DATA SECURITY CLOUD

Anatomy of a **Secure Cloud Service**

phoenixNAP® GLOBAL IT SERVICES

E-book by phoenixNAP | February, 2020

Table of Contents

Leadership and Partnership

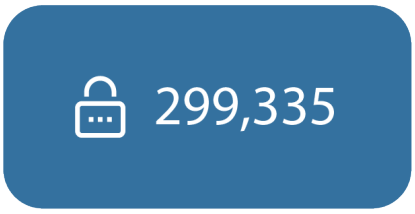
Definitions are critical; essential even. The term "leadership", for example, is defined simply by Google dictionary, as "The action of leading a group of people or an organization." At phoenixNAP, leading in our industry is part of our DNA and culture. We define leadership as creating innovative, reliable, cost-optimized, and world-class solutions that our customers can easily consume.

In that vein, the term "Cloud Infrastructure" (or its predecessor "Cloud Computing") tend to represent multiple different scenarios and solutions, drummed up by overzealous marketing teams. Without a clear definition, clarity around the terms is convoluted at best. "Cloud Security," however, is more often described as representing concerns around data confidentiality, privacy, regulatory compliance, recovery, disaster recovery, and even vendor viability. We aim to bring clarity, specificity, and trust into this space through our Cloud Security solutions.

The Road Ahead: The Security Landscape

According to Heng & Kim (2016) of Gartner, by 2020, 60% of businesses will suffer a failure of some sort, directly attributed to their internal IT team's inability to manage risk effectively. 87% of nearly 1200 global C-Level executives surveyed by E&Y say they needed 50% more funding to deal with the increased threat landscape. Compound that problem by the fact that we are facing a global skills shortage in technology and security services. These issues directly impact the ability of organizations to maintain and retain their Information Technology and now their Cybersecurity staff.

Unifilled Cybersecurity Jobs in AZ



Unifilled Positions Nationwide

Unifilled Positions by 2019

While the industry prepares for this potential security epidemic, predictions state that a consolidation of the vast number of security services providers is going to take place, along with an increased focus and reliance on automation and machine learning tools (Heng & Kim, 2016). Despite public concern, this may not be such a bad thing. The growing sophistication of these tools, the ability to perform analytics and correlation in many dimensions, and the automation capabilities, could create efficiencies or potentially, advancements in our defensive capabilities.

Industry-leading providers in this space are not standing idly by. As such a provider, phoenixNAP is at the forefront of many initiatives, ranging from local to international. For example, it is critical that we begin to foster knowledge in children as young as grade school to gain an interest in the field. Working with industry organizations, we sponsor events and take leadership roles in organizations to support curriculum development and the awareness. We are leading efforts in threat intelligence

sharing, and the use of disparate dark web data sources, to create a predictive analysis that can be operationalized for early threat vector identification. Additionally, we have partnered with the United States Armed Forces and U.S. Department of Veteran Affairs to provide pathways for those service members interested, to have a low barrier of entry, and to have a dedicated support system, so that they can successfully transition into cyber roles as civilians.

"Leadership," we view as our social responsibility and our contribution to enhancing the security posture of our market segment.

Why is this Relevant to the Cloud?

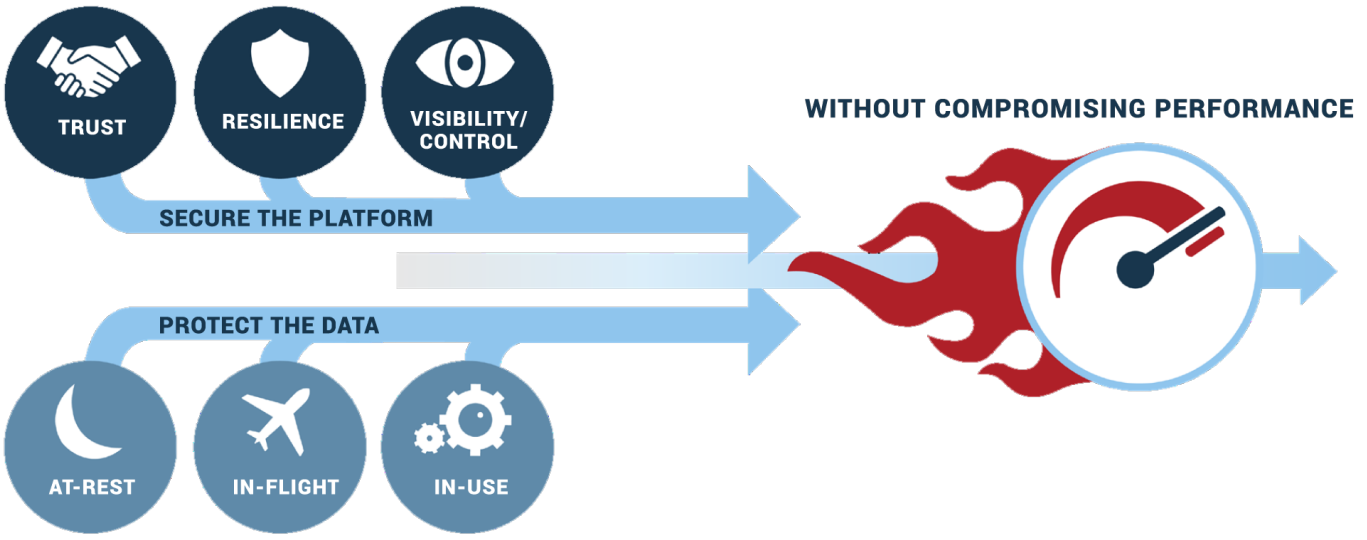
A Gartner study from 2015 predicted a 16% year-over-year annual growth rate. The reality is that as we approach the 2020 mark, we see a 32% increase in IT spending on cloud services. That same study identified that about 40% of IT budgets are now allocating for cloud or SaaS related services.

"These growing statistics are relevant because this is going to influence your existing cloud strategy dramatically, or if you don't have one, this should alert you that you will soon require one."

Secure Solutions From Our Unique Perspective

It is safe to assume you are already in the cloud, or you are going there. Our focus is to educate on what we believe are the most significant components of a secure cloud infrastructure, and how these components complement and support the security needs of modern business. Just as the path-goal theory emphasizes the importance of the relationship to the goal achievement, as a technology service provider, we believe in partnering with our customers and going the extra mile to become mutually trusted advisors in product creation and sustenance. The cloud is in your not-too-distant future. Let us keep you safe and secure, and guide you along the way.

At phoenixNAP, we have a unique perspective. As an cloud services we offer a service portfolio of complementary tools and services to provide organizations with holistic, secure, cloud-based solutions. With that in mind, we identified a gap in the small, and medium-sized business space (SMB), and their barriers to entry, for access to cutting-edge technology such as this. We knew what we had to do: we developed the tools to help these businesses with access to a world-class secure cloud-based solution offering, which met and supported their regulatory needs. We set the bar on performance, recoverability, business continuity, security and now compliance pretty high. Our passion for small to medium-sized businesses and dedication to security is why we built the Data Security Cloud. Our Data Security Cloud is an aspiration to create the world's most secure cloud offering.



We wanted a way to build a solution that would be the Gold Standard in security, but also entirely accessible to everyone. For that to happen, we needed to commoditize the traditionally consultative security services offerings and offer it at an affordable OpEx cost structure. That is exactly what we did.

