Maven Wave™

SECURING PII DATA IN THE CLOUD FOR FINANCIAL SERVICES

ARE WE ASKING THE RIGHT QUESTIONS WHEN IT COMES TO CLOUD SECURITY?

CONTACT

Andrew Dunmore
Senior Principal,
Financial Services Lead

Phone: + 1 312-509-4890

Email : andrew.dunmore@mavenwave.com
Website: www.mavenwave.com

SECURING PII DATA IN THE CLOUD FOR FINANCIAL SERVICES

TABLE OF CONTENTS

Executive Summary

Data protection, particularly for sensitive data like PII (personally identifiable information), is an extremely important consideration for the enterprise. The financial, legal, and reputational costs for non-compliance can be very high. It is a common misconception that moving to a public cloud increases risk. In fact, the adoption of services such as Google Cloud Platform (GCP) can help to augment and strengthen system security, deliver lower costs, greater flexibility, expanded services, and other benefits.

This white paper explores potential data security threats, vulnerabilities, and events that can impact your business and the best practices to make the most effective use of public cloud resources. We then discuss key takeaways from a customer journey and real-world outcomes from moving 100% of customer facing systems for +80 million customers and their PII from the data center into Google's public cloud.

Securing PII Data in the Cloud

Financial services companies are asking the wrong question when it comes to cloud security

It's a known fact that data exposure, particularly of sensitive data like personally identifiable information (PII), is a serious issue for the enterprise. In fact, Juniper Research estimates that the average cost of a major data breach will exceed $150 million by 2020. This is an especially sensitive area for the financial services industry with Equifax as a well-known example for the dangers inherent in a data breach. In September 2017, the company revealed a massive breach involving personal data that ultimately affected 134 million customers and held consequences for the firm that are still being felt today. The cost of the incident has exceeded $400 million through Q3 2018 and the company's share price fell 34% between the time of the loss and the end of 2018. Meanwhile, the shares of its rivals, TransUnion and Experian, rose by 17% and 22% respectively over the same time period.

At the same time, the **increased use of cloud resources presents additional attack surfaces and egress that you need to secure.** The adoption of cloud resources is inevitable, due to the business value proposition and the superior capabilities cloud delivers in terms of cost, speed, power, and flexibility. What's not immediately clear is how to address the issue from the perspective of system security.

Fortunately, the security features and products that are prevalent in public cloud providers are intrinsically more comprehensive and robust than those available in an on-premise data center and, as such, offer a foundation for upgrading the security posture of the enterprise. In this context, the time has come to stop asking if the cloud is secure and instead start figuring out how to move to the cloud securely. To do so, an "inside out and software-defined" approach replaces the traditional perimeter-based security orientation, deploying new methods that are not available in on-prem solutions and applying new security standards across each abstraction layer, from context-aware identity management to data at rest.

SECURING PII DATA IN THE CLOUD FOR FINANCIAL SERVICES

For example, **Maven Wave recently partnered with a large fintech "unicorn" to migrate nearly all of their customer-facing systems to Google Cloud Platform (GCP).** The company's $4Bn valuation is anchored in their ability to not only provide a differentiated and personalized service, but also to protect sensitive information as a data controller and processor for digital tax and credit services. The types of PII they handle include social security number, date of birth, address, borrowing history, assets, income, charitable contribution activity, and even dependent data relating to children and spouses who may not be a consenting customer of the institution.

Given the nature of the personal information to protect, the company chose to set a higher than usual bar for security standards in financial services. In this case, the client benchmarked to the DISA STIGS standards that are employed by the U.S. Department of Defense to protect the company's risk exposure and valuation. We were able to successfully apply those security guidelines through the implementation phase using our best practices to run their business on GCP. Later in this paper we will walk through some of the insights that the participants observed along the way.

