STRATEGY BRIEF

5 Service Provider Essentials for Cybersecurity in a World of Clouds

Service Providers around the world are on a continuous journey to deliver innovative services and offerings, increase value to customers and stakeholders, and transform both themselves and entire industries to excel in new digital ecosystems. This demands transformation, innovation, and collaboration that delivers sustainable growth in a socially responsible way. And cloud is a key ally.

Cloud as a Digital Service Enabler

Cloud is powering digital transformation to modernize Service Provider IT, operational, and business support systems (OSS/BSS), deliver compelling 5G services and use-cases, transform customer experience, and optimize end-to-end operations. Guaranteed outcomes, with no risk, are core to this strategy.

Cloud-savvy Service Providers are being smart about leveraging the full range of cloud platforms - virtualized, public cloud, Software-as-a-Service (SaaS), and containerized environments – to power their digital success. This means adopting the right cloud environment, at the right time, for the right reasons. And the resilience of these cloud environments is critical.

Cybersecurity as a Cloud Accelerator

Risk management, cyber resilience, and compliance are critical to Service Provider long term success. Cybersecurity safeguards customer trust, it drives increasing value for stakeholders, and empowers the ability to meet evolving and demanding market regulations.

Digital evolution with cloud is not just about maintaining security, resilience, and compliance though, it is an opportunity to deliver them more effectively and in a more efficient way that drives additional value for the business. Integrating and aligning cybersecurity strategy with the organization's digital strategy is key to this success.

Today's Cloud Security Challenges

Cybersecurity must now address not just legacy environments but cloud-based data lakes, web front ends, agile development environments, CDNs, edge deployments, OSS/BSS, IT services, and exposed APIs. These digital initiatives are often driven by specific domain owners who independently decide which security tools and controls to put in place, and who frequently have to introduce new tooling to mitigate unforeseen risks.

This fragmented, ad-hoc approach to cybersecurity regularly creates numerous challenges - security policy being shaped to each cloud environment, multiple vendors being used for the same security tooling, and highly variable security event and incident formats. The result is inconsistent user experience, friction in time to market, minimal re-use of security expertise across the organization, and ultimately security gaps and misconfigurations. Add to this security teams burnt out spending a significant amount of time collecting and triaging security insights and events — disproportionately higher than the time proactively spent mitigating the top risks and threats – and the business impact quickly becomes apparent.

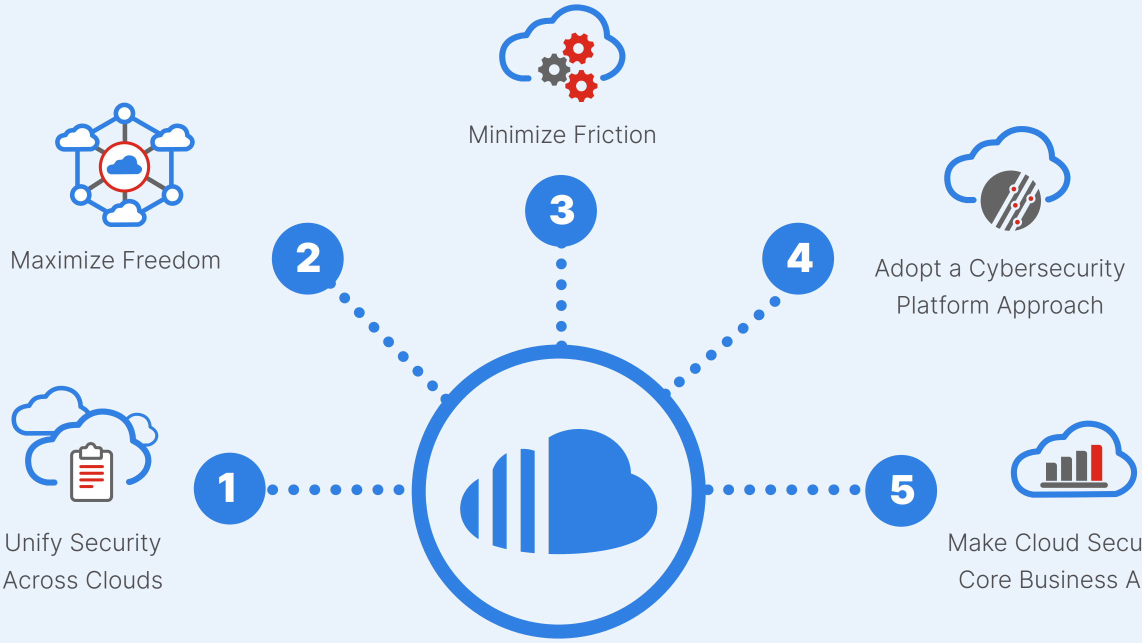
Security system complexity has the highest impact on the total cost of a data breach.*

