FORTINET

POINT OF VIEW

The Future of Cloud for Finance

10 Cutting-Edge Cybersecurity Strategies

In the dynamic realm of finance, a ceaseless quest for innovation, value augmentation, and industry-wide metamorphosis has become the emblem of success. The ubiquitous cloud has emerged as a steadfast ally. But what role is cybersecurity playing to power the sector's digital endeavors?

Key Highlights

- Finance adopts cloud for cyber resilience and a security-focused culture
- DevSecOps breaks silos, fostering a new operating model for success
- Security-as-Code streamlines cloud security, enhancing resilience and compliance
- CCoE empowers alignment for innovation and future-proof security
- Streamlined vendors and partnerships enhance cyber resilience and readiness

Revolutionizing Risk and Compliance: Cloud-Powered Resilience

As the financial sector advances cloud adoption, visionary leaders have recognized it as a unique gateway to optimize risk management, fortify resilience, and simplify the intricate web of compliance obligations. Achieving excellence in this endeavor is essential for maintaining trust with customers, with regulatory bodies, and for propelling the overarching goals driving cloud adoption itself. Embracing these new dynamics extends beyond mere technology adoption; it signifies a fundamental shift in the sector's operating model.

Fusing Innovation and Resilience to Drive Finance Success

As organizations that are vital to global economies, the transformation taking place in the finance sector with cloud holds immense significance. The resilience of the sector's digital services and the protection of its data are paramount to entire ecosystems. Several innovative strategies are now essential to seize this opportunity and avoid potential challenges.

Cloud could unlock

$60-80B in 2030

EBITDA run-rate in the banking sector alone.

McKinsey

Cybersecurity plays a key role in helping to ensure businesses are respected as trustworthy entities. Improved profitability and better customer retention are the top two advantages.

KPMG Cyber trust insights 2022

To unlock the value of your DevSecOps transformation, start with **people**.

Deloitte

1. Cultivating a Strategic Cybersecurity Culture

In this age of cloud adoption, cultivating a culture of cybersecurity, guided by top leadership, has emerged as a potent strategy. Financial sector leaders are restructuring roles and responsibilities to enhance their commitment to innovation and cyber resilience by embedding cybersecurity into their digital strategy. Embracing cloud and the DevSecOps ethos demonstrates a deep commitment to the transformation of practices, culture, and mindset. As executive leaders dismantle traditional silos to bridge gaps between development, operations, and cybersecurity, this new era has the keen attention of employees, partners, regulators, and shareholders alike.

Decreased risk and improved security is one of the **top 3 business outcomes** realized with cloud.

2023 Cybersecurity Insiders, Fortinet Cloud Security Report

2. Enhancing Resilience in the Cloud Era

The cloud is often perceived as a risk by both the business and regulators, but it simultaneously offers an avenue to bolster security posture and alleviate the burdens of security and compliance, if navigated correctly. By embracing the concept of "shift left", integrating security and security policy as code into automated workflows, the cloud offers a transformative opportunity in risk management. From proactive, continuous risk assessment, to accelerated threat detection and response, your teams and the business reap the rewards of reduced friction as they navigate a plethora of global regulatory and security frameworks.

Security as code (SaC) has been **the most effective approach** to securing cloud workloads with speed and agility.

McKinsey Insights

3. Security-as-Code (SaC): A Paradigm Shift

Leading organizations are revolutionizing their security paradigms with SaC. Far more than just a technology shift, SaC heralds a cultural and operational metamorphosis that sits at the heart of security in the cloud era. The very embodiment of a "shift left" ethos and self-service security automation, SAC lays the groundwork for robust, bespoke but automated end-to-end workflows. A streamlined approach that unlocks the full potential of cloud innovation and cyber resilience.

4. Empowering Project-Centric Cloud Freedom

Empowering teams with the autonomy to select the ideal cloud platform for each project is paramount. Simultaneously, they must possess the confidence that stringent security and regulatory prerequisites will seamlessly be met, without unwarranted hindrances. In this context, speed and resilience must be instilled as allies, rather than adversaries. Enter the Cloud Center of Excellence (CCoE), a best practice approach that fosters alignment and optimizes internal expertise to construct a secure, automated cloud foundation. This foundation empowers business unit teams to independently leverage validated, scalable, and repeatable best practice designs.

To ensure cloud adoption success, organizations must have the right skills and structure in place. The optimal way to achieve this is by setting up a centralized **cloud center of excellence**.

Gartner Insights

Automated security operations reduce the time to detect and respond to incidents from weeks to minutes, avoiding up to **$1.39M** of risk per year.

Fortinet ESG Economic Validation

5. Unifying to Reduce Complexity

The adoption of cloud provides an opportunity to reevaluate existing cybersecurity tools and practices, seeking avenues to reduce complexity and friction in the journey toward fully automated workflows. The presence of multiple cloud platforms or internal domain silos does not justify the existence of multiple security tools performing identical functions. This complexity creates an extensive list of potential complications, including heightened friction, elevated risk of misconfigurations, disparity of security policies, extended time to detect and respond to threats, and elevated integration costs, as well as skills challenges. Cloud offers an opportunity to tackle this complexity by adopting a cybersecurity platform approach and standardizing tooling across your digital estate.