For our other customers, securing their data in the cloud begins with other compliance conversations. Our clients include banks, insurance companies, and asset managers who are also subjected to a high level of regulatory standards from the likes of FINRA, FDIC, NAIC, CFTC, GDPR and others. As in the fintech example, **it is critical that you select a cloud provider who has certifications that support your compliance needs.** For example, GCP has 22 certifications including ISOs, SOCs, WORM, Privacy Shield, and other industry and country-specific compliance standards. These certifications help ensure that GCP is a suitable place for your sensitive data.

GARTNER - "IS THE CLOUD SECURE?"

In their "Is the Cloud Secure?" report from March 2018, Gartner dispels several key misconceptions about security in the cloud and makes a persuasive argument that a shift from a "Is the cloud secure?" conversation to "Am I using the cloud securely?" will enable companies to make the most of cloud opportunities.

Among their predictions:

- In 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.
- Through 2020, public cloud infrastructure as a service (IaaS) workloads will suffer at least 60% fewer security incidents than those in traditional data centers.
- Through 2022, at least 95% of cloud security failures will be the customer's fault.

However, it isn't enough to select a compliant platform, you also need to ensure that you are also implementing your systems onto the platform in a secure and compliant way. In fact, Gartner analysts predict "Through 2022, at least 95% of cloud security failures will be the customer's fault" (see sidebar: Is the Cloud Secure?). **To truly secure your data, you need to develop a security posture that is tailored to your business.** In the next section, we will identify the potential risks to your infrastructure, your data, and your business, followed by an overview of 11 best practices to help you address them in a way that your data is safe on GCP.

Protecting PII in the Cloud

The risks to your systems and your data in the cloud are, in many ways the same cyber-threats that face any on-prem system. **These risks can be broken down into three buckets: threats that lead to system compromise, vulnerabilities that leave your systems exposed, and events that could impact your business arising from the vulnerabilities and threats.**

SECURING PII DATA IN THE CLOUD FOR FINANCIAL SERVICES

Threats that lead to system compromise can be either internal or external, such as the actions of malicious insiders or the abuse of cloud resources for activities like phishing. Vulnerabilities also have both internal and external aspects, with failure to patch components as an example of the former and insecure interfaces and APIs representing the latter. Finally, events that can impact your business include data breaches and data loss. For a complete rundown of the twelve threats, vulnerabilities, and events see sidebar at the end.

In order to prevent negative business impacts you must implement a compliant and secure cloud infrastructure; **these threats and vulnerabilities need to be addressed by both your cloud provider and your method of implementation.** From our experience, we will take you through a list of best practices that will help you mitigate security risks to your systems and your business.

11 Best Practices

Using GCP and DevSecOps best practices, it is possible to create a system that both delivers a higher level of security than existing systems and is more flexible and responsive to meet future needs. **By leveraging a cloud-first security approach and deploying security methods to reduce risk beyond what was possible in an on-prem data center, you can increase the effectiveness of the security posture at every step of the process.** To do so, we follow a methodology that embraces the following 11 best practices proven to produce the desired results.

SECURING PII DATA IN THE CLOUD FOR FINANCIAL SERVICES

1. BEGIN WITH SECURITY AND COMPLIANCE END GOALS IN MIND

To achieve positive outcomes, it's critical to establish a strong foundation from the get-go. This means that a clear-eyed examination and delineation of the end goals is an essential first step. Use the security capabilities of the cloud to empower your security and compliance teams up-front during the process of gathering and analyzing requirements. **The goal is to establish baseline security and compliance controls as well as modular methods of leveraging those controls to apply to applications and services.**

We have found success when we fully allocate security and compliance experts to the initial working team and keep them, and all relevant business owners, involved in every step along the way. By **ensuring the security team is in the room from the earliest planning stages, we are able to avoid bottlenecks and maintain compliance** when it is time to go-live in GCP.

Furthermore, our clients' security experts have agreed that the security offerings in GCP can both harden your security posture and simplify the operations and administration of your environment. **The modularity and ease of consumption of the cloud-native security products enhances consistency and reusability** - both of which serve to bolster security and also facilitate audits of the environment on an ongoing basis.