Cloud Security is a Shared Responsibility

The 2017 Cloud Adoption Survey found that 90.5% of respondents believe that Cloud Computing is the future of IT. As many as 50.5% of these respondents still identified security as a concern. Of those concerns, the following areas were of particular interest:

1. **Data and application integration challenges**
2. **Regulatory compliance challenges (54% indicated PCI compliance requirements)**
3. **Worries over "lock-in" due to proprietary public cloud platforms**
4. **Mistrust of large cloud providers**
5. **Cost**

We architected our solution from the ground up, with these perspectives in mind. We identified that we needed to monitor, actively defend, and resource a Security Operations Center (SOC), to respond to incidents 24×7 globally. We designed a solution where we partner with each of our customers to share in the responsibility of protecting their environment. Ultimately, this strategy contributes to protecting the privacy and confidentiality of their subsequent customers privileged, financial, healthcare, and personal/demographic data. We set out to design a system to empower your goals towards your security posture.

Data Security Cloud - The Layers of Security

Data

The good stuff.
The information you want to stay secure.

Threat Management

Know what you have, know your baselines, watch for anomalies.

Reference Architecture

Build it right, by following already vetted designs, minimize the potential holes that can be exploited.

Micro Segmentation

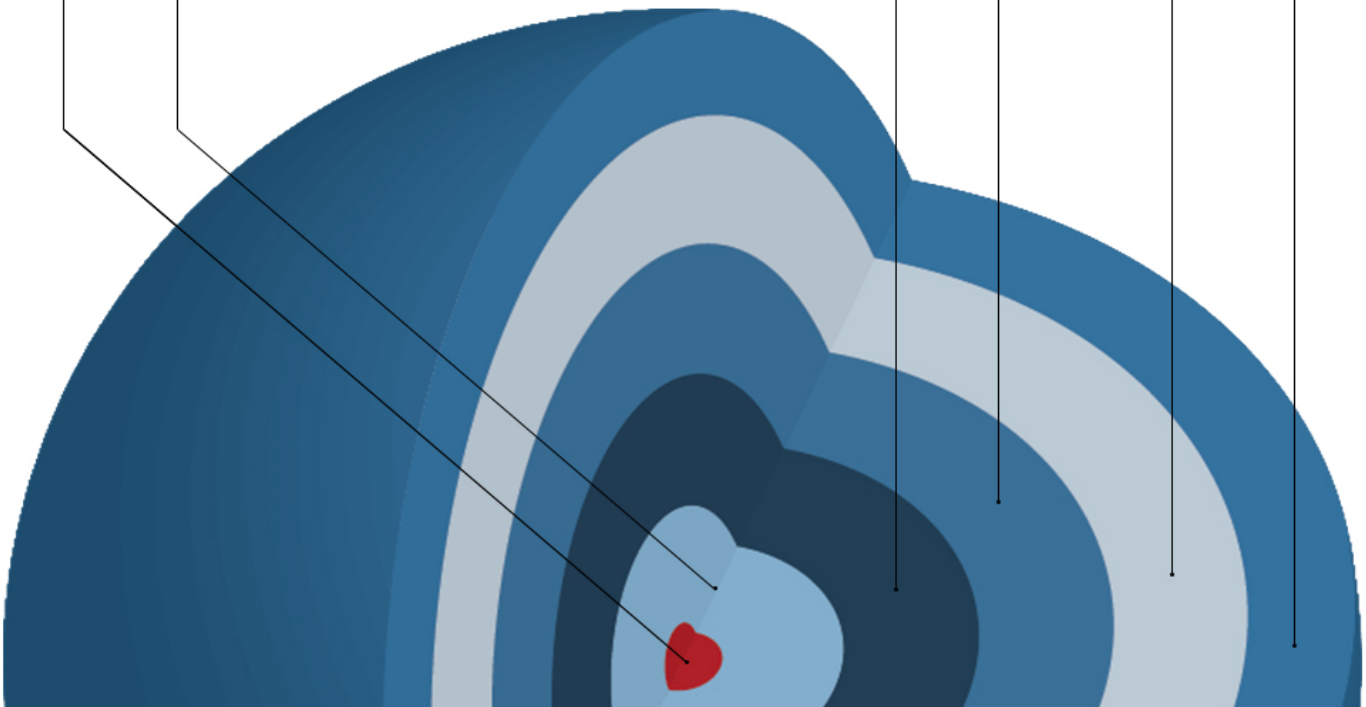
Only let machines and ports intended to talk to each other, to do that. Even on a flat network.

Encryption

Your 1st line of defense. If it becomes compromised, make it harder to penetrate.

Secure OS

Encryption is great 'at-rest'. When your machine is running: work with your data in a hardened environment.



Our challenge, as we saw it, was to commoditize and demystify the security space. We have invested significant resources in integrating tools and pushed vendors to transition from a traditional CapEx cost model to an OpEx pay-as-you-grow model. Ultimately, this strategy enables pricing structures that are favorable for this market segment and removes any barrier of entry, so that our customers can access the same tools and techniques formerly reserved for the enterprise space.

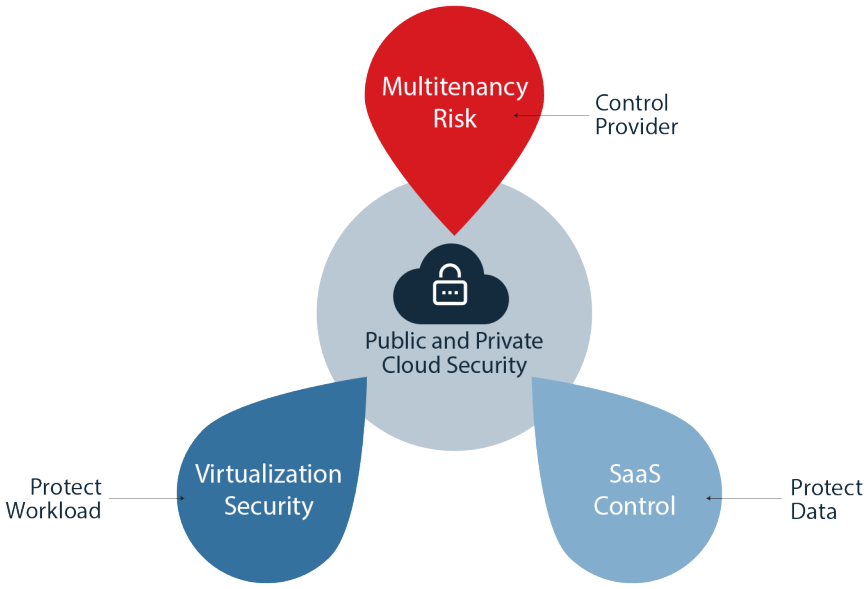
We can't wait to show you what we came up with. We think you are going to love it.

What are Cloud Services?

When speaking of Cloud Services, we have to define the context of:

Private Cloud

- A Private Cloud typically represents the virtualization solution you have in-house or one you or your organization may host in a data center colocation.
- Optimizing the use of idle time on a typical compute workload, by aggregating multiple workloads onto a single host, the Private Cloud will take advantage of the resource over-provisioning inherent of a hypervisor platform.
- You own your Private Cloud. It is technically in your facility, under your operational control. The confidence in the security controls are therefore high, yet dependent on the skills and competency of the operators and their ability to keep up with proper security hygiene.
- The challenge, however, is that you still have to procure and maintain the hardware, software, licensing, contingency planning (backup and business continuity), and even the human resources described above. Including the organizational overheard to continuously develop and manage these resources (training, HR, medical/dental plans, etc.).



