POINT OF VIEW

Financial Services Security Spotlight

Accelerate Time to Value with an Integrated Cloud Security Strategy

The Pace of Change

For financial services organizations, the world has fundamentally changed. Digitalization and innovation, increasing regulations, demographic shifts, a complex global economic environment, increasing cost pressures, and – most importantly – rising customer expectations, are all compelling reasons to transform.

The ability to successfully transform via disruptive innovation, new business models, the delivery of tailored services, and improved customer experiences will separate progressive financial champions and leaders from the fold. Those who act swiftly will seize the opportunity to create a competitive advantage – enhance brand loyalty, attract new customers, and guarantee success.

To thrive in the future financial marketplace, priorities must include addressing technical debt and removing the limitations of legacy systems, breaking down siloed business units to unlock valuable data, evolving information technology (IT) operating models, embracing robotics and artificial intelligence (AI), and rethinking the architecture to deliver a connect to "anything, anywhere" approach.

However, legacy systems and infrastructure have been unable to support and keep up with current technological trends. The old paradigm of applications in data centers, with users connected onsite doesn't work in a world of clouds and mobile devices. Systems must be capable of supporting the latest digital products, services, and applications that customers demand. This means that by shifting towards such systems, financial institutions can optimize the user experience and operate more flexibly and dynamically.

As a result, financial services organizations and their IT teams are facing the ever-increasing challenge of meeting the demands of the business at an accelerating pace whilst complying with evolving legislative guidelines.

Key Factors Accelerating Change

New Disrupters

With open banking levelling the playing field, financial institutions must rethink their business models to reinvent themselves and compete in changing markets driven by open practices and a sharing economy. New and agile digital-native entrants are winning the innovation race as they do not inherit the technical debt and legacy infrastructure that so many incumbents need to consider. As a result, they can bring services and products to market faster and offer premium and tailored customer experiences grabbing more market and wallet share from incumbents. By offering services based on smartphones or tablets and running efficiently in cloud-based environments, they can deliver instant, tailored results to the customer.

Regulation

Financial services organizations need to conduct business in a highly regulated market and with the opening up of financial services markets, governments have introduced legislation in an attempt to protect all stakeholders. Rules on all aspects of the operation have come into force to ensure that the customer and business are protected from criminal activities. Where is the data and who has access to that data? This is what regulators are concerned about, and it's more important now than ever before with online and application-based banking. In addition, regulators have raised the alarm on concentration risks within the financial sector. Given that only a handful of cloud providers dominate the market, business continuity and operational resilience may be compromised with the greatest risk being systemic failure across the financial system.

Security complexity

As markets open and partnerships develop within and across the industry, cyber threats to the business and consumer have grown in complexity and number. With so much of daily life facilitated by smart devices, both access to the system as well as the data that is resident within the business must be protected. As financial institutions move to more flexible cloud-based services and environments, the need for a pervasive approach to security is required, with the ability to show real-time compliance now a mandatory feature. This all adds cost and complexity to the business.

Challenges to Conquer in a Multi-Cloud World

Financial services organizations are developing and deploying services and applications in multiple clouds to gain the flexibility and agility required to play in the new marketplace and meet the demands of the business and its customers. But how safe is the cloud, in particular when multiple providers are involved? What are some of the challenges IT teams are encountering when working in hybrid and multi-cloud environments?

Cloud providers go to great lengths to protect their infrastructure, but protection of the business data and applications hosted or deployed in the cloud is the responsibility of the financial institution.

While there are small differences in how the shared responsibility model is represented between different cloud providers, the biggest difference lies in how native cloud security capabilities are implemented and managed. Each cloud provider offers different security services using different tooling and approaches. In this context, each public, private cloud, and on-premises data center becomes an independent silo in a fragmented network security infrastructure - not an ideal proposal.

When working across multiple clouds, the ability to standardize, manage and automate security is the challenge that IT teams in financial services organizations are seeking to overcome. The major issues facing them include:

- With each cloud hosting a new set of services and management tools, supporting them becomes complex and costly for the existing IT infrastructure and administration teams.
- The greater flexibility clouds provide to instantiate new cloud workloads can make it difficult for IT teams to have full visibility of all workloads, let alone manage and secure them.
- Most financial institutions have a hybrid environment, but all regulatory mandates and basic security tasks still broadly apply, no matter where the workloads are running.
- Important as it is to demonstrate compliance, in a hybrid environment it is inefficient to use different solutions to manage or secure workloads, and to integrate data across various environments.

A new security paradigm is required to address these challenges.