* IBM Cost of a Data Breach Report 2022

A Strategic Approach to Cloud Security

Realizing the full benefits of cloud demands a strategic approach to cybersecurity that aligns with both Service Provider and customer digital strategies. This business-focused approach must embrace the diverse and distributed cloud environments that empower innovation, collaboration, and modernization. It must also deliver cyber resilience in a way that minimizes friction, optimizes costs, and contributes to business growth.

Let's take a look at the five essential elements that have proven key to accelerating Service Provider cloud success.


Minimize Friction
3
Maximize Freedom
2
4
Adopt a Cybersecurity Platform Approach
1
5
Unify Security Across Clouds
Make Cloud Security a Core Business Asset

1

Unify Security Across Clouds

Security policy is something that is defined by the organization - and often prescribed by the regulator - to ensure resilience. How it is implemented will always need to be adapted to the underlying cloud environment but it should never be revised according to the built-in security services each offers. Security should be consistently enforced regardless of the cloud - or physical - environment in which applications or data reside.

Standardized security offerings that abstract away the underlying cloud platform enable delivery of this same security policy everywhere, for every cloud environment. This unified cloud security foundation is not about centralized control though, it's about alignment across teams to empower distributed, independent implementation. A Cloud Center of Excellence (CCoE) being a best practice approach to doing this.

The result is much more than just consistent security policy. It ensures the same user experience – for internal users, developers, and operations, as well as external partners, contractors, and customers – and facilitates cross-team digital initiatives, collaboration, and innovation. It helps maximize cloud and cloud security expertise that is often difficult to come by and challenging to retain. Security policy is simpler to enforce, threats identified and mitigated sooner, misconfigurations and security gaps minimized. More efficient and effective management of business risk and compliance being the ultimate outcome.

2

Maximize Freedom

Consistent cloud security must not come at the price of restricted delivery models. Neither internal teams nor customers want to be locked into a single approach or single cloud platform that may not be the best fit for their particular needs. Depending on each digital initiative – and even the phase of any particular initiative - the right delivery model can vary significantly. This may sometimes favor security delivered as a SaaS offering for minimal overhead, cloud-based infrastructure or containerized functions to meet specific security requirements and scale to demand, it may even mandate virtualized or hardware-based on-premises delivery to meet specific compliance restrictions.

Maintaining consistency despite these variable delivery needs is key to optimizing costs while continuing to offer both internal teams and customers the freedom that they demand. Minimal variations in the features and functionality, as well as look and feel - despite the different delivery model chosen - ensure that costs are optimized, maximize existing integration investments, and build on internal expertise.

3

Minimize Friction

Cloud is all about speed and agility. Cybersecurity teams must not slow down or hinder the business, in fact, the objective is to accelerate digital initiatives. The only way to achieve this is by making security integral to today's automated, modern workflows. This demands that security teams embrace the same cloud principles, practices, tools – and culture – as development teams. Friction is the anti-pattern to avoid at all costs.

This is perhaps one of the most challenging aspects of cloud that security teams must navigate, and where strategic, cloud-savvy partners are key. They can help guarantee success – and accelerate time to value – by supporting teams on their cloud journey. This includes integrating and automating security throughout the entire lifecycle - from design to build, from purchasing and licensing to deployment, from protection to detection and mitigation, from risk assessment to compliance and incident response. The result is consistent but distributed, self-service consumption and delivery of security on-demand.

