CIO

SPONSORED CONTENT

Building a More Advanced Cloud Security Framework for Financial Institutions

Achieving strong security across multicloud environments is paramount.

Clouds have transformed the enterprise and emerged as mission-critical tools that support faster, better, and more flexible business frameworks. Today these systems handle enormous, complex workloads that power financial networks, manufacturing operations, biomedical research, and much more.

Yet, despite all the advances, there are growing challenges associated with managing clouds and ensuring that they remain cybersecure. A recent IDG Market Pulse survey examined enterprise cloud adoption and how various factors shape enterprise security strategies at financial services firms. This research was conducted among 300 IT leaders at companies with more than 1,000 employees in the U.K., France, and Germany.

The results, which are threaded throughout this paper, provide a window into the demanding and rapidly changing security requirements surrounding hybrid-cloud and multicloud adoption. Typically, financial institutions rely on a mix of strategies, processes, vendors, and applications to build out and protect cloud infrastructure.

Unfortunately, this approach can mean that organizations end up with disjointed and sometimes incompatible tools and strategies. Although many products and processes may be well designed and useful, especially within a single application or cloud, they often deliver limited value across a multicloud enterprise. This lack of a single unified view may introduce gaps that make it difficult to fully protect clouds and the data that resides within them. In some cases, these issues can extend to on-premises legacy solutions.

paloalto NETWORKS

accenture

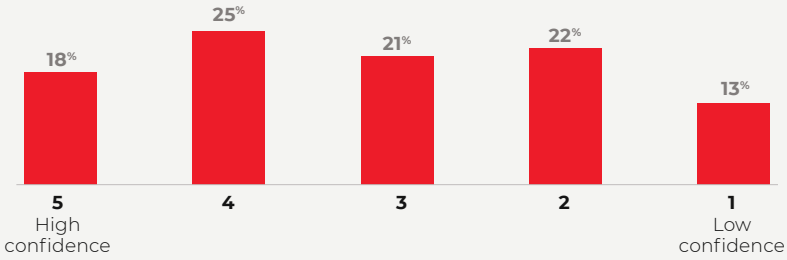
Figure 1.

Public Cloud Security Challenges

Source: IDG

Figure 2.

Confidence in Public Cloud Workload Security Is Relatively Low



Source: IDG

Clearly, there is a need to rethink, reevaluate, and reassess one's cloud strategy and consider ways to adopt a more centralized and overarching model for multicloud and hybrid-cloud management and security. This model must encompass people, processes, and technology.

The State of Cloud Security

It is no secret that financial institutions are turning to the cloud for a growing array of business and IT needs — many of them mission-critical. Today 98% of the respondents use software as a service (SaaS), 92% rely on infrastructure as a service (IaaS), and 87% tap the cloud for platform as a service (PaaS). Increasingly, these solutions are table stakes for doing business.

Although the benefits — including an ability to gain advantages in speed, flexibility, performance, innovation, and costs — are clear, fundamental challenges have emerged *(see Figure 1)*. These include visibility into cloud environments, integration with on-premises legacy solutions, and the learning curves for cloud service provider-specific tools.

Yet, the challenges do not end there; they are magnified by multicloud environments. The survey found that 31% of the financial institutions surveyed have workloads on AWS, 26% on Azure, and 21% on Google Cloud. In addition, these organizations typically rely on other cloud vendors to supplement or complement their cloud environment as needed.

These public and hybrid clouds are used for many different tasks, but they increasingly hold valuable and sensitive data, including personally identifiable information (PII), Payment Card Industry (PCI) data, protected health information (PHI) data, and intellectual property.

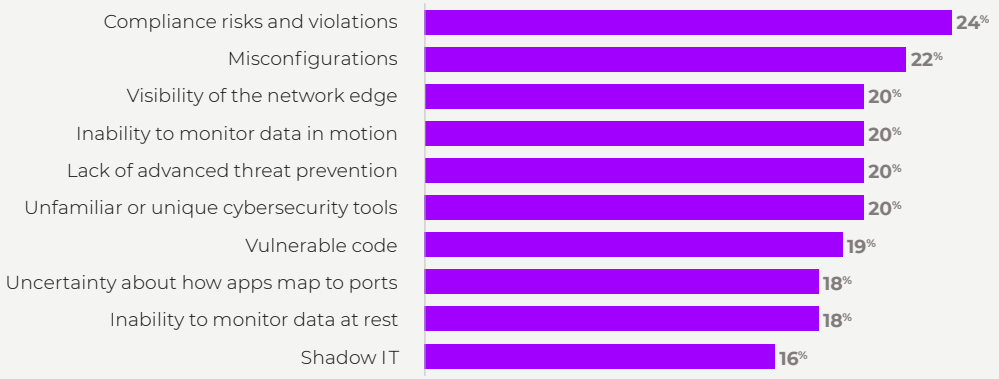
Protecting all this data is critical. Yet, 56% of the respondents from the surveyed financial institutions said that they have moderate to low confidence in their cloud security *(see Figure 2)*. Only 18% rated their confidence level as high.