2. FOCUS ON "WHAT TO DEFEND" RATHER THAN THE ENTIRE "ATTACK SURFACE"

The traditional security orientation of a fortress mentality assumes no amount of protection is sufficient. Alternatively, an effort that focuses on pre-defining the data that truly impacts your business gives you the ability to then **leverage the power of the cloud to dynamically evaluate, classify, and treat the most sensitive data with the proper level of due diligence.**

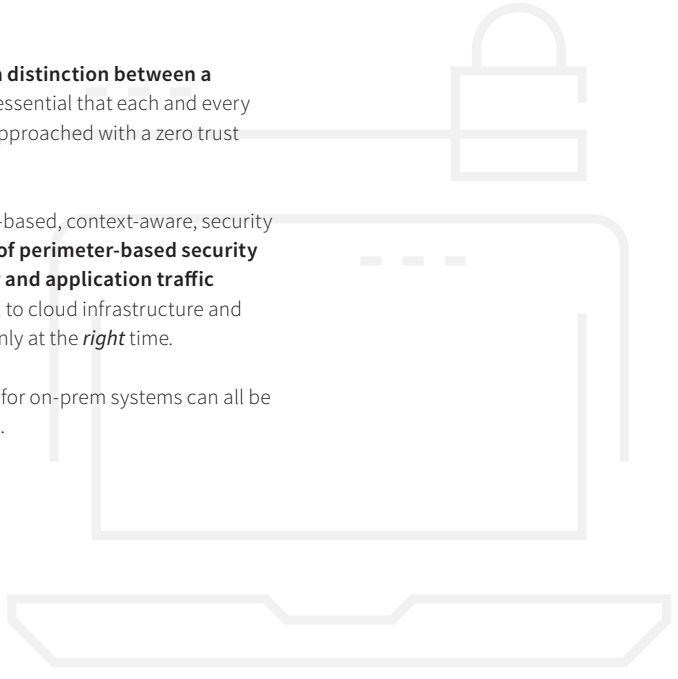
The cloud offers unprecedented control and automation around data security assessment and operations. For example, we have used Google Cloud Storage (cloud object storage) in order to leverage the Data Loss Prevention API to automate data classification and ensure that data sets contain only the types of data that should be present. In this way, any non-conforming data can be redacted, tokenized, or made inaccessible via automation. Cloud storage services also offer a purpose-crafted interface with access control mechanisms that can be used to limit data access based on need, with immutable audit logging of access or changes in access. Ultimately, our customers agree that this has enabled their data to be more effectively categorized, secured, and monitored.

3. DEVELOP A "ZERO TRUST / ALWAYS VERIFY" CLOUD

Moving to a posture of total defense invalidates the traditional model of making a distinction between a hard security perimeter protecting soft systems and data. In the cloud model, it is essential that each and every element of the technology environment - from software all the way down to data - be approached with a zero trust mentality.

We have achieved success on projects where we have transitioned towards an identity-based, context-aware, security model for everything from the network to the data store. **A traditional on-prem view of perimeter-based security models does not adequately provide the visibility, control, and protection of user and application traffic that is necessary in the cloud.** On the other hand, adding a zero trust design principal to cloud infrastructure and applications ensures that only the ***right*** actors have access to only the ***right*** data and only at the ***right*** time.

Context aware access, VPC service controls, private API-access, and private API-access for on-prem systems can all be used together to both secure and extend the API perimeter of a Google Cloud presence.



4. CONSIDER SECURITY FOR YOUR HYBRID CLOUD ENVIRONMENT FIRST

In our experience, it is rare that all of a company's data center workloads are ready to fully migrate to the cloud. Hybridization of workloads drives additional complexity in both the cloud as well as your data centers. These additional complexities need to be taken into consideration throughout the planning and architecture of your cloud. **All of the practices discussed in this paper are applicable to a hybrid cloud environment, and we typically pay special attention to the additional compliance and security burdens that hybrid workloads can create.** By considering these matters up front, you ensure not only that your cloud workloads are secure, but also that you do not introduce any additional security gaps for hybrid connectivity scenarios in the process.