Public Cloud

- A public cloud is an environment where a service provider makes a virtualization infrastructure available for resources such as virtual machines, applications, and/or storage. These resources are open to the general public consumption over the internet. The public cloud is typically an environment operated under a pay-per-use model, where the customer pays only for what they have subscribed and/or committed to.
- We can categorize public cloud further as:
  - Software-as-a-Service (SaaS). A great example of SaaS is Microsoft's Office 365. Although you can use a lot of the tools via the internet browser itself, you can also download the client-facing software, while all the real work happens within the cloud environment.
  - Platform-as-a-Service (PaaS). A solution where the cloud provider delivers hardware and software tools, typically in an OpEx model.
  - Infrastructure as a Service (IaaS). When we refer to the public cloud, this is typically the service most people refer to. A typical scenario is when you visit a website and order a virtual Windows Server; with X amount of processors, Y amounts of RAM, and Z amounts of Storage. At phoenixNAP, we offer this style of service. Once provisioned, you install Microsoft Internet Information Services (IIS) and Wordpress, you upload your site, and now you have an internet facing server for your website. Consumers drawn to this model are typically cost-conscious and attempting to create their solution with the least expenditure. Things like an Internet-facing firewall could be overlooked or entirely skipped. Strong system architecture practices such as creating separate workloads for web platforms and database/storage platforms (with an internal firewall) may also suffer. What might be obvious at this point is that this is one of those areas of intense focus when we created our solutions.
- Our value proposition is that this type of cloud platform reduces the need for the organization to invest and maintain its on-premise infrastructure, resources or even annual service contracts. Although this will reduce resource needs, it will not eliminate them. As most licensing costs are either included via the provider and most likely available at significantly reduced price-points through the provider's economies of scale, you are also guaranteed to get some of the best pricing possible.

TRADITIONAL IT	PUBLIC CLOUD

Asset Costs
• Server Hardware
• Storage Hardware
• Networking Hardware
• Software Licensing
	Virtual Infrastructure Costs
	• Server Costs
	  • vProcs
	  • vRAM
	  • vStorage
	• Software License Costs
	• Professional Services
	• Bandwidth Costs
	• Managed Services Costs

Labor Costs to Maintain Infrastructure	
Physical Data Center Costs • Power • Cooling • Security • Insurance	
Outsourcing/Consulting Costs	
Communications/Network Costs	

The following table contrasts the shifting cost allocation model (Ji, 2017):

Hybrid Cloud

- Consider the Hybrid Cloud as a fusion between the Private and Public Cloud. The desired goal is for workloads in both of these environments to communicate with each other, including the ability to move these workloads seamlessly between the two platforms.
- Though this is also possible in the other scenarios, in the case of the Hybrid Cloud, it is typical to see a public cloud environment configured like an on-premise environment. This scenario could have proper North-South traffic segmentation, and in the rare case, proper East-West traffic segmentation facilitated by either virtual firewall appliances or most recently VMware NSX based micro-segmentation technology.

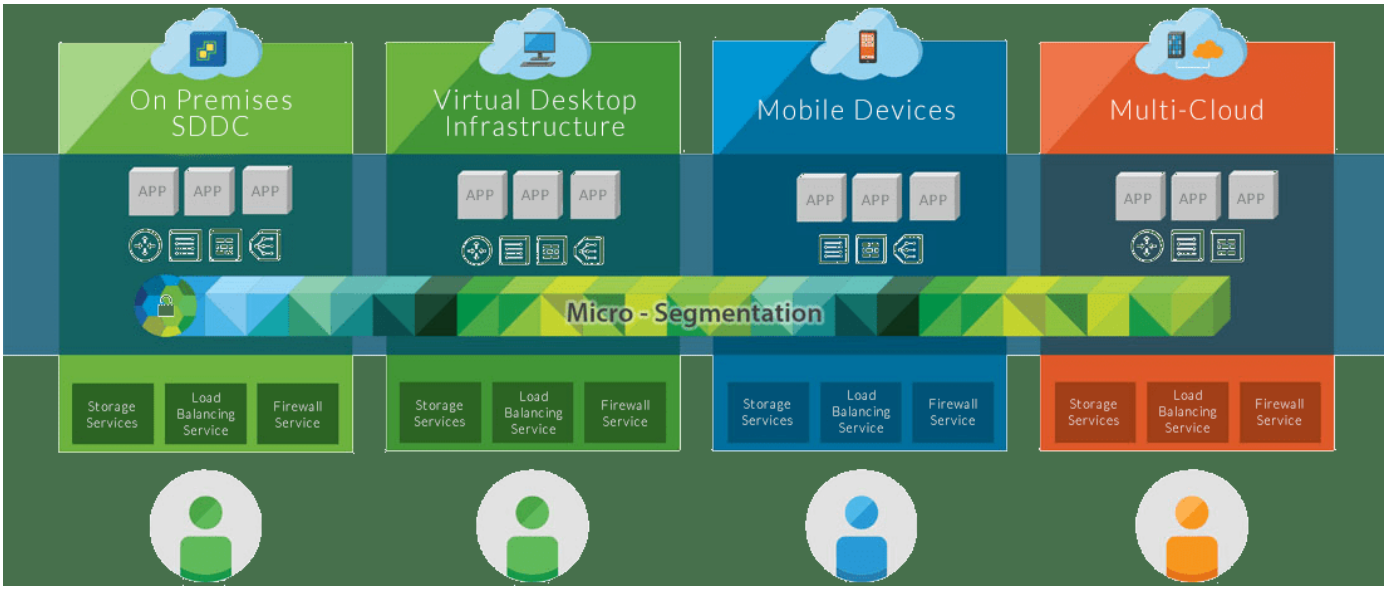
What Role Do Control Frameworks Play?

Control Frameworks are outlines of best practices. A strong and defined set of processes and controls that help the provider adhere to proper security posture. Posture that can be evaluated, audited and reported on, especially when subject to regulatory requirements verified by an audit process. What this means to a consumer is that the provider has built a standards-based solution that's consistent with the industry. They have not cut corners, they have made the effort to create a quality product that's reliable and inter-operable should you need to port-in or port-out components of your infrastructure. A standards-based approach by the provider can also be leveraged for your own regulatory compliance needs, as is may address components on your checklist that you can assign to the provider.

Partnering With the Best

Market share numbers are a quantitative measure, although subject to a level of alpha, it is still statistically sound. Intel and VMware are clear leaders and global innovators in this space. Product superiority, a qualitative measure, is a crucial asset when integrating components to create innovative solutions in a highly demanding space. At phoenixNAP, we are proud of our ongoing partnerships and proud to develop products with these partners. We believe in the value of co-branded solutions that innovate yet create stable platforms due to longevity and leadership in the space.

Developing our Data Security Cloud (DSC) product offering, we had the pleasure of working with the latest generation of Intel chipsets and early release VMware product code. We architected and implemented with next-generation tools and techniques, not bound by the legacy of the previous solutions or methodologies.



