RAPID7

Rebalance Your Security Portfolio:

How to Make Cloud Security an Asset for Financial Services Companies

Businesses of all shapes and sizes have embraced the benefits of the cloud. From speed to flexibility and scalability to cost savings, the cloud helps organizations innovate faster and more efficiently to provide an enhanced customer experience. It's no surprise, then, that the cloud is a top priority for businesses; Gartner has forecasted cloud services spending will reach $482 billion in 2022.

Financial services companies have been at the front of the pack on cloud innovation. But the digital transformation required to meet customer demand at scale must be balanced with security in the cloud. And this is often easier said than done, especially in such a highly regulated industry. Financial services companies — and in particular, enterprise-sized organizations with legacy tech infrastructure and multi-cloud environments — face unique pressures when it comes to the cloud. So security can quickly become a major roadblock to continued innovation.

It doesn't have to be that way. This eBook is designed to help large financial services organizations gain actionable guidance on turning cloud security from a liability into an asset that drives innovation forward.

WHO THIS GUIDE IS FOR:

Security leaders and senior practitioners at large financial services organizations with complex multi-cloud environments.

We'll share:

1. The unique security challenges faced by finserv companies

2. Three pillars to focus on as you work to balance innovation with cloud security

3. 2-3 practical steps to help apply each pillar to your organization

RAPID7

DEFINING THE PROBLEM

Why does cloud security feel like it's holding innovation back for enterprise financial services companies, right when you most want to accelerate their cloud adoption?

The answer involves a range of factors, including:

- **Strict regulations**
- **Complex hybrid and multi-cloud environments**
- **Intense competition**
- **Highly publicized data breaches**

But we don't have to tell you; you're living it. Here's a high-level overview of these complexities.

Regulatory Compliance — Compliance can slow innovation if you don't have a strong strategy in place or the technology to support it.

Technical Debt — On-prem infrastructure that can't be turned off, coupled with the hesitation to abandon the tech your organization has heavily invested in, can lead to a nightmare of disparate infrastructure technologies that don't integrate well together.

Internal Politics — No one likes to admit it, but (especially at very large companies) different priorities and personalities can create clashing over the best way forward, at times leading to more technical debt or suboptimal conditions for innovation.

Competition for Customers — Continuously offering customers new, higher-quality experiences is a requirement to succeed in today's highly competitive financial services market.

Competition for Talent — Clunky and disparate tech stacks are not exactly appealing to engineers. Combined with the dynamics of the Great Resignation, this can make it even harder to attract and retain top tech talent.

The Impact of Data Breaches — The cost of a data breach goes beyond just dollars and cents; reputational damage, and a fear of exposing the organization to greater risk, can unintentionally hinder strategic digital transformation efforts.

Board Involvement — Friend or foe? The presence of more cybersecurity experts on boards means security leaders and practitioners will find their work under the microscope.

RAPID7

MULTI-CLOUD IS THE FUTURE

Gartner research shows 81% of organizations using the cloud have a multi-cloud strategy. Some do this to avoid lock-in, maximize investment, or to cherry-pick the best solutions from several vendors. This is especially true for financial services organizations. In fact, data from our Trust in the Cloud Report shows **financial services organizations use more than 15 different cloud services on average.**

It makes sense; the cloud is constantly evolving and changing, and most companies realize there are benefits to embracing different providers rather than sticking with just one. These days, AWS launches 10 new services or features every time they have a conference. And it's not just the big players that are making waves in the cloud. AWS, Azure, and GCP — once the only players in the space, for all intents and purposes — are increasingly finding competition from smaller players with more niche cloud services and applications.

Plus, Kubernetes and container usage in general is on the rise. Many financial services organizations are adopting Kubernetes as a way to access the benefits of the cloud with less hassle. Across all industries, 31% of backend developers used Kubernetes in 2021, a 67% increase from 2020. Containers and serverless applications are helping financial services companies stay innovative without forcing developers to continually manage cloud infrastructure.

> **Infrastructure as code (IaC) is helping financial services companies stay innovative by allowing developers to take control of infrastructure without needing to become experts. As long as this is done with a "security by design" mindset, it's a win/win proposition.**

Of course, with complex multi-cloud and containerized environments come security challenges, particularly related to visibility. Gartner predicts that, through 2025, **99% of all cloud security failures will be caused by customers, not cloud providers.**

To that end, Rapid7 recently looked at 121 publicly reported data exposure incidents. We found that misconfigurations are the main cause of breaches, with 25% resulting from misconfigured permissions on AWS buckets. For financial services organizations, this type of risk is untenable.

The good news is that with some planning and good hygiene (i.e., you know what you're exposing, and what safe and resilient configurations look like) and automation (i.e., you have automated processes in place to monitor said configurations, alert on errors, and remediate automatically when possible), you can avoid seeing your organization's name in breach headlines.

