It's time to productize your Cloud Security!

FS Cloud Engineering

Productizing your cloud security

It’s no secret that the public cloud is on every organisation’s agenda with the sector set to account for around $400 billion in revenue by 2025[1], which continues to expand year on year. Many organisations start out on their cloud journey with a few pathfinder projects that rapidly grow and expand as engineering squads realise the value of services that are designed around delivering value at pace.

This also brings challenges, as the number of workloads grow, this can often lead to sprawling cloud estates which may not be configured in the best way, opening risks that could bring your organisations data under threat. **With over 90% of organisations hosting workloads in the cloud around 80% of companies have reported at least one cloud based data breach in the last 18 months[2]**.

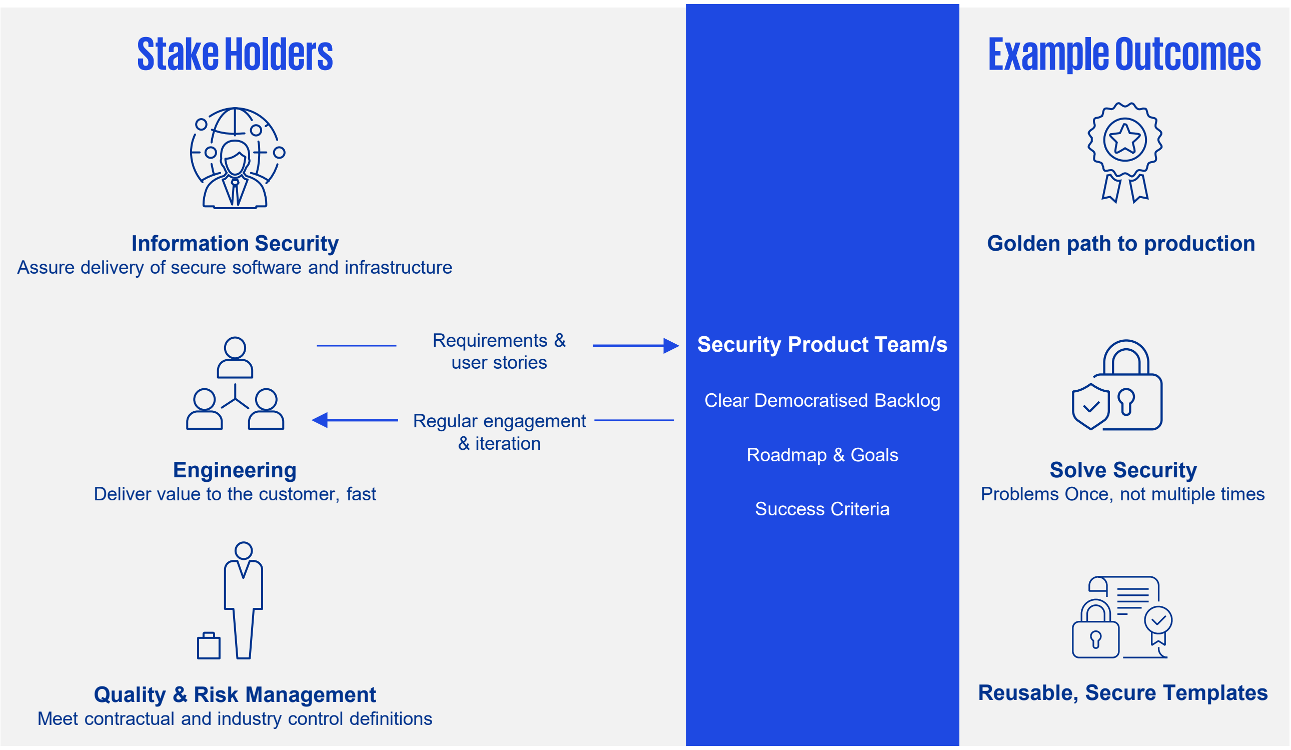
There is always a desire to deliver value quickly in technology, particularly during the COVID-19 pandemic, where cloud-based workloads formed the backbone of the international response to tackle the pandemic. One key threat vector is human error and subsequent resource misconfiguration, this is exacerbated when deadlines are tight and the customers demands keep growing.

More traditional approaches to managing risk, such as detailed point in time assessments combined with often cumbersome and outdated controls can lead to delays in delivering value, this can cause significant friction and internal frustrations between information security and engineering cohorts.

One way of reducing this friction, ensuring you can deliver value through technology securely and at pace is to **treat your cloud security estate as a product.**

[1] https://www.idc.com/getdoc.jsp?containerId=prUS48129821#:~:text=The%20combined%20Public%20Cloud%20IaaS,the%202021%2D2025%20forecast%20period.

[2] https://expertinsights.com/insights/50-cloud-security-stats-you-should-know/#:~:text=the%20latest%20figures.-,The%20Frequency%20Of%20Cloud%20Attacks,more%20breaches%20in%20that%20time



Stake Holders

Information Security
Assure delivery of secure software and infrastructure

Engineering
Deliver value to the customer, fast

Quality & Risk Management
Meet contractual and industry control definitions

Security Product Team/s

Clear Democratised Backlog

Roadmap & Goals

Success Criteria

Example Outcomes

Golden path to production

Solve Security
Problems Once, not multiple times

Reusable, Secure Templates

What is a product, and how to ensure it is successful?

Let’s talk about productization, defined as the process of developing or altering a process, idea, skill, or service to make it marketable for sale.

Usually this term is used when selling products to the public, however in this context the customers of your cloud security product will be within your organisation, likely a combination of information security and the engineering teams.