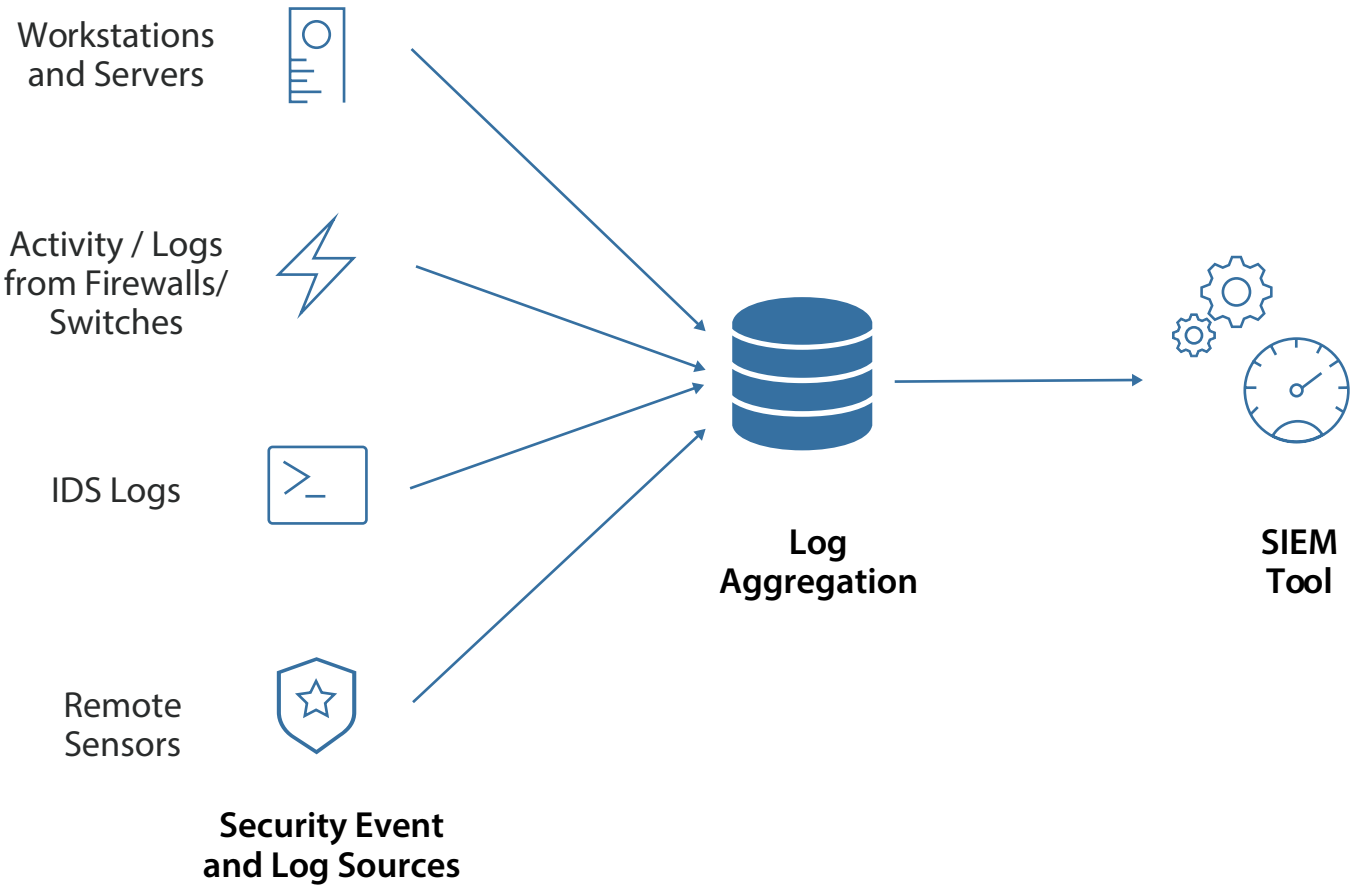
We incorporated VMware's vRealize Suite and vCloud Director technologies into a world-class solution. At phoenixNAP, we not only want to empower our customers to manage their operational tasks themselves but by using the industry standard VMware as a platform, we can create hybrid cloud solutions between their on-premise and Data Security Cloud implementations.

Starting Fresh

As we wanted to design a secure cloud service offering, we chose not to be influenced by legacy. Starting with a whole new networking platform based on software-defined-networking, we created and built a flexible, scalable, solution, incorporating micro-segmentation and data isolation best practices. We designed this level of flexibility and control throughout the entire virtualization platform stack and the interconnecting communications fabric.

Design Methodology

We drew upon our extensive background in meeting compliance goals; incorporating a framework approach, using industry best practices, anticipating the needs and limitations inherited with achieving industry and compliance certifications such as PCI, HIPAA (coming soon), and ISO 27002 (coming soon). We designed a flexible, yet secure architecture, supplemented by a VMware LogInsight log collection and aggregation platform, that streams security-related incidents to a LogRhythm SIEM, monitored by our 24×7 Security Operations Center (SOC).



We Proved It

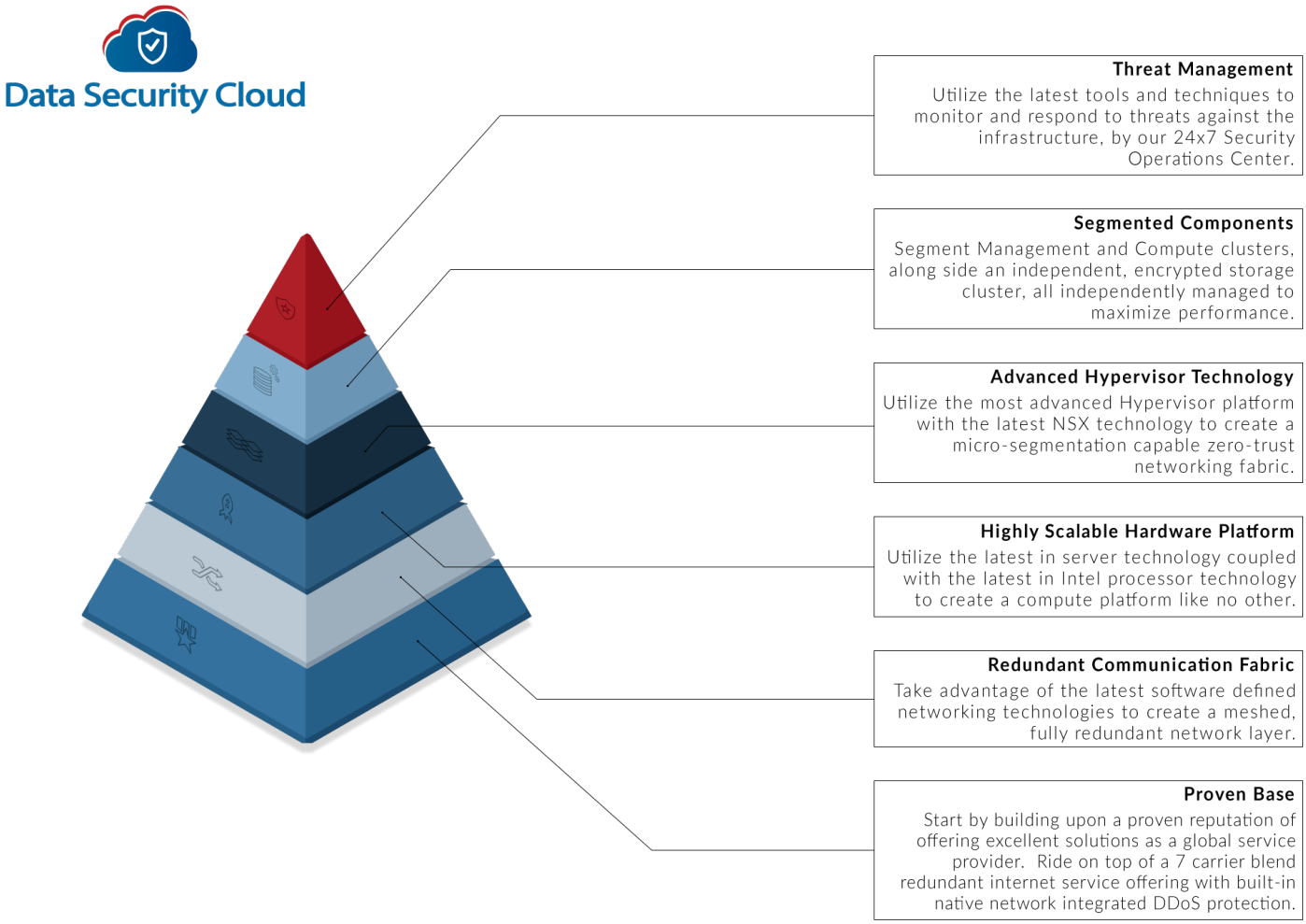
What better way to prove that we achieved our goals in a security standard than to have the most respected organizations validate and certify us. We had TrustedSec evaluate our environment, and have them attest that it met their expectations. However, we didn't stop at just achieving compliance alone. Additionally, as security professionals, we audited our environment, going over and beyond the regulatory standards. We designed our framework to have a "no compromise approach," and our fundamental philosophy of "do the right thing" from a technical and security perspective. Proved by our PCI certification of this secure cloud platform.

