
GlobalDots
Your 2022 Guide to a Successful Cloud Strategy
#2: Cloud Security Tooling
Author: Steven Puddephatt, Senior Cloud Architect at GlobalDots
#1 How to Choose Your Cloud Provider(s)
#2 Cloud Security Tooling
#3 Cloud Governance Best Practices
#4 Budget Allocations & Procurement
#5 Building Your Company's Cloud Centre of Excellence(CCE)
Download Full Guide

Table of contents

Executive Summary

This whitepaper is part of a 5-whitepaper series suggesting guiding principles for moving towards a successful cloud environment. It applies to both newly migrated and already cloud-based organisations.

A successful cloud environment is one that provides maximum benefit to business processes, with minimal spend and complexity, and with the utmost security.

GlobalDots has been helping organisations successfully migrate to the cloud for years, and in that time we have seen businesses fall foul of the same mistakes over and over.

It's much easier, cheaper, and more efficient for your business to plan how you will use a cloud estate before you migrate there. In other words, spend more time planning your cloud estate before you let everyone loose in it, thereby turning it into what I like to call a 'double W' estate, or a Wild West estate!

If you have already migrated to a cloud provider, don't worry – the principles laid out here still apply. However, tidying up is a slightly more laborious task than starting from scratch.

Why is a cloud strategy necessary?

Shift problems left:

By spending time now to determine a set of rules (that are enforced by software tools), problems later can be severely reduced. By setting up rules and governance policies you can ensure your cloud journey runs smoothly right from the start.

The most common mistake we see is rushing into the cloud. It's easier to set up a safe landing zone for your cloud resources than it is to try and clean it up once production workloads are already running. Spend the time setting up in advance and make sure your cloud estate is clearly organised from the outset. That way, clean-up operations won't be necessary.

Spend money to save money:

Most organisations are reluctant to spend large sums of money on governance software before they build out their cloud infrastructure. This is actually a harmful mindset and will cost more in the long run.

SREs, DevOps and senior sys admins are some of the most expensive human resources on the planet, and it is exactly these people that you'll be asking to monitor and investigate goings on in your platform. They'll end up writing a complex set of admin scripts in order to ensure IAM roles are used correctly, API access keys are rotated, resources are spun down when they are not needed, and so on.

As your cloud estate grows your IT engineers will be swamped with requests. It's not realistic to expect them to be able to keep eyes on the whole estate. That's why it's so valuable to spend money on governance and security tools at the outset. Adding tools too late in a cloud journey will lead to a bumpy integration and security dashboards will be flooded with unremediated alerts.

Long-term thinking is a must:

Simple cloud platforms quickly become complicated, single VPCs become many and the connections between platforms can become vast and complex. When deciding on a cloud strategy the long-term effects of early decisions must be thought through, as these decisions will determine all the legacy systems, not just the new ones.

A well-governed cloud environment takes careful planning, budgeting and execution. Be prepared to fight the budget holders for money which won't reap benefits for 12 - 24 months. Be brave with proposals and use examples of horrific cloud sprawl (a quick google search will turn up results) to scare money from the company coffers.

Cloud Security Tooling

Next generation security products should be part of any cloud strategy, and there should be a security officer in charge of investigating tools to protect your estate. GlobalDots is a world leader in bringing new security products to market and we have been doing so successfully for 15 years. We recommend looking at some of these next generation cloud security tools. The list below is not exhaustive, but covers the most important aspects of cloud security for most organisations.

Zero trust access & SASE

As organisations expand their cloud estate the boundaries of the company will become more blurred. This happens for a number of reasons, including taking on more SaaS providers, more remote workers and the increase of BYOD (bring your own device, i.e. phones and tablets).

It's no longer acceptable to use VPN technologies in order to connect users and it's recommended that organisations look to decommission all VPN access. Look to replace outdated VPN user access with Zero Trust tools, which only give users access to the specific applications they need, and can be linked to permissions in existing directories such as MS Active Directory or a SAML identity provider.

Site-to-site VPN access can remain, as this is more secure, although in reality organisations should look to combine all their networking into a Secure Access Service Edge (SASE). A **SASE** would move all networking configuration to the cloud and replace SD-WAN, MPLS and Branch VPNs. A SASE would also cater for WAN optimisation, Zero Trust access and mobile device access, as well as provide a gateway for SaaS applications, enabling you to lock down tools such as Salesforce and Office365 to only your employees.

Open source security

It's a common misconception that using the 'latest' versions of open source software means that they are safe and/or bug free. As you move toward a microservices based environment it's natural that the number of open source dependencies will increase.

A typical example is Nginx, which is probably one of the most common docker packages used globally. In the **latest test** "nginx:latest has 106 known vulnerabilities", without sufficient tooling you risk unnecessarily introducing vulnerabilities. Luckily, there are tools available to catch these vulnerabilities in the IDE (internal developer environment), CI/CD pipeline and in the code repos themselves, ensuring bugs don't enter production.