Just as if you were selling to the public it is absolutely paramount to listen to the voice of the customer, in this scenario it’s likely the customers may have differing opinions. With engineers wanting to focus on delivering value through their products without additional security overhead ,whereas information security will be keen to ensure that new and existing cloud workloads are de risked across the estate.

When thinking about productizing an element of your Cloud security you should think about the following areas to ensure it is a success, many products fall into the trap of not covering off the basics.

Problem Statement

What is the problem you are trying to solve, this could be a risk or threat to your cloud environment and how will your product drive value in this area?

Success Criteria

What is the problem you are trying to solve, this could be a risk or threat to your cloud environment and how will your product drive value in this area?

Democratised backlog

What is the problem you are trying to solve, this could be a risk or threat to your cloud environment and how will your product drive value in this area?

Clear Roadmap / Product Journey

by listening to your security stakeholders and engineering functions, a clear published roadmap on what problems the team will tackle next and their delivery date.

Regular forums and reveals

it’s very common for organisations to implement security products and toolsets without consulting the end user, don’t fall into this trap and ensure you provide multiple forums for stakeholders and subject matter experts to input into the platform.

User First

User experience is such an important hallmark of any product, the product should have great documentation and be easy to use or consume.

How to use products in the context of Cloud Security?

By treating your cloud security a product, with a dedicated set of engineers and product owners you can start to offer this as a service to your engineering and risk functions. I'm a huge fan of the "paved road" analogy - your goal will be lowering the barrier of entry to running secure cloud workloads! In order for a tool /product to be widely accepted it must provide tangible value to it's customers.

Your security product team/s could be responsible from everything to analysing and implementing third-party toolsets such as vulnerability scanners through to writing custom solutions to report and remediate mis configured resources within the cloud estate.

Some examples of cloud security products that could deliver value are as follows, it's worth noting that every companies architecture is different so it's worth selecting products that provide the most value based on the voice of your customer!

Cloud Account "Vending"

Enabling self service around provision of Cloud Accounts ensuring a baseline security policy is applied, reducing the barrier to running secure workloads for engineering teams.

Compliance as Code

A centralised set of code defined security policies that govern your cloud environment in line with your information security policy. This may include dashboards and reports to ensure teams are accountable for their solutions.

Hardened Infrastructure Modules

Infrastructure modules using tools such as Terraform that are built in accordance to security best practice, that teams can both consume and contribute to.

Cloud Health Checks

The public cloud has so much rich data available via APIs, cloud health checks aggregate this information and provide a view of compliance over time for leadership and infosec.

The benefits of product focused Security

We've talked about the definition of a product, how to launch a successful product and even some examples of potential cloud security products your organisation could work on, now let's talk about the value these products can bring.

Reducing barrier to entry for engineering teams

Teams can focus on innovation and delivering features to keep the customer happy. Whilst your suite of security products and guardrails keep their workloads safe.

Bake lessons learnt into reusable templates

Teams across your business will constantly be getting feedback from security reviews, audits and other assessments. Any lessons learnt can be factored back into the security product so they are not faced again.

Solve problems once, not multiple times

This problem particularly effects large organisations with lots of moving parts, but treating your security as a product ensures that feedback will be directed to the right team to solve once, and not leave it lingering to be solved multiple times by various different teams.

Inner-Sourcing and collaboration

Technology is a moving target, inner sourcing is the practice of sharing code across teams internally. This fosters a large sense of collaboration which means the product will likely be kept up to date by the community as new regulations land etc.

Golden path to production

Taking an idea from a sandbox to production can be a daunting task for product teams. Having a set of pre-approved modules ready for consumption can really help on this journey.

With the right investments in security products you can ensure you can continue to deliver value at pace in the Public Cloud, whilst lowering the risk of a costly data breach or disruptive cyber-attack on your environment.

How we have productized Security within KPMG's Cloud Engineering Practice

The KPMG Cloud Engineering Practice has over **200 engineers based across UK**, Malta and India, responsible for thousands of cloud workloads across our **AWS, GCP and Microsoft Azure** communities. In order to support this scale we developed our Platform Centre of Excellence team, with a designated squads dedicated to **DevSecOps, IAM** and **Developer Productivity**. This team bridges the gap between our infosec and risk functions and our diverse software engineering teams.

We have made several key investments in our own inner-sourced security products to continually monitor our assets to ensure they are compliant with our **"secure by default"** ethos. We have also heavily invested in developer productivity synergizing both feature velocity and security.

Lastly in combination with our expert team of architects and cyber professionals we regularly help customers across all industries deliver secure value through the public cloud using our established **Cloud Care** product suite and engineering expertise. **Cloud Care** is an expansion of our incubated internal security tools and practices that allow a rapid and accurate identification of cloud risk and compliance. Our toolsets also allow customers to trend their compliance journey over time – with visualisations suitable for various stakeholders. From customers starting out on their cloud journey to those running enterprise scale landing zones, we can work with you to combat the threats facing your workloads, please reach out.

The Cloud Threat landscape continues to amplify, listen to your internal customers and drive secure engineering outcomes by productizing your cloud security!

Contact our author(s) for assistance

Arron Dougan

Lead DevOps Engineer –
FS Cloud Engineering

✉ Arron.Dougan@KPMG.co.uk

Arron is a Lead Engineer within the Cloud Transformation team at KPMG holding broad technical experience ranging from service management to enterprise grade cloud architecture. Arron has spent most of his career designing, implementing and consulting on secure solutions using Microsoft Azure and more widely DevOps implementation and culture shift.

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.

kpmg.com/uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Document Classification: KPMG Public

CREATE: CRT143124A