The Launch of our Security Services Offering

After years of extensive testing and feedback from our customers, we built our Threat Management and Incident Response capabilities into a service offering, available to our entire customer base. We enhanced our Security Operations through the integration of advanced Security Orchestration and Automation tools, and through strategic partnerships with public and private Information Sharing and Collaboration (ISACs) organizations. By collecting threat vector data globally and from the dark web, we utilize unique enrichment techniques to perform predictive profiling of the social structure of this society. Our goal is to create actionable intelligence or early warning systems, to support our defensive posture in real-time through our own systems.

What this means is that we are building advanced tools to detect threats before they impact your business. We are using these tools to take preventative action to protect customer networks under our watch. Actions which could see the latest threat pass you by without including you in its wake.

Layered Approach to Creating a Secure Cloud Infrastructure

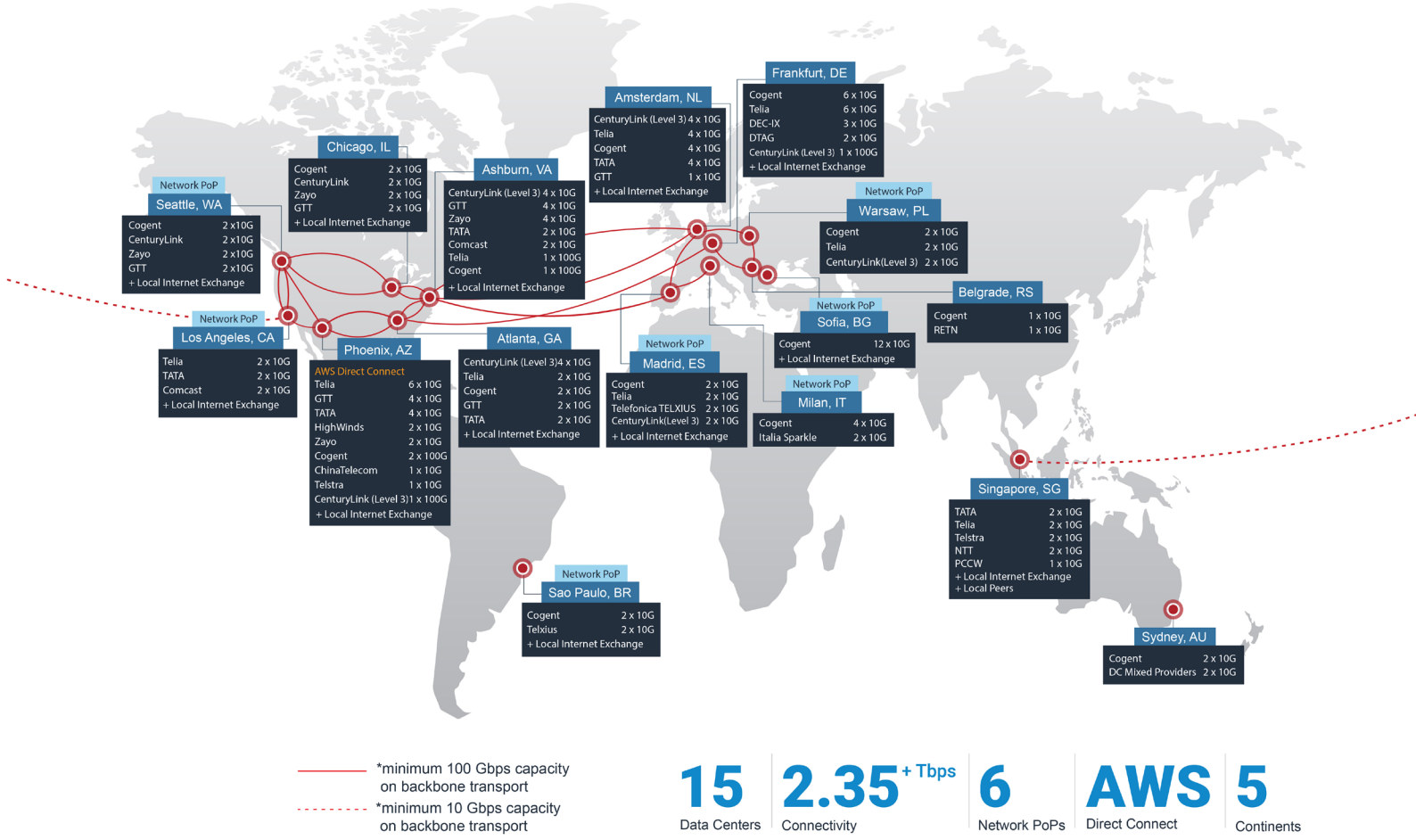


Proven Base

phoenixNAP has a long and proven history in designing, developing, and operating innovative infrastructure solutions. With a parent company in the financial transactions sector, we have extensive knowledge and expertise in the secure operations of these critical solutions. As an operator of global data center facilities, we have established a trustworthy reputation and operational process, to support the needs of our diverse and vast client base.

Our certifications in SOC-1, SOC-2, and SOC-3 establish a baseline for physical and logical access control, data security, and business continuity procedures. Our Type II designation verifies these capabilities in practice. Our PCI-DSS certification establishes our commitment and credibility to "doing the right thing" to create an environment that exemplifies your concerns for the highest level of security posture.

Redundant Global Communication Fabric

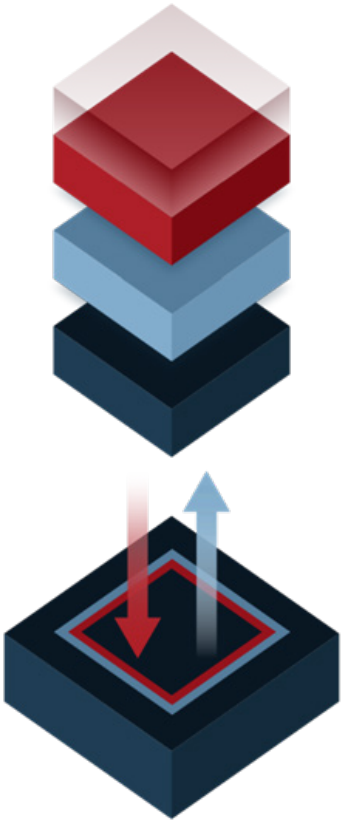


At phoenixNAP, we believe that every customer deserves the highest form of security and protection. At our most consumer level, our customers benefit from an Internet Service riding on top of a six-career blended connection, with technologies such as DDoS mitigation built into the communication fabric. Every one of our customers receives this exceptional level of protection out-of-the-box. Piggy-backing on our datacenter availability expertise, we designed a meshed switching fabric that is resilient as it is fast, eliminating single points of failure that gives us the confidence to offer a 100% Service Level Availability (SLA) guarantee.