PRESSURE IS MOUNTING

There is major pressure on enterprise financial services companies to stay innovative and nimble as M&A-driven consolidation and tech-driven disruption bring tougher competition for customers to the market. Breaking through the noise means you'll need to be constantly innovating — staying on top of the latest trends and consumer desires.

Success can't be achieved without the cloud. But it also can't be sustained without a complete and holistic cloud security strategy.

Below we'll cover the three pillars of achieving cloud security as a financial services organization, what these pillars mean in practical terms, and a few examples of how to apply them to your organization.

RAPID7

PILLAR 1

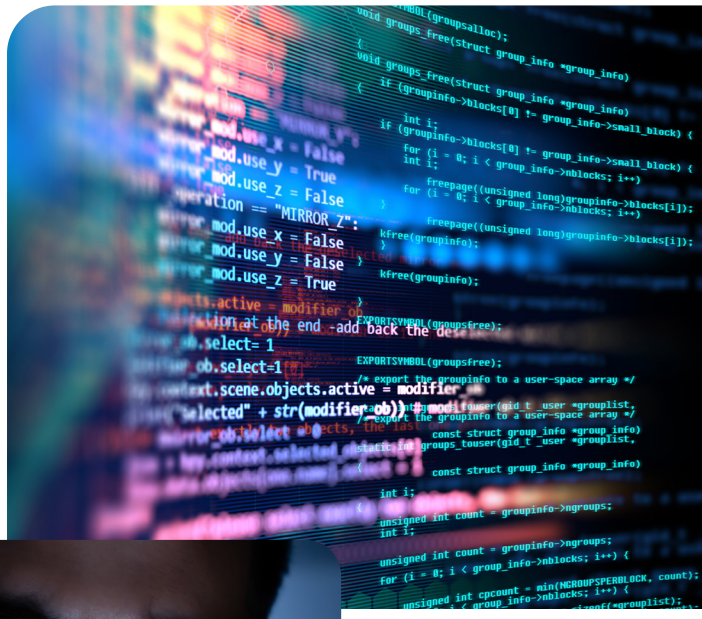
Achieve security by design

Balancing cloud security and compliance with innovation is mission-critical for financial services companies, so meet engineers where they already are: in the code.

What this means, in practical terms

The cloud is dynamic. Because of that, security teams struggle to keep up to the overwhelming volume of potential issues, including:

- **Infrastructure misconfigurations**
- **Workload vulnerabilities**
- **Escalating permissions**
- **Shadow IT**
- **External threats**
- **And other sources of risk**



Security teams with a reactive approach generally do not fare well in this reality. **For this reason, preventing the majority of cloud security problems from occurring in the first place is the key to staying nimble and innovative without introducing unnecessary risk.** It's also the key to reducing friction and increasing harmony between security and development teams.

Most large financial services companies have adopted DevOps and, as a result, the role of the security teams has shifted. As many organizations look to integrate security into the DevOps culture via DevSecOps, it is important to minimize real or perceived friction between teams with competing short-term priorities (but the same long-term goals). Legacy approaches to security, for example, can cause bottlenecks that demotivate talented engineers, or lead them to find workarounds, introducing increased risk and more frustration between teams.

A key part of the DevSecOps evolution is adopting modern developer-friendly security paradigms, like infrastructure as code, security by design, and automation. These security paradigms support the developer-driven, API-centric, and infrastructure-agnostic patterns of innovation.

Adopting forward-thinking security tools and processes increases speed and flexibility and keeps engineers happy (which generally keeps customers happy, too).

HOW TO ACHIEVE THIS GOAL

Continuous compliance and security is a necessity for financial services organizations. It is best achieved through "security by design." Here's three key tips:

- **Adopt developer-friendly security tools:** Provide self-service access to security checks and balances for developers right in the code. This way they can feel confident about security without being bogged down.
- **Embrace full-lifecycle security tools:** Shift security and compliance policies left into the CI/CD pipeline, allowing security professionals to evaluate the risk of Infrastructure as Code (IaC) templates before they are built.
- **Choose security tools that integrate well:** Security tooling should integrate with your CI/CD orchestration tools, so developers can build more secure applications faster. Not all tools support all cloud environments, so choose wisely based on current reality and future plans.

In summary, invest in cloud security tools that are easy for developers to use without sacrificing security or compliance.

PILLAR 2

Achieve security at scale with automation

Traditional and manual approaches to identifying and remediating risk don't work anymore — there's just too much noise in the cloud. Automation is the only way forward.

What this means, in practical terms

Just as climbing Mt. Everest without any gear is beyond the limits of the human body, managing security manually in the cloud is beyond the limits of the human mind. The cloud has outstripped the human capacity to manage. To achieve a security environment at scale, automation and orchestration are necessary.

Automation and orchestration can free up security professionals to focus on more strategic tasks and empower devs to handle more of the security workload. Automating (and ideally documenting) processes also means that, if there is team turnover, important controls and policies don't slip and create risk.

