FORTINET

POINT OF VIEW | 2025 Edition

The Future of Cloud for Finance

10 Cutting-Edge Cybersecurity Strategies

In today's financial services and banking ecosystem, success belongs to organizations that work to continually innovate, increase value, and keep up with industry-wide transformation. Cloud computing has become an essential part of this success strategy. And getting the greatest benefits out of cloud requires a strategic approach to cybersecurity.

Key Highlights

- Adopting the cloud opens opportunities for financial organizations to meet regulatory requirements, build resilience, and better manage risk
- The cloud enables the financial sector to deliver the trust, reliability, and modern services that customers expect
- Successful cloud transformation requires a commitment to cybersecurity best practices. It also provides access to capabilities to make security more effective, automated, and cost efficient
- A cybersecurity mindset depends on leadership from the top, but everyone in the organization must embrace a security-first mindset
- AI can enable greater efficiency and innovation, but users must consider new risks and regulatory compliance

Revolutionizing Risk and Compliance: Cloud-Powered Resilience

Financial sector industry leaders recognize that cloud adoption can help to optimize risk management, fortify resilience, and make it easier to manage compliance obligations. It also helps to maintain trust with customers and regulatory bodies, and achieve business transformation goals. The key for cloud adoption success is to remember that it's not just about embracing new technology, but about enabling a fundamental shift in the sector's operating model.

How Cloud Adoption Brings Financial Benefits

The cloud is critical for financial organizations that want to free up technology capacity to deliver the modern, value-adding services that customers expect. Leading cloud service providers recognize this. And they're making investments across Europe and the Middle East to pave the way for the economic benefits that such transformation can bring.

> The key for cloud adoption success is to remember that it's not just about embracing new technology, but about enabling a fundamental shift in the sector's operating model.

Fusing Innovation and Resilience to Drive Finance Success

The financial sector needs to approach cloud transformation with a sharp focus on risk and security. That's because the global economy depends on the industry's ability to safeguard its digital services and data. Banks and financial organizations must consider a number of innovative cybersecurity strategies to optimize cloud transformation while mitigating risk.

10 Strategies

1. Establish the Right Governance and Culture

This requires guidance by top leadership, with due diligence and possible restructuring of roles and responsibilities. Enabling a culture of strong security risk management means aligning cloud transformation with technology strategy, risk tolerance, and overall business goals. It also requires promoting a security-first mindset so everyone in the organization understands the need for cybersecurity best practices. Organizations can enable the right culture through regular training and cybersecurity exercises, embracing DevSecOps, and dismantling the silos of development, operations, and cybersecurity.

Enabling a culture of strong security risk management means aligning cloud transformation **with technology strategy**, risk tolerance, and overall business goals.

2. Focus on Enhancing Resilience

Moving to the cloud creates opportunities to enhance resilience. Done right, the cloud can reduce security and compliance burdens, improve threat detection and response, and integrate security as code into automated workflows for greater innovation and cyber resilience. Banks that do this pave the way for compliance with recent EU regulations such as the Digital Operational Resilience Act (DORA), the Capital Requirements Directive, and the NIS 2 Directive, as well as the UK's forthcoming Cyber Security and Resilience Bill, set to be introduced to Parliament in 2025.

3. Integrate AI to Support Tech Advances

AI opens new opportunities to enhance operational efficiency, drive innovation, and move cloud convergence forward. But it also creates new risks and requires thinking about regulatory compliance and addressing the potential for new kinds of cyber threats. Banks and financial institutions need to be aware of, and address, the different levels of risk defined by the EU AI Act, which came into force in August 2024.

4. Enable Project-Led Cloud Freedom

Teams need the autonomy to choose the right cloud platform for each project. They also need to be confident that their security and regulatory needs will be met. Use a Cloud Center of Excellence (CCoE) to support these objectives. This provides businesses with insights and guidance from experts across multiple disciplines, enabling them to develop a comprehensive and coherent approach to cloud adoption that meets the organization's needs. It also supports best practices, accelerated adoption, regulatory compliance, strong cybersecurity, and efficient cost management.