Highly Scalable Hardware Platform

"A new platform that represents the largest Data Center Platform advancement in a decade"

- Lisa Spellman – Intel VP/GM of Xeon and Datacenter



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.

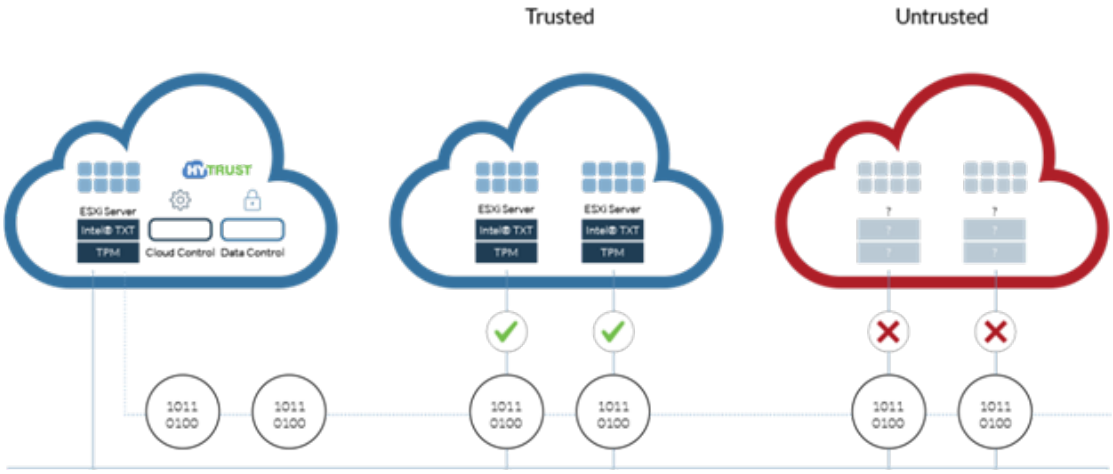
Built-in Ecosystem

- Secure, Enterprise Key Management
- Trusted connectivity
- Remote attestation for the secure platform
- Compliance and measurement at the core

Designed around the latest Intel Xeon processor technology alongside our extensive expertise in managing highly scalable workloads in our other cloud offerings, we built a computing platform that achieved 1.59X performance gains over previous generations. These increases that are passed down into our customer's workloads, providing them with better performance, and a higher density environment to optimize their existing investment, without any capital outlay; in most cases without any additional OpEx commitments.

Advanced Hypervisor Technology

We build a foundational commitment to VMware, and our commitment to integrate the latest tools and techniques to empower our customers to do what they need, whenever they need it.



Using VMware HCX (Hybrid Cloud Extension) we can help customers bridge the network gaps to hosted cloud services while maintaining network access and control. VMware's industry leading NSX network virtualization product portfolio allow for the creation of logical security policies that can be applied to a Virtual Machine regardless of location (cloud or on-prem). The integration of the latest Intel Cloud Integrity Toolkit allows for platform security with unmatched data protection and compliance capabilities.

Our VMware vRealize Suite and VMware vCloud Director integration is no different. We provide our customers with direct access to the tools they need to manage and protect their hybrid cloud environments effectively. In the event the customer wishes to engage phoenixNAP to perform some of these tasks, we offer Managed Services through our NOC and 3rd party support network.

Segmented Components

Experience has taught us how to identify and prevent repeat mistakes, even those made by strategic or competitive partners in the industry segment. One of those lessons learned is the best practice to section and separate the "Management" compute platform, from the "User compute platform." Segmentation will significantly minimize the impact of a "support system" crash, or even a heavy operational workload, from impacting the entire computing environment. By creating flexible and innovative opportunities, we train our teams to reflect, communicate and enhance their experiences, creating a knowledgeable and savvy operator who can step onto the batter's box ready to do what's asked of them.

Threat Management

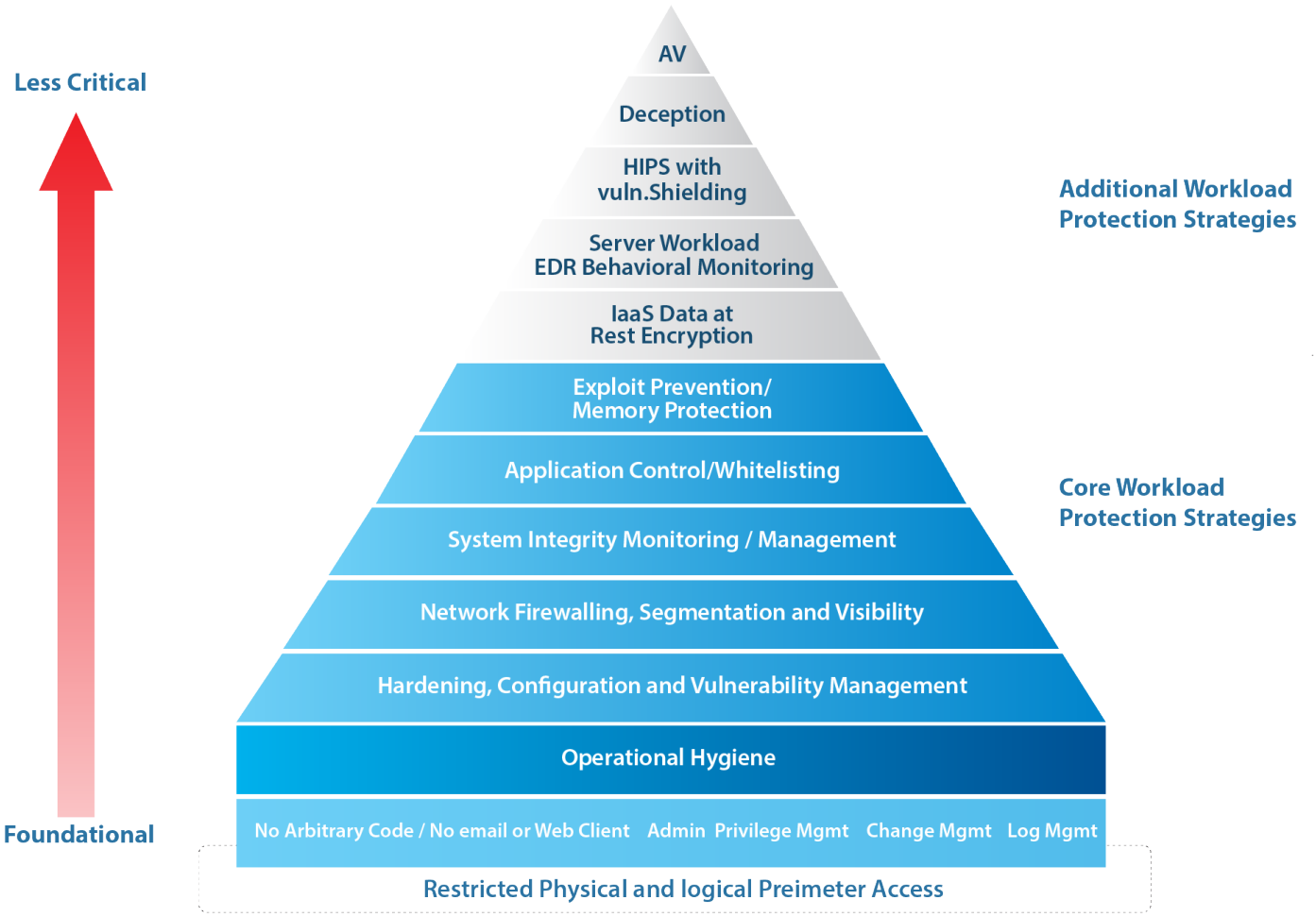
We believe that we have created a state-of-the-art infrastructure solution with world-class security and functionality. However, the solution is still dependent on a human operator. One, that based on skill or training, could be the weakest link. We, therefore, engage in continuous education, primarily through our various industry engagements and leadership efforts. This service offering is designed to be a high touch environment, using a zero-trust methodology. A customer, who is unable to deal with the elements of an incident, can see us engage on their behalf and resolve the contention.