Abstraction is the fundamental power of the cloud, and it is what enables complex applications to be delivered as easy-to-consume services. You can use Google's Cloud Endpoints for services deployed on GCP, and also for on-premise API management layers (e.g. Apigee) to apply the same powerful abstraction to your applications. By exposing these as APIs, you can utilize the same authentication and authorization practices for these services as Google does for their own.

Additional cloud-native practices can and should be adopted to simplify the provisioning, operations, and governance of your hybrid workloads:

- Classify and categorize your data and understand how it will be consumed by your hybrid workloads. Use automated scanning tools to validate that your data sets only contain the information they are supposed to contain.
- Ensure encryption is everywhere - both at rest and in transit.
- Apply zero trust principles to your data center.

In the final analysis, there is more often than not an unavoidable and complex relationship at the intersection of data center and cloud assets, the full treatment of which is beyond the scope of this study. It's a topic that we will return to in more depth in a subsequent white paper.

5. UTILIZE THE EFFECTIVENESS OF A GLOBAL CLOUD NETWORK

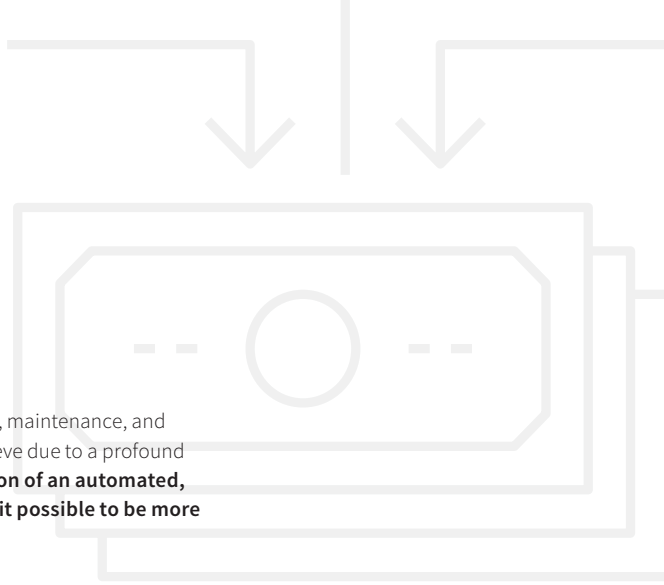
The fundamental nature of a global cloud network provides incredible benefits right out of the box. For traditional VM-based workloads, the compute engine firewall service takes some complexity out of firewall management through the use of tagged and service account-based firewall rules to simplify management over traditional source/destination IP/port-based rules. For containerized workloads, Kubernetes Engine's network-policy features make it possible to disallow any unnecessary east-west traffic. This not only reduces the surface in need of protection but also contains the threat in the event of a breach.

In our experience, other benefits naturally accrue from a global cloud network as well:

- Tools such as "Shared VPC" allow centralization of administrative duties and control for security and network policies that apply across cloud assets.
- Native firewall service also allows for network based micro-segmentation. Because firewall rules are applied at each and every instance, there is no communication allowed even between two VMs on the same subnet without an explicit firewall rule to allow the traffic. Micro-segmentation can also be applied to microservice workloads as well.

Once attached to a shared VPC, service projects inherit relevant controls that are common across cloud assets. It is then possible for changes to be made to the security posture in a single location and applied across desired assets in the cloud. As a result, customers have agreed that shared VPC minimizes opportunities for inconsistency and simplifies their enforceability.