6. Elevating Security Operations in the Cloud

Standardization, automation, and the adoption of proactive cybersecurity practices offer substantial benefits to security operations (SecOps), but financial sector leaders have now realized the importance of factoring in the day-to-day impact of security tooling choices. This involves more than just checking if a vendor's tools work with a specific cloud platform. It means also assessing how well they can fit into the broader automation system, whether they have robust APIs, and if their licensing is flexible enough to make automated operations smooth. Cyber Threat Intelligence (CTI) feeds play a crucial role in continuously adapting this protection to the current threat landscape.

By 2024, organizations adopting a cybersecurity mesh architecture will **reduce** the financial **impact** of security incidents by an average of **90%**.

Gartner

7. Strategic Security: Beyond Short-Term Gains

Teams tend to focus on meeting the immediate security needs of a project and potentially overlooking the broader business objectives. While this approach may suffice in the short term, it can lead to security choices that necessitate a future re-architecture or even a complete redesign. Driving the adoption of cybersecurity solutions offering a seamless transition path to Zero Trust, built-in integration with Secure Access Service Edge (SASE), and the mature integration of Artificial Intelligence (AI) and machine learning (ML) can deftly guide and support you through future cybersecurity needs.

Zero Trust and **Cloud** are the top priorities for the financial services industry.

Cloud Security Alliance Report

Organizations are desperate for **highly effective** procurement.

Deloitte

8. Streamlining Vendor Management Across Your Digital Estate

Your cybersecurity estate now spans physical, cloud, and SaaS platforms. Managing different security vendors across these different platforms can be complex and detrimental to both security posture and contract negotiations. Modern, flexible, points-based programs that consolidate spending without jeopardizing flexibility are now bringing agility to procurement that simplifies spending and maximizes efficiency. Along with the ability to utilize cloud commits for cybersecurity procurement, they are offering a unique way to optimize both cloud and cybersecurity budgets to drive innovation and cyber resilience.

9. Beyond Compliance: Advancing Incident Readiness

Incident readiness is crucial, as underlined by its prominent role in industry regulations such as DORA. This requires specialized skills, collaboration, and the engagement of numerous teams both within and outside the business. Involving PR, marketing, and the board ensures a comprehensive approach. Cybersecurity partners with a proven track record in handling critical incidents can offer valuable insights to help craft effective playbooks. They can also facilitate exercises to rigorously test these playbooks and enhance your teams' preparedness in lifelike simulation scenarios.

10. Uplifting Resilience: The Power of Strategic Cybersecurity Partnerships

Strategic partnerships with cybersecurity leaders offer access to deep industry expertise, experience, and innovation. These partnerships enhance cyber resilience and expedite the advancement of staff awareness and skills. By collaborating with trusted cybersecurity partners, financial institutions can strengthen their security posture and engage in the global fight against cybercrime.

78% of organizations felt **prepared** for ransomware attacks, yet **half** still fell **victim**.

Fortinet 2023 Global Ransomware Report

One stellar illustration of the power of transformative partnership involves a leading **global financial institution** embarking on a cloud and automation journey to replace its legacy firewall infrastructure. The institution's stringent criteria encompassed deep firewall integration with its chosen automation platform, scalability for its extensive network, performance enhancement, and efficient management tools. Fortinet's impressive offering, marked by robust REST APIs, **scalability, and superior performance, left an indelible impression during the rigorous proof of concept (POC)** phase. The results of this **strategic alliance** were nothing short of remarkable, with projected **cost savings and productivity enhancements surpassing $100 million** over a span of five years. Fortinet's solutions **streamlined operations, curtailed downtime, and elevated the overall security posture**. Furthermore, Fortinet Professional Services teams accelerated the time to deploy, validate, and automate tasks, ensuring a fast implementation, sustained success, and continuous improvement.

Read the full case study.

Embracing Cloud Security for Finance Success

The cloud is central to the digital transformation of the financial sector. Collaborating with cybersecurity leaders like Fortinet enables financial institutions to build a secure, efficient, and agile cloud foundation that accelerates digital success. The Fortinet Security Fabric streamlines security services, enhances automation, and maximizes cloud's security potential. Breaking free from siloed security and adopting a visionary, open platform approach delivers the cybersecurity that your organization, the regulators, and your customers are looking for to enable everyone to thrive in a cloud era powered by trust and resilience.

For more information on how Fortinet Cloud Security strategy, services, and solutions can accelerate your success in the financial services sector, contact our dedicated experts at fsi@fortinet.com

FORTINET

www.fortinet.com

October 24, 2023 2:17 PM

fortinet:Shared:CREATIVE SERVICES:EMEA Creative Server:03_DOCUMENTS:21_PointOfView-POV:2023:FSI-Cloud:2023-Q4-PoV-Cloud-FSI-02

2279526-1-0-EN