Empowering SaaS Providers with a Secure Cloud Architecture

White paper by phoenixNAP
February, 2021

INTRODUCTION: Why Security is Key to Delivering Excellent SaaS Solutions

Software as a Service (SaaS) remains the largest market segment in cloud computing. According to Gartner, the SaaS market is on track to surpass the $130 billion mark in 2022[1].

This growth offers a great potential for SaaS providers to expand their business and diversify their offering. However, as organizations continue to rely on SaaS solutions to enhance business productivity, employee collaboration, and data security, SaaS providers are facing increased pressure to deliver advanced levels of performance and security. Underperforming apps will inevitably have a negative impact on providers' ability to acquire new customers, ensure user satisfaction, and, most importantly, grow their revenue stream.

Similarly, the lack of mechanisms to protect against common security threats can cause significant business disruptions, resulting in loss of productivity and profit. The 2020 survey report by Infrascale reveals that SMBs lose between $10,000 and $50,000 per one hour of downtime[2]. The stakes are much higher in enterprise, where a quarter of organizations report per-hour downtime costs of $301,000 - $400,000, while 17% loose more than $5M[3]. In addition to this, cyber breaches and major outages can make a permanent damage to the company's reputation and cause loss of customers' trust.

SMBs lose between **$10,000 and $50,000** per one hour of downtime.

This is why data security is a common concern for SaaS providers, especially if they operate in regulated sectors such as Finance and Legal where security is the core business foundation. Recognizing their challenges, this white paper aims to provide guidelines and best practices for ensuring data security by leveraging phoenixNAP's Data Security Cloud platform. SaaS providers looking to enhance their infrastructure security will learn:

- What the common SaaS security concerns are and what it takes to ensure data security.
- How SaaS providers can meet the demands for performance and security using a scalable infrastructure.
- How to easily deploy a secure cloud-based architecture that offers multi-layered data protection.
- What the key features of phoenixNAP's Data Security Cloud are and how it helps SaaS providers meet their security and compliance goals.

[1] **Gartner Press Release, November 17, 2020.**

[2] **Survey highlights the heavy cost of business downtime for SMBs, TechRadar**

[3] **Average cost per hour of enterprise server downtime worldwide in 2019, Statista**

SaaS Security Concerns

SaaS customers are increasingly worried about data security in the cloud. While the original resistance to moving critical applications to remote servers has largely faded over the past few years, there are still concerns over the secure implementations of SaaS software. SaaS vendors are under pressure to keep their customers' data protected even in case of a breach or a data disaster on the customers' end. Achieving that often requires SaaS vendors to ensure:

- **Access to enterprise-grade cloud security systems** to ensure automated threat detection and monitoring, vulnerability scanning, real-time security analytics, and off-site backups.
- **Availability of skilled security engineers** to enable implementation of these systems and ensure environment security.
- **Implementation of security policies and procedures** to minimize risks and enable timely response to potential attacks.
- **Sufficient budget and cost control** for all security investments.

The lack of comprehensive security strategy stifles SaaS providers' abilities to respond quickly to security threats and protect their sensitive data. However, development of such a strategy if often associated with high implementation costs. SaaS providers, therefore, need to choose a solution that provides them with adequate safeguards while enabling them to optimize their IT costs.

Agility and Security Requirements for SaaS Providers

SaaS enables faster and more standardized implementations of software solutions. This is largely due to the fact that SaaS reduces the financial and operational burdens that traditional software places on the end-user. With SaaS, all those troubles are transferred from the end-user to the SaaS provider. By exchanging CapEX for OpEX, users benefit from low cost to entry, optimized spending, and no software or hardware maintenance costs. Businesses that leverage SaaS solutions also reap the benefits of greater software efficiency, reduced operational complexity, and business agility.

To deliver this level of flexibility to end-users, SaaS providers rely on powerful yet highly agile and cost-effective cloud infrastructure. After all, SaaS providers are not delivering just software apps, but a complete solution. This is why improved delivery, support, and maintenance at the infrastructure level play a pivotal role for SaaS providers.

SaaS providers have a **greater responsibility** in terms of security.

In addition to that, SaaS providers have a greater responsibility in terms of security. Hosting third-party data requires total control over security operations both at the application and infrastructure levels. Even though the public cloud provides advanced security, data-sensitive SaaS apps need much higher levels of protection compared to the traditional public cloud. For example, providers that store or process credit cards, PII, or health records, need their infrastructure to be compliant with legal requirements and have appropriate certification.