SECURING PII DATA IN THE CLOUD FOR FINANCIAL SERVICES



6. EMBRACE INFRASTRUCTURE AUTOMATION

A key benefit of moving to the cloud is that it creates the ability to fully automate provisioning, maintenance, and security. In the traditional, on-prem model, such an outcome is difficult or impossible to achieve due to a profound lack of uniformity and Infrastructure as a Service (IaaS) tooling in the data center. **The adoption of an automated, cloud-based model not only enables a higher level of overall security, but it also makes it possible to be more efficient and effective in maintaining and updating the entire system.**

We have been able to codify and automate entire cloud infrastructures while exiting the data center, thereby improving DevSecOps practices. In many instances, we have had success with Terraform by HashiCorp as an infrastructure coding framework. Using automated provisioning, it is possible to perform automated security analysis, rapid build up and tear down, and dynamic monitoring and recovery. Coupled with improved code-review processes, these solutions have made it possible to vet a security posture early in the development lifecycle, to continuously monitor it after any deployment, and respond in a fully-recoverable production state. Building an "automate everything" mindset has helped our customers ensure consistency and effectiveness in both preventative security and response across cloud infrastructure assets.

7. TREAT SYSTEMS AS "CATTLE, NOT PETS"

Immense benefits can be gained by adopting an approach that shifts systems from being bespoke (pets) to interchangeable commodities (cattle). The former are brittle, vulnerable, and fragile because of their uniqueness while an undifferentiated approach yields interchangeable parts and components that can quickly be swapped and replaced in the event of unforeseen events. Specifically, cloud instances, such as compute and containers, can be standardized to meet security requirements and be hot-swappable so that vulnerable systems are easily replaced and patched with zero down time.

To simplify creation of immutable systems, we have employed containerization of services wherever possible. We have additionally been able to ensure that systems remain up-to-date with the latest security patches by leveraging managed services to define infrastructure workloads, such as Google Compute Engine images for compute and Google Kubernetes Engine (GKE) for container orchestration. **Combined with automated pipelines, changes to immutable infrastructure are traceable for quick recovery and can be deployed and updated without interrupting your critical services.**

8. UTILIZE CLOUD-ENHANCED DATA MANAGEMENT

With a comprehensive cloud security practice, it is no longer necessary to cobble together on-prem solutions to have a fully integrated lifecycle for encrypting and managing your data. **GCP provides the management tools needed to ensure that data is kept safe and highly available.**

The use of managed data stores facilitates automated backups and restores and includes options for performant, multi-regional disks for high availability or more cost-effective nearline or coldline storage for long-term retention. We have used GCP-managed data stores for SQL, NoSQL, and file storage, which is backed by standard GCP encryption at rest. Additionally, if compliance requires additional data encryption, we have used Google's Key Management Services. For additional data availability, we have used automated GCP Disk Snapshots to Google Cloud Storage Buckets. **This enables cost-effective recovery and resilience in response to a security event.**

9. LEVERAGE IDENTITY MANAGEMENT AS A SERVICE

In the cloud, more critical services need to authenticate autonomously using service accounts rather than via human intervention. This necessitates using a dynamic, cloud-integrated secrets management solution. In doing so, **it is possible to integrate a secrets management solution with automated deployment pipelines as part of infrastructure automation** as described above. This ensures frictionless releases with a highly-enforced, traceable, and mature identity management process.

Wherever possible we have used cloud-integrated secrets management solutions to govern all access policies in one place to ensure that services access the appropriate systems for the minimum duration required. We've had success building highly-available, enterprise secrets management solutions with Hashicorp's Vault by deploying it into a GKE environment.

10. UTILIZE PROACTIVE AND REACTIVE SECURITY ENFORCEMENT

While proactive enforcement through static Infrastructure as Code (IaC) scanning is advantageous, it is not enough to protect your organization because it doesn't guard against malicious insiders that may be able to circumvent established pipelines. For this reason, and to more generally **ensure adherence to your overall cloud security posture, robust, reactive security enforcement is also required.**

Fortunately, security enforcement is also exposed through services. We typically implement policy as code (PaC) which can be enforced through pipelines before and after infrastructure has been provisioned. Enforcing security PaC during the transition to GCP has allowed our clients' security policy and operations to mature and evolve with their growing products and customer bases.