Although it is good that organizations acknowledge today's multicloud security challenges, it is also concerning, because these low numbers often reflect real-world vulnerabilities and tangible risks. For example, 24% said that compliance risks and violations are a major cause of concern. This also impacts organizations in other, less apparent ways:

- **25%** are hesitant to move workloads because of security concerns.
- **23%** said that public cloud impacts their ability to use IoT data.
- **22%** echoed the concern about artificial intelligence/machine learning (AI/ML) data.

Figure 3.

Financial Institutions Cite Multiple Concerns With Public Cloud Workload Security



Source: IDG

Furthermore, these challenges continue to grow. More than half (51%) of the survey respondents have no plans to increase their cloud security budget in 2022.

Contrast this finding with the fact that 79% of workloads in public clouds are now mission-critical or a combination of mission-critical data and other forms of data. "Organizations have become reasonably comfortable with on-premises security, but the cloud introduces new challenges — including how multicloud environments intersect with on-premises systems," says Accenture Security Managing Director Sanjeev Shukla.

The takeaway: Many organizations are finding that they are limited by current cloud security tools and technologies. They're also discovering that their strategies and processes are lagging — and often not up to the security challenges multicloud environments create. As a result, they are unable to protect their data and assets in the way they require.

Minding the Gaps: The Risks Grow

There is good news: Financial institutions recognize the need for a more comprehensive and connected cloud security framework. Although respondents are generally satisfied with the security point solutions they now have in place, 74% believe there is room for improvement.

The research found that concerns center on five key areas *(see Figure 3)*.

Not surprisingly, the situation is likely to become even more challenging in the months and years ahead. At present, about 28% of financial services workloads are in the public cloud. But 33% are destined for the public cloud, companies reported. This will add to the volume and variety of data and also increase the complexity of multicloud environments, including security.

Financial institutions are focused on improving security in several critical areas:

- Cloud infrastructure entitlement management (**77%**)
- Cloud security posture management (**76%**)
- Cloud access security broker **(75%**)
- Cloud workload protection (**75%**)
- Application programming interface security (**73%**)
- Security information and event management (**73%**)

Other key areas of concern include devsecops tools, cloud network security, data loss prevention (DLP), Kubernetes Security Posture Management, and microsegmentation.

Intentions are a good start, but throwing more money and technology at the problem will not get the job done. In reality, financial institutions are reaching an inflection point. Using an assortment of point tools and technologies to address various security risks leads to additional staff time, cost, and technical debt. Increasingly, teams grapple with the lack of central visibility into public and private cloud security, multiple pricing and licensing models, and a lack of support for containers or serverless functions.

> "In many cases, cloud management and security frameworks wind up becoming very human-intensive."
>
> *Sanjeev Shukla,*
> *Security Managing Director, Accenture*

There are also issues involving training, malware scanning, scalability, interconnectivity issues, support spread across multiple vendors and tools, and difficulty using various products and achieving ROI. In the end, it is not unusual for financial institutions to seek a more effective and sustainable path.

"In many cases, cloud management and security frameworks wind up becoming very human-intensive," Shukla says.

Making Cloud Security More Manageable

The solution is a more comprehensive and holistic approach to cloud security. Organizations benefit when they develop an overarching strategy, identify more effective processes, and build the right technology foundation. This includes a single dashboard with a unified view of resources, along with a security model that connects, automates, and simplifies tasks. Such a framework improves protection and lowers costs.

Consolidating tools and technologies makes it easier to control, manage, and protect clouds — and all the data stored in them. Various initiatives, including devops and devsecops, become easier and more manageable.

"A mature cloud management and security framework greatly increases the odds that templates, code, containers, and various other components are secure — and that they remain secure as they are used and reproduced across an organization," says Taylor Smith, senior product manager for Prisma Cloud by Palo Alto Networks.

To be sure, the right cloud security platform can deliver a broad collection of technologies that help control, manage, and protect clouds — and the data stored in them. It can aid in establishing a cloud security framework that balances people, processes, and technology to deliver the highest-possible level of protection. Moreover, it can work with on-premises security to ratchet up the overall level of protection.

All of this points to the need for a platform that is API-based, highly extensible, and highly customizable. This approach makes it possible to reach out and connect to whatever service is needed. With a single vantage point and a high level of connectivity, an organization can see dramatic improvements in cloud security posture management, cloud workload protection, cloud network security, and cloud identity security. In the end, all of this takes a financial institution to a higher and more secure level.

As Smith puts it, "The goal is to move from a programmatic model rooted in legacy on-premises systems to a far more effective collaborative security model that can simplify and automate diverse tasks and processes."

A New Era Emerges

Today's multicloud environments hold enormous and growing volumes of valuable data, and they increasingly manage mission-critical processes. Although they deliver a remarkable array of features, capabilities, and benefits, they also create significant operational challenges and security risks. As financial institutions accumulate cloud services, applications, and data, the stakes grow and the dangers increase.

Make no mistake: When financial institutions replace multiple cloud security point solutions with a unified cloud-native application protection platform, they're far better equipped to navigate today's chaotic and demanding business and IT environment. With a broad and deep view into the clouds and a solid security foundation that extends to on-premises systems, they are ready for whatever changes and challenges come their way.

Visit Palo Alto Networks and Accenture to evolve your comprehensive cloud security strategy.