If all else fails, and the environment is breached, we rely on 3rd party pre-contracted Incident Responders that deploy in a rapid format. The proper handling of Incident Response requires a Crisis Communication component. One or more individuals trained in handling the details of the situation, interfacing with the public and law enforcement, and based in the concepts of psychology, are trained to be sensitive and supportive to the various victim groups of the situation.

As we bundle backup and recovery as a core service in our offerings, we can make service restoration decisions based on the risk of overwriting data vs. extended downtime. Using the cloud environment to our advantage, we can isolate systems, and deploy parallel systems to restore the service, while preserving the impacted server for further forensic analysis by law enforcement.

It's All About the Layers

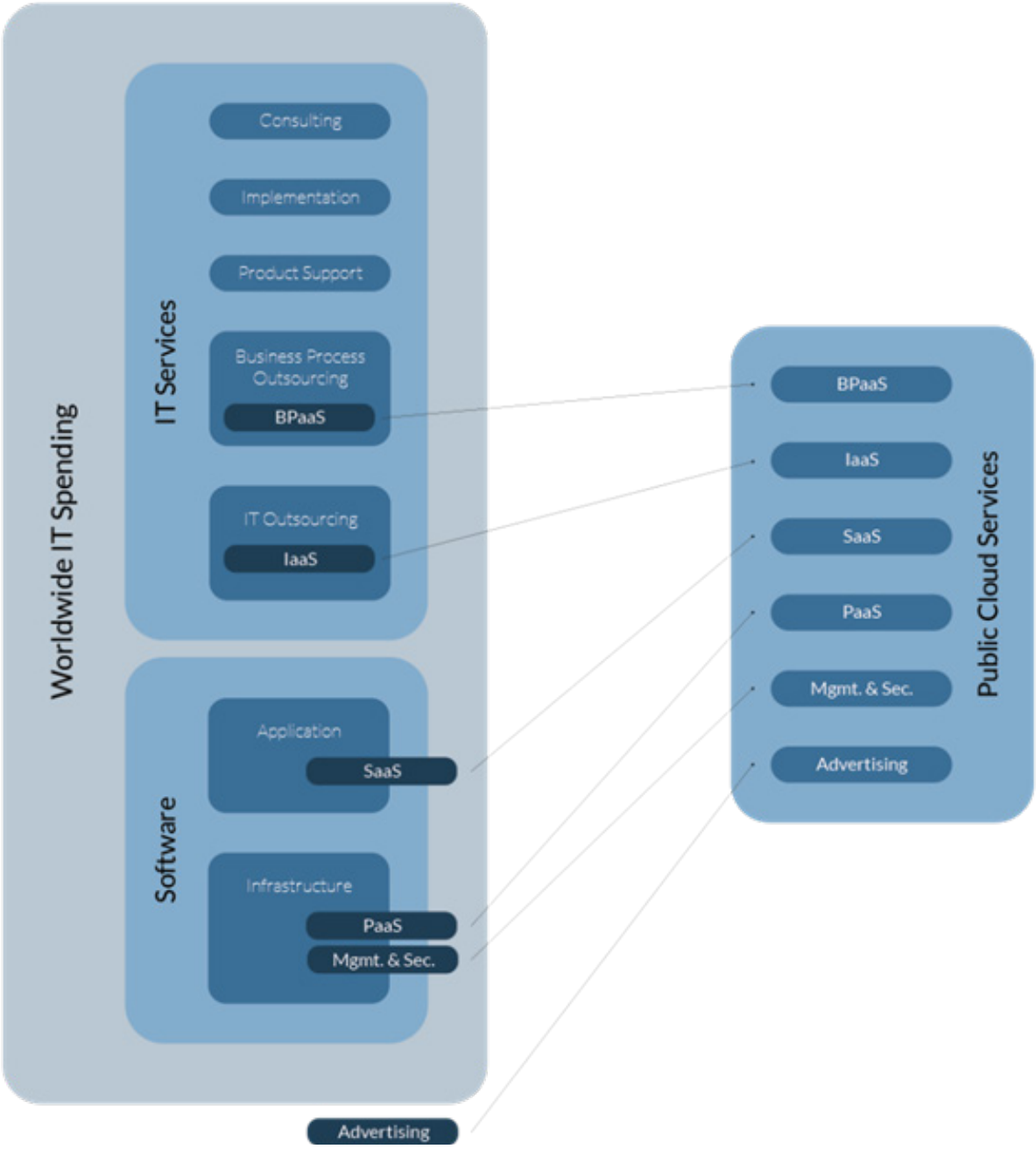
Hierarchy of Virtual Environment Security Technologies



Security solutions are designed to defend through depth. If one layer is compromised, the defense process begins by escalating the tools and techniques to the next tier. We believe that a layered approach as described creates a secure and stable solution that can easily be scaled laterally as the needs and customer base grows.

Why Does This All Matter?

In one of his articles in the CISO Playbook series, Steve Riley (2017) challenges IT leaders not to worry that migration to the cloud may require relinquishing total control but encourages them to embrace a new mindset. This mindset is focused on identity management, data protection, and workload performance.



The primary is likely a reference to the cost savings achieved from consolidation, and transfer of responsibility to a service provider.

- Converting CapEx expenditure to OpEx ones can surely improve cash flow to those in the SMB market space.
- Reducing technical overhead through the elimination of roles no longer required, can provide far more operating capital, and
- By re-focusing core-resources to concentrate on core-competencies, create business advantages in the areas that are important to the organization

Immediate ROI

See an immediate return on sales investment and ability to get to market quickly.

Expertise

Take advantage of a providers expertise in hard-to-staff skill areas.

Security

Minimize business risk that comes with securing a customers data.