11. PRACTICE RISK EXPOSURE, ISOLATION, AND REMEDIATION

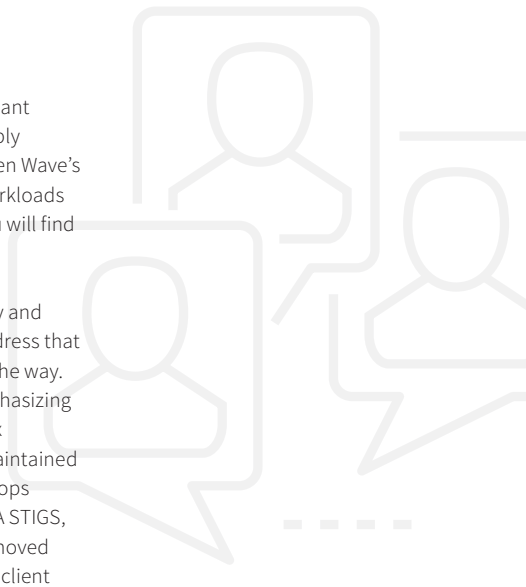
Effective monitoring is important in the cloud due to the enormous amount of information being generated. **Aggregation, filtering and sorting of monitored data into an intuitive and self-descriptive representation in the form of a dashboard is essential.** This helps drive effective automated remediation of threats and quick response to exposed risks.

We have used GCP's embedded Stackdriver service to deliver monitoring and alerting for resource spikes and anomalies so we can immediately help identify compromised systems and networks. With Stackdriver, our clients can now create internal security audit trails and alerts to know who is accessing each system and be alerted immediately of violations. Given the quantity of the monitoring data generated, we have designed dashboards and views tailored to response teams that isolate manageable, actionable information sets. We are also planning to implement GCP Cloud Security Command Center, a new product that streamlines the creation of those assets. Finally, in addition to auditing internal changes, the Access Transparency service allows for audit tracing in GCP itself to correctly isolate and respond to upgrades and changes.

Customer Security Journey and Results

Earlier in the paper, we mentioned that Maven Wave partnered with a $4Bn fintech firm to move all of their PII data to GCP. With over 80 million customers, this was no small task and was also one that carried both significant requirements and risks. The financial risks and rewards in a case like this are extremely high, a fact that is amply demonstrated by the case of the Equifax breach that opened our discussion at the top of the paper. With Maven Wave's assistance and our 11 best practices in mind, the client was able to migrate 100% of their customer-facing workloads to GCP, and the remaining on-prem assets will be completely transitioned over a three year period. Below you will find our top 5 insights learned along the way.

1. **Integrate your security and development teams from the start.** Often, a wall exists between security and development resulting in bottlenecks due to an insufficiently compliant implementation. In order to address that challenge, the security team was included from the earliest design discussions and at every step along the way. Inversely, people with an automation-first mindset were also embedded into their security groups. Emphasizing "workable security" over "work around" security was key to ensuring that even in the midst of a complex migration, security solutions remained streamlined and relevant, a rigid security posture was always maintained and compliance bottlenecks were avoided. Conducting pair programming and cross-functional workshops with your automation experts and your security teams also created trust and shared buy-in. In fact, DISA STIGS, ISO 27001 and ISO 27018 became common terms on the cloud team. At go-live, the development team moved quickly given that they had already adopted security requirements into their core product. In effect, our client



now has development culture and capabilities embedded their security team which established better working relationships across their operating model.

2. **Carefully consider the tradeoffs between migration paths.** The business drivers for this project demanded a very aggressive migration deadline, which led to a bias towards "Lift and Shift" (L&S) over "Move and Improve" (M&I). While L&S is purely mechanical and may miss differences between legacy and cloud capabilities, M&I distinguishes between the two and makes it possible to vastly improve results by taking advantage of superior attributes that can be attained in a cloud environment. Deprioritizing improvement in an initial L&S migration made sense for this particular client, but at the cost of operational efficiency. Fortunately, a second phase is already in progress to address optimization gaps, which will result in additional cost savings, reduction in unnecessary complexity, and simplification of their security enforcement. This demonstrates the importance of striking a balance between the impetus to move fast and taking time to identify "quick wins" along the way in order to provide the best near-term and long-term ROI for operational cost, simplicity, and enhanced security.