Watch our recent video for more information.

Cloud workload & Kubernetes protection

As workloads in the cloud increase, sprawl is inevitable. With new resources constantly popping up, an organisation's attack surface is greatly increased. Trying to keep a watchful eye on so many moving data points becomes impossible, and thus it becomes necessary to use a data-driven cloud workload protection tool.

We at GlobalDots review and assess these tools (**click to watch our CWP demo**) so we are familiar with the latest developments. With a cloud workload protection tool in place you'll be able to spot major security vulnerabilities, over-permissioned users and threat intelligence timelines.

If you're serious about security, we recommend Cloud Security Data Platforms as a **cloud workload protection** tool. This 4th generation of solutions uses machine learning and smart algorithms to spot anomalies and find your security 'needle in a haystack'. Its main benefit is the ability to take billions of events and distil them down into a manageable number of alerts. This emerging category defines its ICP (Ideal Client Profile) as young, growing companies (50-5,000 users) with a minimum of $100K monthly cloud spend.

Dedicated **Kubernetes security** tools are another option to look at. However, at GlobalDots we tend to recommend solutions that allow tooling consolidation, such as Cloud Security Data Platforms. Such a strategy proves more beneficial as the company grows, along with complexity potential.

Cloud workload and Kubernetes protection is an area where organisations will have to budget and plan early to stop attacks and data leaks in the future. **This infographic** might help (switch filter to 'poor security') to see where cloud workload protection would have helped.

API protection

The final part of our recommended new security stack is **API security**, which has been an official part of **OWASP** since 2019. APIs have become the de facto way for systems to interact, and as such are now a prime focus for hackers. Many companies already use tools like WAF protection, but those traditional tools won't catch API based attack vectors. In order to properly catch zero day attacks it's necessary to have specific API traffic inspection.

With a cloud workload protection tool in place you'll be able to spot major security vulnerabilities, over-permissioned users and threat intelligence timelines.

Summary

The cloud can enable businesses to grow rapidly but without a good strategy you'll end up in a mess.

Technical staff are required to build a competence centre or a 'Cloud Centre of Excellence' (CCE). With this team in place better engineering and technical decisions can be made on behalf of the whole business. The CCE should oversee enterprise-wide technology decisions and responsible for introducing good governance of those tools.

By bridging the gap between business units, technical teams, and management, a CCE would make sure the right decisions are made, reducing technical debt and standardising the tools and technologies used in cloud environments.

Only through good governance, good tooling and good teamwork will an organisation achieve an optimised cloud environment. Time, money and effort needs to be expended up front in order that the future cloud environment is flexible, tidy and well governed.

Additionally, most tech stacks remain unprotected at some level. Therefore, there is a specific importance to cloud workload protection and open source vulnerability detection. We highly recommend organisations look at tooling to address these common blind spots.

There is an ever-growing variety of cloud solutions for performance and security. The right ones for each business are a needle in a haystack. Therefore, consulting an impartial cloud technology partner can save much of the investment in research, evaluation, and proper implementation.

Download Full Guide

Appendix: Example toolset

Below is a summary of example technologies needed to ensure good governance and effective security in cloud environments.

To learn more about them, make sure to read all 5 parts in this Cloud Strategy series! Download Full Guide

A

API Security

Application monitoring

C

Cloud cost reduction

Cloud Governance (SDO)

Cloud migration

Cloud Workload Protection

I

Identity Management

K

Kubernetes Security

L

Log management

O

Open Source Security

P

Passwordless Authentication

S

SD-WAN & SASE

Z

Zero Trust Access

GlobalDots Your Tech Innovation Partner

GlobalDots is a world leader in discovering and implementing cloud & web innovation. Over the last **17** years, GlobalDots enabled streamlining and smart growth in over **500** business customers, providing enterprise-grade web performance & CDN; Web Security & anti-fraud solutions; DevOps & Cloud services; Cloud Security; Corporate IT; Cloud-native networking and infrastructure.

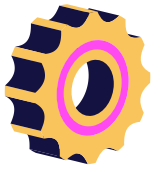
Our vendors range from world leaders to innovative, cutting-edge startups.

Our seasoned engineers test & master each solution's capabilities, pros, cons, and best practices. This allows them to quickly spot your perfect fit of technology and enable fast, smooth adoption.

The GlobalDots Innovation Edge

Innovation Hunters

Constantly tracking the industry to provide spot-on solution s for your ecosystem.

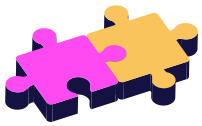


Vendor-Agnostic

Our ever-evolving portfolio and customizable solutions cater for each unique use case.

Streamlining Technology Adoption

Breezing you through from selection to deployment, exhausting every feature to your business benefit.



Holistic, Business-Oriented Approach

We align your IT architecture with your business profile, use case and goals focusing on what matters in terms of complexity and financial impact.

Do you want to know more? Contact Us