sysdig

BRIEF

6 Tips to Help Strengthen Financial Services Security in the Cloud

A panel of experts from the financial services sector and Sysdig met in London to discuss the security and compliance challenges facing businesses as they move to the cloud. They included:

- Kevin Fielder, CISO, Mettle Bank
- Bernd Malmqvist, Director Platform Engineering, Worldpay
- Anna Belak, Director of Cybersecurity Strategy, Sysdig
- Glenn Wilson, Author of DevSecOps – A Leader's Guide

Here's their forecast: cloudy with a chance of curveballs

As early adopters of cloud, financial service providers have been quick to realise its potential for fast, agile application innovation. But this new-found freedom has come with a price. Cloud environments also create new security unknowns that attackers are exploiting all too eagerly. With customer financial details easily tradable on the dark web, it's no surprise that financial services and insurance had the **second-highest share of cyber attacks in 2022**.

In this guide we've curated the panel's expertise and experience into 6 actionable takeouts that can help you to better navigate cloud security.

01 Cloud security is everyone's business

Security can be seen as the 'team that says no', but often they only get a look-in when a product is on the verge of release. Especially in start-ups, DevOps culture may encourage unrestricted use of new programs while viewing security as a systemic issue developers can do little about. To mitigate risk and minimise rework, security must move up the pipeline and become an integral part of product teams, for example, by approving vulnerability scans during development. Providing product teams with security guardrails helps free up developers to focus on what matters and what customers care about, like building outstanding login and payment flows.

> "In a highly regulated industry, the challenge is to move fast and deliver great features while also staying secure. Developers need guardrails from security teams, so they can put their thinking power into making products awesomex."
>
> mettle. **Kevin Fielder**
> CISO, Mettle Bank

Action

Bring security champions into product teams to encourage closer collaboration, mitigate risk and allow development teams to share their deeper understanding of the product and business.

54%
of financial institutions expect to shift at least half of their workloads to the public cloud over the next 5 years[1]"

02 Managing vulnerabilities requires runtime context

Cloud automation has revolutionised application development, helping to speed up build and reduce deployment times from days to minutes. But those same automation capabilities can run out of control when it comes to security, flagging up vast numbers of vulnerabilities for security teams to wade through. To stop teams from being overwhelmed, security tools must not only find vulnerabilities, but also provide context so that the most critical issues can be addressed first – that is, those exploitable at runtime.

> "Organisations must use technology and automation in a smart way. Implement only if it's solving a business problem, not just because it's the next big thing."
>
> **Glenn Wilson**
> Author of DevSecOps – A Leader's Guide

Action

Choose a cloud security solution that allows you to prioritise vulnerabilities with runtime context.

[1] *Source:* **McKinsey**

03 Not every vulnerability needs fixing immediately

Rising vulnerability disclosures and elevated supply chain security concerns are deluging developer teams with risk decisions they're ill-equipped to make. In reality not all vulnerabilities have to be addressed straight away, but developers may not be the best judges of which ones need urgent attention – and given the business implications of a security failure, the temptation is to be overly cautious. To minimise delays to pipeline, security and engineering teams must work together to prioritise risks and agree a timeframe to fix vulnerabilities, based on the organisation's risk tolerance.

Action

Agree on a tiered timeframe for fixing vulnerabilities, based on your organisation's risk appetite. Commit to adapting these over time as your business evolves and grows.

> "You can't shut everything down because of a vulnerability. A risk-based approach works best, where you have the option of going into production with vulnerabilities, but with a defined timeframe to fix them."
>
> worldpay from FIS
>
> **Bernd Malmqvist**
> Director Platform Engineering, Worldpay

04 Shift-left is only one part of securing financial services

Shift-left is about catching security issues early in the application lifecycle. But new threats are constantly emerging, and realistically it's impossible to ship something completely impervious to attack. Chances are, at some point a zero day will hit that no-one could have predicted – and when that happens, organisations will need to activate their 'shield-right' capabilities by quickly identifying the affected workloads, and prioritising them for mitigation and remediation. It's why real-time threat detection and response are a critical pillar of any security programme, utilising tools that surface the necessary context to understand impact and take action immediately.

Action

Make real-time, end-to-end threat detection and response an integral part of your security programme. Ensure your incident response process is solid by regularly practising it in simulations or tabletop exercises.

1 in 5
cyberattacks targeted financial service providers in 2022[2]

[2] *Source:* **Statista**

05 Cyber insurance won't compensate for lack of due diligence

Rising vulnerability disclosures and elevated supply chain security concerns are deluging developer teams with risk decisions they're ill-equipped to make. In reality not all vulnerabilities have to be addressed straight away, but developers may not be the best judges of which ones need urgent attention – and given the business implications of a security failure, the temptation is to be overly cautious. To minimise delays to pipeline, security and engineering teams must work together to prioritise risks and agree a timeframe to fix vulnerabilities, based on the organisation's risk tolerance.

Action

Assess whether your organisation would benefit from cyber insurance, but keep investing in a strong cybersecurity program and vulnerability management. Note that insurers are increasingly refusing to pay out claims where the victim was demonstrably negligent.

06 Security should be made easy – and fun

Security starts with people. Your employees are your first line of defence, but they can also be the weakest link if they're not vested in your organisation's safety, or believe it to be other people's business. Companies must bring everyone along on their cloud security journey with engaging training and education programs tailored to people's roles. Technology must enable non-security experts to do their jobs safely and ensure security is always the easiest option to choose. By making culture a pillar of their security strategy, organisations will give themselves the best chance of withstanding attacks, fostering collaboration and delivering growth.

Action

Make building a strong security culture a key pillar of your security and company strategy.

> "Building a security culture is about motivation. People have to care about your business. Incentives work, and they don't necessarily have to be security related."
>
> sysdig — **Anna Belak**, Director Thought Leadership, Sysdig

Wrapping up

Cloud is empowering financial service providers to innovate at speed, but is also creating new security and compliance challenges as attackers take advantage of misconfigurations and visibility gaps. Shifting security left in the development pipeline is important, but without proper process and context, this can overload developers with remediation tasks and slow down releases. Given that Sysdig research shows 87% of containers contain high or critical vulnerabilities, but only 15% of these are exploitable at runtime, security tools that provide runtime context can dramatically reduce workload by helping development teams prioritise the most critical tasks. This, along with real-time data enabling fast response to threats, is key to safeguarding systems and freeing up teams to focus on what they do best – building the products your customers want.

About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

Sysdig. Secure Every Second.

To learn more about Sysdig, visit **sysdig.com.**

READY TO POWER UP YOUR CLOUD SECURITY? →