3. **Be mindful and rigorous in making "build versus buy" decisions.** With a plethora of useful management services available in GCP, our client still wanted to explore the design of a custom identity management solution to service one of their applications. Following the initial investment in this solution, the custom initiative was abandoned for its complexity and inadequate security. This experience served as a useful reminder that when it comes to "buy vs build" for something as critical as security, one must exhaust exploration of established solutions before committing to a custom build out. Fortunately, owing to an emphasis on agility, we were able to quickly course correct and implement our recommended third-party solution to solve the problem.

4. **Diagnose and call out old practices that may have a negative impact on the implementation of new solutions.** In any transformation, the dichotomy between old and new approaches can create a tension. Our client occasionally struggled with the push toward solutions aligned with the stated vision for the cloud and the pull from implementers within the legacy culture who were accustomed to a traditional view emphasizing ownership and attribution. In one case, this resulted in deprioritizing a superior cloud optimization solution because teams could not decide who would own the new product. With our help, however, the client ultimately established a feedback cadence between the thought leaders behind the vision and the delivery teams to capture items such as these and prioritize them for eventual implementation.

5. **Embrace agility and drive towards powerful transformation.** Optimal security is a journey, not a destination. The process of building a secure cloud environment never ends. With our client, we emphasized a culture of continuous improvement that promotes constant feedback and rapid response to evolving business demands and technology advances. Armed with a proven agile approach to security and development, we are confident our client will be able to grow and evolve to meet whatever challenges they encounter.

Customer Cloud Advancements and Outcome

Maven Wave was able to successfully help its client exit the data center and move their business to the Google Cloud Platform. As an end result, the company is not only positioned for growth, but it now has a strengthened overall security posture. Below we outline the benefits and results that were achieved.

- **The security posture on the perimeter improved dramatically.** In fact, a third-party, highly-sophisticated penetration testing team was engaged to assess the new cloud deployment. The penetration testing team walked away from the exercise estimating from their efforts that the backend services were completely invisible. In the future, due to the adoption of advanced PaC and preventative enforcement methods, the company can expect a 60% reduction in incident count.

  With advanced monitoring and enforcement methods, the company estimates that they have the ability to identify and isolate issues twice as fast in their new GCP environment than they did in the data center. Further, due to the advancements in automation, container management and monitoring, the company has the ability to tear-down and rebuild workloads with zero downtime. They estimate their response and recovery times will improve by a factor of 10.

- **We estimate they will realize at least a 30% savings on infrastructure.** The company was able to exit the data center for their production workloads and they are in the process of optimizing their compute and storage only for what they will use.

  The company helped its technology teams gain efficiencies from leveraging security services and automation early and ubiquitously across their infrastructure as well as from advanced enforcement and response methods. We project that they will be able to repurpose 50% of their work activities toward improving security over manual operations.

- **Being able to "move at the speed of the cloud" has improved time-to-market, data insights, and scale.** As a result of a security-first and repeatable DevSecOps process, the company estimates that they are able to securely ship code five times faster. Further, by protecting their reputation and improving the agility of aligning product to market, the company estimates that recent growth to $4Bn and + 80 million users is supported by the new streamlined infrastructure and practices on GCP.

Data Security is a Growing Issue

It's a common misconception that the public cloud is not an acceptable environment for sensitive data such as PII, but it should now be evident that this belief is simply not true. In fact, by fully embracing the superior technology and practices that are available in a public cloud like GCP, an enterprise can not only lower cost and increase efficiency, they can also dramatically improve their overall risk profile in a way that will produce extremely favorable results. The issue isn't going away and the consequences of data failure will be increasingly severe in the future.