Done right, the cloud can reduce security and compliance burdens, improve threat detection and response, and integrate security as code into automated workflows for greater innovation and cyber resilience.

5. Unify to Reduce Complexity

Cloud adoption creates an opportunity to reevaluate cybersecurity tools and practices, helping to reduce complexity and friction. An optimized cloud environment lets you standardize tooling across your digital estate. The cloud provides access to a wide range of automated cybersecurity capabilities, including traffic monitoring, vulnerability scanning, threat-hunting tools, patch management, and AI-powered analytics. These capabilities free up security teams to focus on the highest priority tasks and can reduce problems such as alert fatigue.

6. Elevate Security Operations

Assess vendors' security tools to ensure they are comprehensive and fit into your broader systems. Do they have robust APIs? How flexible is their licensing? Do they support cyber threat intelligence (CTI) feeds so you can continually adapt protection to the changing threat landscape? Security needs to be considered at every level, from how it impacts users of mobile apps or browsers, to how it interacts with third parties such as merchants, payment gateways, and regulators. Organization leaders must maintain cybersecurity oversight across every level. This means thinking about robust defenses for identity and access management, APIs, and payment gateway integrations.

Focus **on future-proofing cybersecurity** solutions so that they can support a seamless transition to Zero Trust, built-in integration with Secure Access Service Edge (SASE), and future integration of AI and machine learning.

7. Think Strategically and Long Term

When you extend your security thinking beyond short-term goals, you can reduce the need for re-architecting or redesigning down the road. Focus on future-proofing cybersecurity solutions so that they can support a seamless transition to Zero Trust, built-in integration with Secure Access Service Edge (SASE), and future integration of AI and machine learning.

8. Streamline Vendor Management

Modern programs help to consolidate costs across physical, cloud, and SaaS platforms, simplifying spending and maximizing efficiency without jeopardizing flexibility. Using cloud commits - a commitment to spend a minimum amount for cloud services over a specific period - for cybersecurity procurement helps to optimize budgets and drive innovation and cyber resilience. Cloud service provider marketplaces are becoming a significant procurement channel, and enterprise sales through marketplaces could reach $85 billion by 2028. This strategy can streamline procurement and billing, delivering faster time to revenue and shorter sales cycles.

9. Advance Your Incident Readiness

Think about application security posture management and choose cybersecurity partners with a proven record in handling critical incidents. This can help you craft and test effective playbooks to enhance your teams' preparedness using realistic simulation scenarios.

10. Nurture Strategic Cybersecurity Partnerships

Partnering with cybersecurity leaders lets you access deep industry expertise, experience, and innovation. This helps your organization to build staff awareness and skills, strengthen your security posture, and prepare to fight cybercrime. Because no one business can combat today's cyberthreats alone, partnering with other organizations - public and private, and across industries and borders - is essential.

One Middle East investment group lowered its costs by 60 percent and increased security with Fortinet Secure SD-WAN. As a business spanning over 180 sites across multiple countries and business sectors, it needed fast, reliable, secure connectivity between every part of the organization.

By adopting the FortiGate Next-Generation Firewall, the organization can simultaneously activate multiple layers of defense and perform advanced SD-WAN management without degrading throughput.

Through a high-availability configuration at its three data centers, the group significantly improved business continuity and resilience.

It can also classify sensitive data, such as personally identifiable information for customers, according to the potential risk of loss or unintended exposure, which has reduced administration and compliance burdens.

Read the full case study.

Embracing Cloud Security for Finance Success

To remain competitive, banks and financial services organizations must digitally transform and embrace the cloud. By collaborating with cybersecurity leaders like Fortinet, financial institutions can 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. This helps you to break free from siloed security and adopt a visionary, open-platform approach to cybersecurity. It's the way to deliver the trust and resilience that your organization, regulators, and your customers expect.

www.fortinet.com

March 10, 2025 4:52 PM

/Users/eme/Documents/Boulots/FORTINET/Requetes/- Documents/PoV-FSI-Cloud-2025/2025-Q1-PoV-Cloud-FSI

EMKTG-557-1-1-EN