5 Critical Components for SaaS Provider Infrastructure

From an infrastructure perspective, there are five critical components SaaS providers in finance and legal sectors must consider before choosing an infrastructure provider.

PERFORMANCE

Slow-loading or unresponsive SaaS apps can negatively impact revenues, conversion rates, brand reputation, end-user satisfaction, and service level agreements. While the underlying infrastructure, servers, and networking technologies have a big impact on performance, those are not the only factors. Performance and app responsiveness also depend on the number of users trying to connect to the app, quality of the code, resource optimization, and other factors. To get optimal performance results, SaaS providers have to be able to scale their compute, network, and bandwidth resources easily, and ensure consistent performance even at peak times.

SCALABILITY

Most SaaS solutions on the market today are hosted in virtual cloud environments because virtual resources offer unlimited scalability, greater flexibility, and agility. This gives SaaS providers the ability to add compute, memory, or storage resources on demand. If the number of users grows rapidly, they can scale resources instantaneously while ensuring maximum performance. Hosting SaaS apps on highly scalable infrastructure means that providers can avoid scenarios in which they are forced to make big investments in hardware in order to support growth.

COSTS

Apart from scalability, virtualization is all about cost-optimization and right-sizing infrastructure eliminate spending on unused IT resources. Cloud environments include pay-per-use billing options which help SaaS providers reduce their capital expenses. This level of flexibility allows them to offer their services at a much lower price-point compared to hosting apps on an on-premises infrastructure. The cloud also makes growth planning much simpler, as providers do not need to worry about purchasing hardware in advance. As a result, end-users never have to suffer through extensive maintenance windows or service outages.

SECURITY

As SaaS apps grow in complexity, providers must take a security-first approach when building their hosting environments. The attack surface for SaaS apps becomes greater as they span across multiple providers and hosting solutions, making it more difficult to secure all end points. In general, SaaS apps are usually susceptible to volumetric DDoS attacks, brute force attacks,

as well as vulnerability and unencrypted data exploits. The impact of these attacks ranges from service downtime, reputational damage, customer and revenue loss, as well as high costs related to damage control.

COMPLIANCE

Ensuring the integrity and confidentiality of sensitive data is paramount for delivering SaaS apps, especially those built for finance and legal sectors. Apps that deal with credit card data and personally identifiable information (PII) must comply with different security standards. With on-premises environments, SaaS providers are burdened with capital expenditures related to network security devices, staffing, regulatory compliance, physical security requirements and access controls, and so on. Running SaaS apps in a cloud environment helps providers significantly reduce infrastructure compliance issues. That is because the burden of infrastructure compliance is transferred over to the infrastructure provider. However, most public cloud providers do not offer compliance-ready virtual environments. When choosing an infrastructure vendor, SaaS providers that process sensitive data must host their apps in environments that comply with PCI DSS and other relevant industry standards.

AVAILABILITY

In this day and age, where milliseconds of downtime can impact revenue, SaaS customers require 24/7 availability of their apps. They need fast and highly available resources to maintain business operability. As a result, SaaS providers often guarantee near-100 percent availability levels coupled with rigorous RTO/RPO commitments. When SaaS apps are latent or experience prolonged downtime, customer frustrations grow and they start looking for alternatives. This can result in lost revenue, customer churn, and a damaged reputation. Cloud solutions that include robust DDoS protection are a must for apps that require high availability. In addition to that, regular backups and disaster recovery options play a critical role in maintaining operability in case a disaster strikes.

Addressing SaaS Security with a Secure-by-Design Cloud Platform

phoenixNAP's Data Security Cloud was designed to address common infrastructure security concerns by providing high-performance architecture that delivers reliable performance and advanced security on an OpEx-based model.

As a multi-tenant virtualized cloud platform, Data Security Cloud offers the flexibility and agility of the public cloud coupled with the addition of advanced built-in security components. Powered by the latest generation hardware and advanced hypervisor technologies from VMware®, Data Security

Data Security Cloud was designed to address common infrastructure security concerns.

Cloud delivers speed, agility, and unlimited flexibility in managing virtual machines. As a secure-by-design platform, it is a layered architecture complemented by intelligent threat detection and automated vulnerability scanning technologies. This gives SaaS providers even in Finance and Legal sectors peace of mind in delivering redundant and security-centric apps to their customers.