Automation also helps save both time and money in the face of ever-evolving threats and regulations. **McKinsey estimates that automation can empower agile ways of working that reduce issue resolution time by 30% to 50%**. Reducing alert fatigue can also help teams focus on the most pressing issues and avoid letting anything important slip through the cracks.

HOW TO ACHIEVE THIS GOAL

- **Automate policy application:** When regulations or benchmarks change or a new service or solution is implemented, compliance needs to be re-assessed and any policy updates quickly applied. To do this, financial services organizations must invest in solutions that automate policy application across all services. This ensures a policy can be changed once and applied everywhere. Without this, the process of maintaining compliance can be extremely tedious.

- **Automate remediation:** Incident response time skyrockets when security experts have to sift through large amounts of data to figure out what happened. It's best to invest in security tools that can auto-remediate at least some security issues. Ideally, they should also be able to automatically fix misconfigurations and address vulnerabilities before exploits can take place.

- **Automate identity and access management:** One of the biggest sources of risk is privilege escalation, especially as organizations adopt more and more cloud and container services. For this reason, implementing an identity and access management tool that can automatically handle user provisioning or deprovisioning can drastically reduce risk. For this to work, your organization should employ a least privilege access framework. As the saying goes, "identity is the new perimeter." (P.S. It's challenging enough to manage human identities and ensure proper access controls are implemented across multi-cloud environments; Gartner predicts managing machine identities is the next challenge on the horizon…)

It's important to select tools and strategies that can automate as much as possible of rote security and compliance tasks because, by nature, the multi-cloud, hybrid environments that large financial services organizations are dealing with are too complex and ever-changing to be manually secured.

PILLAR 3

Simplify compliance and future-proof security

In highly regulated industries, streamlining cloud security is about having complete visibility and control across your entire multi-cloud infrastructure. There's a strong desire in many financial services organizations to make compliance more routine and automated so it's not a huge burden at audit time. This reduces the risk of noncompliance, regulatory fines, and actual security breaches.

What this means, in practical terms

Organizations need **full visibility** into all cloud resources at all times in order to achieve continuous compliance and security. Obviously, this is a tall order.

To this end, cloud security posture management (CSPM) is key. **Security posture management tools can reduce vulnerabilities using continuous scanning to identify and remediate configuration mistakes.** Gartner argues that security posture management will have an increasingly significant role over the next five to ten years.

Another facet of simplifying compliance and future-proofing security is evolving the way we think about identity and access management (IAM). Credential theft is an increasingly popular way for attackers to gain access to sensitive data, especially at financial services organizations. In fact, it's the number one tactic used in security breaches, according to Gartner. Because of this, laws, such as New York state's SHIELD Act, require organizations to meet certain standards to safeguard credentials.

The level of monitoring, investigation, and remediation necessary to meet these standards is only possible to do at scale with automation.

HOW TO ACHIEVE THIS GOAL

- **All of the above:** Fortunately, the tips shared above around security by design and automation will also go a long way toward helping you simplify compliance. But we've got two more pieces of advice below:

- **Single pane of glass:** Choose security tooling that enables unified visibility and monitoring across your whole multi-cloud environment. You want to invest in a platform that is future-proof in the sense of being able to keep eyes on your whole infrastructure environment, even as you add new services. A single pane of glass is the best path to meeting compliance.

- **Out-of-the-box policies:** Invest in security tools that can automatically apply the compliance and industry standards that are relevant to your business and industry, such as PCI DSS, HIPAA, GDPR, SOC 2, ISO 27001, CIS Benchmarks for AWS, GCP, Azure and Kubernetes, NIST CSF, NIST 800-53, FedRAMP CCM, and CSA CCM. This way there is no need to manually review and implement changes when new policies are released or new services are added to your environment.

Unified visibility and smart reliance on automation and dev-friendly security tools will help your financial services organization maintain compliance no matter how fast you innovate and change.

Summary: Embrace comprehensive, cohesive cloud security

Today's financial services organizations are doing their best to innovate safely by hiring teams and spending money on security, but they also need to empower security professionals to focus on the most strategic areas, and empower developers to handle more aspects of security themselves (without forcing them to become subject matter experts).

Because of the intense competition in the financial services industry, organizations must find a way to innovate better and faster so they can continue to win new business and retain current customers. But it's crucial to balance innovation with the need to mitigate risk. And the best way to do that is to ensure a secure cloud environment with complete visibility.

You need to invest in comprehensive and cloud-native security solutions, not piecemeal point solutions. **The more comprehensive your approach to cloud security, the less likely you are to be a target.** Investing in a cloud security strategy that upholds the three pillars above (security by design, relying on automation, and simplifying compliance) will help future-proof your business and decrease risk while enabling continued innovation. In this way, you can achieve cloud security that helps drive innovation forward, instead of slowing you down.