General Data Protection Regulation (GDPR) was introduced in the European Union in 2018, but its effects are being felt globally: for example, Equifax could have suffered greater damages given today's regulatory landscape. The issue will likely become even more restrictive in the future, with the likes of California's Consumer Privacy Act slated to take effect in 2020. The stakes around sensitive data such as PII are high and they're only going to get higher.

In this environment, a new solution is necessary and the superior security results that can be obtained by a prudent and holistic embrace of public cloud resources can be a lifeline for the security teams at financial services companies.

TWELVE THREATS, VULNERABILITIES, AND EVENTS

As discussed, the threats to your systems and your data in the cloud are closely related to those of an on-prem system. These risks fall into one of three categories: threats that lead to system compromise, vulnerabilities that leave your systems exposed, and events that could impact your business arising from the vulnerabilities and threats.

Threats That Lead to System Compromise

- Malicious Insiders: A threat that originates from the inside, whether from your own staff or from trusted partners, is often the hardest to detect and is, therefore, potentially the most dangerous type.
- Abuse and Nefarious Use of Cloud Resources: Insufficiently secured cloud service deployments expose a number of risks, some of which can extend outside of the enterprise, such as email phishing or the mining of cryptocurrencies.
- Account Hijacking: This involves bad actors gaining control of accounts and stealing information, maliciously altering data, or re-directing traffic to illegitimate sites. The resulting confusion and loss of reputation can cause incalculable harm.
- Advanced Persistent Threats (APTs): APTs are notable for their long-term and often slow strategy of infiltration followed by long-term operation, making them particularly difficult to detect. In many cases, significant damage has already been inflicted by the time an APT is detected.

SECURING PII DATA IN THE CLOUD FOR FINANCIAL SERVICES

Vulnerabilities Leaving Your Systems Exposed

- Poor Identity, Credential and Access Management: If the tools to manage and monitor identities and access are incomplete or have blindspots and holes, the whole system is vulnerable to attack, theft, and more.
- Insufficient Planning & Security Design: Adding new resources and processes without first performing sufficient analysis and testing can lead to heightened financial, legal and business risk.
- Insecure Interfaces and APIs: Interfaces and APIs are entry points into a system and, if poorly designed, they can become chinks in the security armor. Any weakness at these points provides an entry for malicious actors who then have an unfettered ability to wreak havoc.
- Systems Vulnerabilities: Bugs in underlying hardware, firmware and software such as CPUs, OSs and third party components can also expose a system. Services that share data in close proximity are particularly susceptible in such an instance.
- Shared Technology Vulnerabilities: Flaws in the security of underlying third-party or open source components provide other vulnerability vectors to be dealt with. A small flaw can become a big liability if it is exploited in order to circumvent system security.

Events That Could Impact Your Business

- Data Breaches: As large corporations such as Yahoo, Marriott, Target, Equifax and many others can attest, a data breach is a major security lapse. Whether the breach is due to a targeted attack, human error, or lax policies, the legal, financial and reputational costs can be astronomical.
- Data Loss: Not all issues with data stem from it being stolen: sometimes it is lost due to accidental deletion or a physical catastrophe, such as a fire, storm, or earthquake. In addition to the high cost and difficulty in trying to recover lost data, there may also be business continuity and contractual concerns.
- Denial of Service (DoS): A DoS attack occurs when system resources are overwhelmed by a large, coordinated traffic influx. These are nothing new, but the proliferation of cloud capabilities can make them faster, stronger and potentially much more expensive. A DOS attack also puts the company's reputation at risk and can impact contractual obligations.

The amount of exposure to these issues and the relative importance of each is variable based upon the specific facts and circumstances of each case but this list serves as a handy guide to ensure that all issues are addressed and, more importantly, no threats, vulnerabilities or events are overlooked in your analysis.

CONTACT

Andrew Dunmore
Senior Principal,
Financial Services Lead

Phone: + 1 312-509-4890

Email : andrew.dunmore@mavenwave.com
Website: www.mavenwave.com