Data Security Cloud Architecture Overview

Data Security Cloud is built through strict virtualization and segmentation controls leveraging advanced hypervisor technologies from VMware. Running on top of VMware's vRealize Suite and vCloud Director technologies, Data Security Cloud makes it easy for SaaS providers to create hybrid cloud solutions between their on-premises and Data Security Cloud implementations. The platform is also supplemented by a VMware vCenter Log Insight log collection and aggregation platform that streams security-related incidents to a LogRhythm SIEM. This allows our 24×7 Security Operations Center (SOC) to take immediate action to mitigate cyber threats before they make an impact.

Using VMware HCX (Hybrid Cloud Extension), Data Security Cloud helps SaaS providers bridge the network gaps to hosted cloud services while maintaining network access and control. VMware's industry-leading NSX network virtualization product portfolio allows for the creation of logical security policies that can be applied to a Virtual Machine regardless of location (cloud or on-prem).

Directly integrated into Data Security Cloud, threat intelligence provides SaaS vendors with always-updated intelligence feeds, anti-virus and vulnerability scanning, end-point protection, as well as Machine Learning and behavioral analytics. These intelligent threat monitoring features significantly reduce the likelihood and impact of cyber threats, enabling SaaS providers to keep their customers' data protected at all times.

To mitigate potential damage and ensure operability and availability even in case of a disaster, Data Security Cloud is integrated with an industry-leading backup solution. This ensures SaaS providers are able to restore a fresh copy of their workloads and quickly recover from a potential ransomware attack or other types of cyber-attacks.

Physical Security

phoenixNAP's data centers that house the Data Security Cloud infrastructure are SOC-1, SOC-2, and SOC-3 audited. These certifications establish a baseline for physical and logical access control,

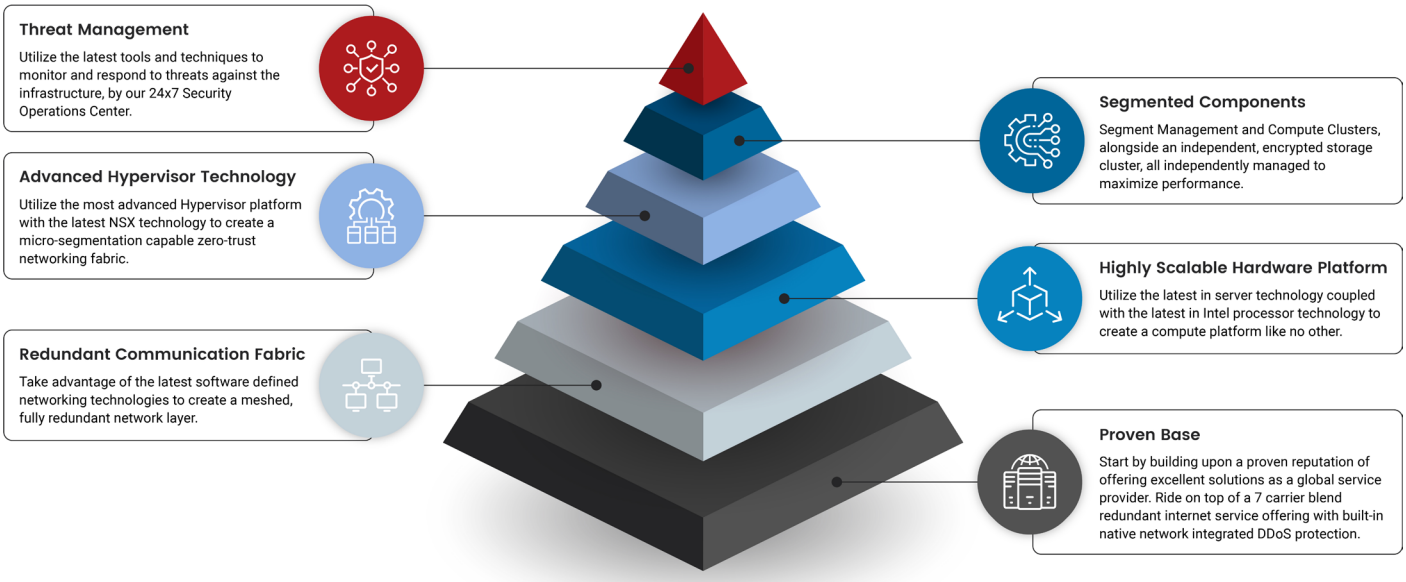
data security, and business continuity procedures. On top of that, our PCI-DSS certification allows financial and legal SaaS providers to process sensitive payment data with confidence and without worrying about compliance.