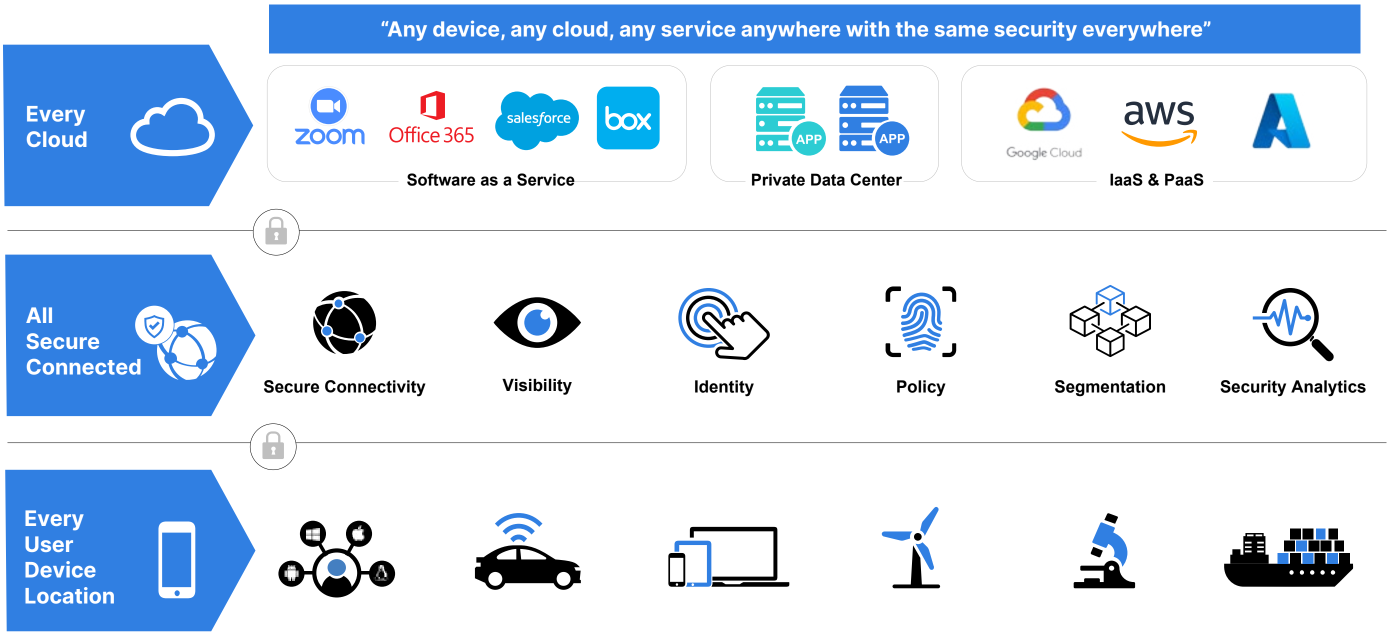
A New Security Paradigm for Cloud Security Success

To leverage the advantages of cloud and simplify operations, financial services organizations must adopt a unified security architecture that runs across multiple cloud platforms and embodies the following key capabilities:

- Native integration with all major cloud providers
- A platform approach encompassing a broad suite of integrated security tools to address the entire attack surface
- The ability to centrally manage the security infrastructure
- Simplify and tailor policies
- Standardize and automate security operations
- Visibility of the infrastructure, devices, and applications

To that end, a unified cloud security approach that leverages the strengths of each cloud will become the new standard, ensuring every system runs optimally across a sprawling estate of service offerings.

Fortinet's Mission – Creating a Digital World You Can Trust



"Any device, any cloud, any service anywhere with the same security everywhere"

Every Cloud

Software as a Service

Private Data Center

IaaS & PaaS

All Secure Connected

Secure Connectivity

Visibility

Identity

Policy

Segmentation

Security Analytics

Every User Device Location

Fortinet has developed an innovative approach to security, the Fortinet Security Fabric, which is an intelligent and integrated security platform designed to underpin financial organizations' business initiatives and engineered to protect their entire technology estate – including Cloud.

The Security Fabric extends a financial institution's security framework to all cloud services, thus providing the necessary visibility, policy enforcement, and automation across multiple clouds, and enables secure applications and connectivity from an on-premises data center and a distributed workforce to the cloud.

This unified security framework provides consistency, standardization, and comprehensive protection, enabling financial services organizations to benefit from the unique capabilities of each cloud while levelling up protection across the estate, improving risk posture and operational efficiency.

Fortinet integrates cloud-native services and real-time threat intelligence into its cloud solutions to simplify the delivery of advanced threat protection for a diverse range of cloud environments – from next-generation firewalls, intrusion prevention systems (IPS), and web application and API protection, to high-performance resilient connectivity with end-to-end encryption and inspection built-in. This enables IT teams to protect cloud workloads, resources, applications, and data in even the most dynamic cloud environments.

Fortinet also offers the largest ecosystem of partner integrations via APIs for maximum visibility, integration and a stronger end-to-end security solution. This ensures that IT teams maximize their current investments and maintain the flexibility to choose the right solution for any particular project, without jeopardizing the integration that is critical to automation.

With Fortinet security underpinning their cloud strategy, financial services organizations can innovate, accelerate time to value, and realize their future vision, knowing that they are creating a digital future they can always trust.

Learn more

For more information on Fortinet's cloud security strategy and solutions for the financial services sector,
contact us at fsi@fortinet.com