in-house research team and proprietary threat intelligence thanks to which we enable our customers to focus on what matters most, and actively contribute to the cybersecurity community. Our experts regularly publish white papers, articles and tools on cybersecurity which are widely recognized and used throughout the industry and featured at global conferences, including Infosec, RSA, 44Con, BlackHat and DefCon.

T: +31 88 1234 200
E: info@gb.orangecyberdefense.com
https://orangecyberdefense.com/gb/

www.orangecyberdefense.com
Twitter: @OrangeCyberDef