Advanced Performance

Along with advanced security, Data Security Cloud enables SaaS providers to deliver fast, responsive, and performant services across the globe. This is thanks to the latest generation processor technologies that power the Data Security Infrastructure at its core. SaaS providers can rely on stable performance even under peak load which directly translates into greater customer satisfaction. As the number of customers increases and the need for more compute power grows, SaaS providers can easily scale their Data Security Cloud infrastructure to support growing demand. Data Security Cloud can be scaled vertically and horizontally, just like a typical public cloud solution. All providers have to do is leverage familiar VMware tools to add CPU, memory, and storage resources to the resources pool.

It's all about the layers

Data Security Cloud is a layered secure-by-design cloud infrastructure. This means that if one security layer is compromised, the defense process begins by escalating the tools and techniques to the next one. In building this type of infrastructure, we were guided by the notion that a layered approach creates a secure and stable solution that can easily be scaled laterally as the needs and the customer base grows.



Secure at the Foundation

- Root of trust module (TPM)
- Built-in instruction sets for verification (Intel TXT)
- Fast, high-quality random number generator (RDSEED)
- Firmware assurance (BIOS Guard)

Built-in Ecosystem

- Efficient provisioning and initialization (Intel PTE)
- Scalable management with policy enforcement (Intel CIT)
- Direct integration with HyTrust and VMware, etc.
- Secure Enterprise Key Management
- Trusted connectivity
- Remote attestation for the secure platform
- Compliance and measurement at the core

Empowering Financial and Legal SaaS Providers

Infrastructure is key to running a successful SaaS business. Developing, testing, and deploying SaaS apps on Data Security Cloud enables providers to lower their total cost of ownership and time to market. Along with that, Data Security Cloud helps providers maintain:

1. **Easier development and deployment:** Having the ability to deploy infrastructure quickly into new and existing environments is what SaaS providers often struggle with. Waiting for days or even weeks to deploy resources delays the process of onboarding users, releasing new features, and generating revenue. Data Security Cloud helps providers spend less time managing their environments and more time on developing and releasing new features that generate revenue.

2. **Optimize resource management and costs:** Accurately planning for the growth of SaaS apps may seem like an impossible task. The adoption rates may vary, and providers are likely to experience occasional peaks in demand. Choosing the right infrastructure provider is critical to handle such peaks. Data Security Cloud gives SaaS providers the ability to scale their resources seamlessly without straining their budgets. It allows for granular scalability and unlimited freedom for customization to support growing demand. As a result, SaaS providers can grow on their terms all the while reducing their IT costs with predictable budget-friendly billing options.

3. **Data security and segregation:** Segmenting user data to ensure privacy is critical for financial and legal SaaS solution providers. If one virtual machine experiences a breach, providers must be able to contain the impact and prevent attackers from moving laterally through the data center. Data Security Cloud gives SaaS providers granular control over security across multiple VMs. Providers leverage VMware tools to carefully segment and configure their VMs according to specific needs and requirements. Along with that, its built-in backup solution enables them to recover fresh copies of their data in case of a breach, disruption, or accidental deletion.

CONCLUSION

The SaaS market is growing rapidly because businesses realize the operational and financial benefits of offloading certain operations to third parties. In doing so, businesses of any size can meet market demand more quickly.

This is especially true in the rapidly evolving financial and legal sector. SaaS providers not only have to deliver right-sized feature-rich solutions, but they also have to worry about the underlying digital infrastructure powering their apps. Apart from performance, scalability, and cost-effectiveness, advanced security is a top priority item for SaaS providers offering solutions in the financial and legal fields.

phoenixNAP's Data Security Cloud is an ideal solution for hosting and running data-sensitive workloads. It gives SaaS providers complete control over their environments, along with intelligent threat detection and off-site backups out-of-the-box. As a compliance-ready solution, Data Security Cloud also allows providers to store sensitive data and meet regulatory demands.

For details about **Data Security Cloud features and plans**, visit: **phoenixnap.com/security/data-security-cloud** or contact **sales@phoenixnap.com** for a quote.

vmware Principal Partner Cloud Provider

vmware CLOUD VERIFIED

About phoenixNAP

phoenixNAP is a full-service IaaS provider delivering programmable, OpEx-friendly infrastructure solutions from strategic edge locations worldwide. Focused on innovation, cyber security, and compliance-readiness, phoenixNAP collaborates with technology industry leaders to make enterprise-grade technologies available at an OpEx-based model. Its cloud, dedicated servers, availability, HaaS, and colocation solutions can be customized to meet any businesses requirement.