Key to this is creating an overall security framework, designing the right architecture for each cloud environment, writing the core building blocks – to best practices and jointly validated with each cloud platform provider – that can be used as the basis for standardized offerings. A CCoE plays a critical role here. The objective is overall automation that not just simplifies security integration but also shifts security from reactive to proactive, mitigating risks ahead of incidents, simplifying compliance, and reducing time-consuming manual processes. Robust APIs that enable the full automation of security by design and policy enforcement, as well as automated threat detection and mitigation, are critical, along with artificial intelligence and machine-learning that make security intelligent enough to discern simple errors from malicious actions.

Adopt a Cybersecurity Platform Approach

4

Security capabilities and services must be delivered at business speed, in the face of an ever-evolving threat landscape, and despite challenges in talent recruitment and retention. Reducing complexity, harmonizing approaches, and minimizing management overhead are thus critical. This is driving the adoption of a collaborative, platform approach - converging multiple security domains towards integrated tools that deliver a whole greater than the sum of the parts.

A converged cybersecurity platform approach reduces complexity, simplifies integration, and increases operational efficiency. Critical to this are integrated consoles, cross-domain security collaboration, reusable components, and threat intelligence engines that power, and are driven, by multiple security domains. This is key to driving increased business value.

A platform approach doesn't mean being obliged to go all in on everything in any single security platform though. There may be security domains outside those offered in the security platform, specific security needs where a different vendor solution is preferred, and cloud-native automation tools that are needed for orchestration. To maintain the value of an integrated and converged security approach, look for platforms that support an open ecosystem of deeply integrated technology partners, along with a demonstrated commitment to ongoing innovation and expansion to address new security challenges.

5

Make Cloud Security a Core Business Asset

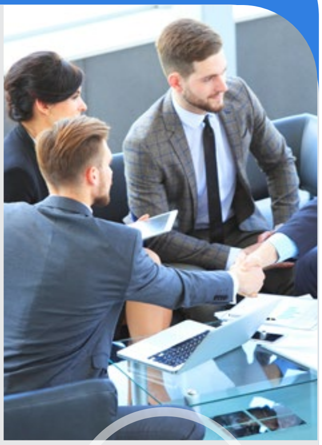
Cybersecurity is a board level topic, placing security at the heart of strategic business initiatives. And cloud security is no exception. But cybersecurity is not just about risk management. Cybersecurity is a valuable asset that the market, and the regulator, are keenly watching. Add to that customer demand for assistance with securing their journey to cloud, and the market opportunity for high value cloud security services drives additional stakeholder interest.

Seize this opportunity by embracing each of the four previous steps to create standardized cloud security offerings that are simple to deliver, with higher margins, and that offer the ability to easily up-sell and cross-sell services across the security platform. Look for security offerings that easily enable the addition of new value-added services without changing the underlying security solution. For instance, by offering a simple transition to advanced services such as Zero Trust Network Access (ZTNA) on the same platform that is currently delivering VPN access, adding zero-day threat protection through a cloud SaaS-based add-on, or a consulting service for cloud risk assessment.

And don't forget the opportunity that cloud service provider marketplaces offer to reach a potentially new and global customer base, along with access to committed cloud budgets.

Partner for Success

Cloud is integral to Service Provider digital strategy and cybersecurity is critical to success. A strategic approach to cloud security, aligned to digital strategy, is key. Partnering with a cybersecurity leader with a demonstrated commitment to open, innovative, and continuous evolution can help power Service Provider success. Fortinet's visionary, collaborative cybersecurity platform – the Fortinet Security Fabric – delivers an integrated security platform that extends award-winning cybersecurity across all cloud environments, and all phases of the systems lifecycle.



This cybersecurity platform enables the creation of standardized security services that don't restrict individual team freedom, it simplifies full security lifecycle automation, and accelerates time to value, delivering the reduced risk and optimized costs that drive business growth. It's time to move away from a siloed security approach and turn cybersecurity into the key business asset that the organization, the regulator, and customers are looking for.

Find out more about
Fortinet Cybersecurity Solutions for Telco Cloud

March 23, 2023 2:21 PM

MacintoshHD:Users:spare:Library:CloudStorage:Egnyte-fortinet:Shared:CREATIVESERVICES:EMEACreativeServer:03_DOCUMENTS:28_STRATEGY_BRIEF:5SP-Essentials-for-Cloud-Security:2023-SB-5-Essential-points-Cloud-Security

2052406-0-1-EN