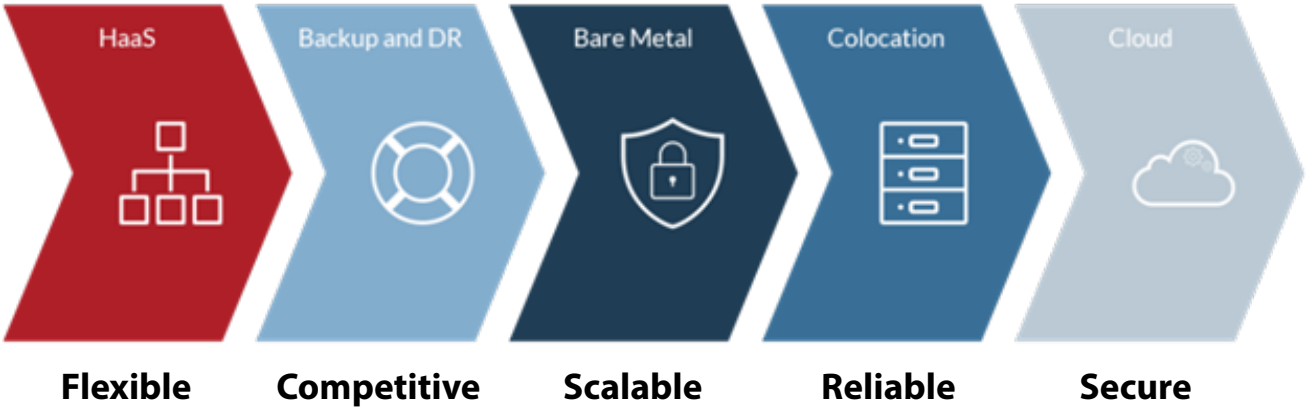
According to Gartner, Justification for cloud migration include the following (Ji, 2017):

- Shorter project times: Cloud IaaS is a strong approach for trial and error, offering the speed required to test the business model success.
- Broader geographic distribution: The global distribution of cloud IaaS enables applications to be deployed to other regions quickly.
- Agility and scalability: The resource is pay-as-you-go. If an application is designed correctly, then it is simple to scale the capability in a short period.
- Increased application availability: As described, we have demonstrated the highest levels of security and reliability. If you have the right application design, you can develop application availability accordingly.

What's Fueling the Cloud-First Strategy?

We hear many organizations adopting a cloud-first strategy, where they default to a cloud-based solution, until it proves unable, or not feasible before they consider other options. Factors driving this trend include:

- Reduced infrastructure and operational costs. From a reduction in capital expenditures, using the elasticity of cloud services, lower overall software costs and potential reduction of IT staff, organizations report approximately 14% in savings.
- Flexibility and scalability to support business agility. Agility is defined by the ability to bring new solutions to market quickly. The ability to control costs, leverage different types of services, and being flexible to adapt to market conditions.
- Cloud services tend to use the latest in innovation. Being able to leverage the high rate of innovation in this space, an organization can benefit by incorporating it as part of their business strategy.
- A cloud-first strategy can drive business growth through a supportive ecosystem.



Things to Consider

Not every workload is appropriate or destined for cloud-based compute platforms. The scoping part of any cloud migration project should start by identifying and selecting workloads that are easily migrated and implemented in multi-tenant cloud implementation.

The customer needs to understand the profile and characteristics of their workloads. For many years we would have never considered moving database workloads off of physical hardware. This is a similar case where high I/O or hardware timer reliant workloads (such as GPS or real-time event processing) may be sensitive to being in a shared, multi-tenant computer environment.

- More importantly, cloud services predominately revolve around x86-based server platforms. Therefore, workloads that are reliant on other processor architecture, or even specialized secondary processing units or even dongles, do not make ideal cloud candidates.

In contrast, cloud-based infrastructure allows for:

- Business Agility – for rapid deployment, and even rapid transition from one platform to another, with low transition costs.
- Device Choice – The flexibility to deploy, tear down, and redeploy various device configurations in a matter of clicks.
- Collaboration – Cloud providers typically provide an expert-level helpdesk, with direct access to a community of experts that can support your needs

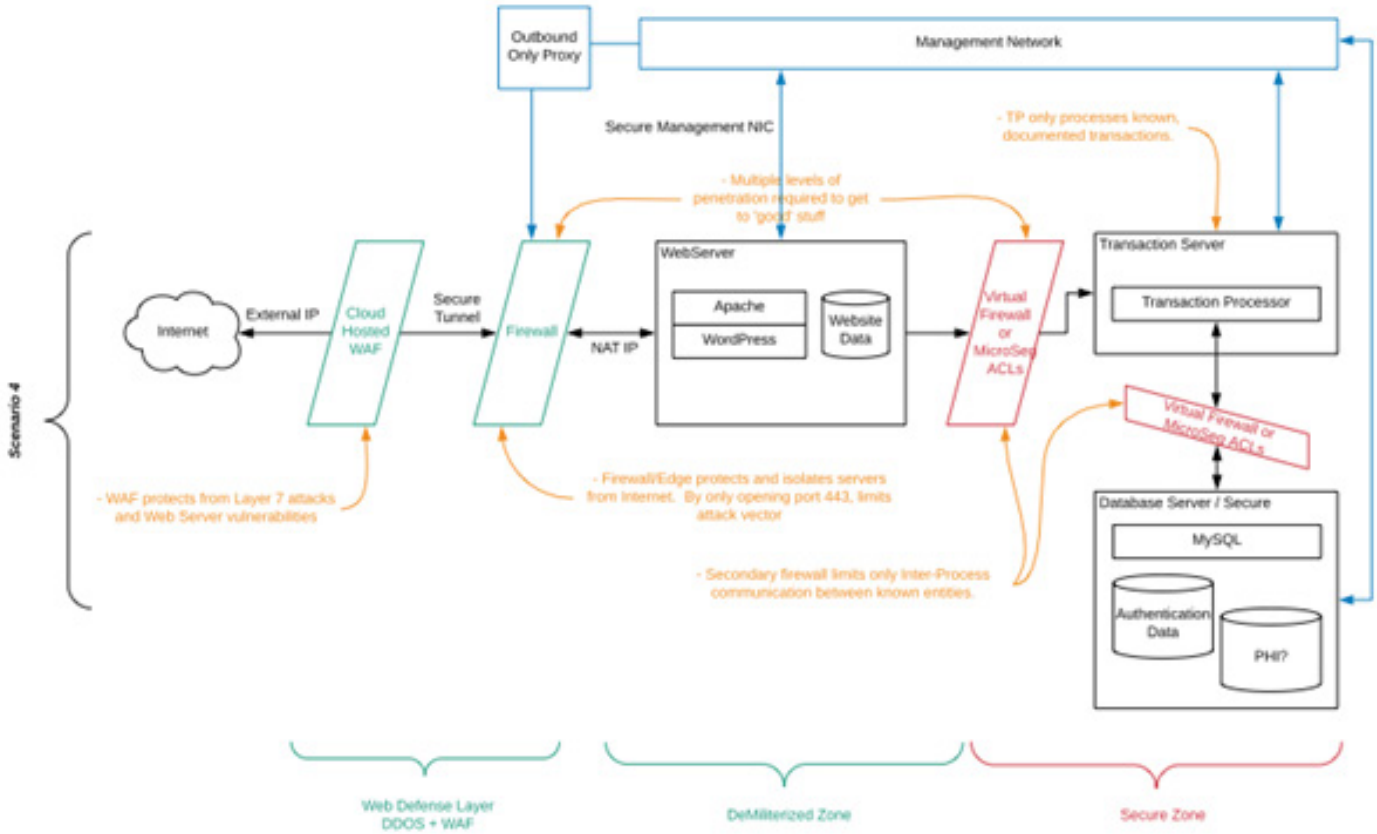
There are many reasons to consider a hybrid strategy where you combine workloads. What needs to stay on bare-metal can remain on bare metal, either in your facility or a colocation facility such as ours, while staying connected to the cloud platform via a cross-connect, gaining the benefits of both scenarios.

Cloud security consists of a broad set of concerns. It is not limited to data confidentiality alone, but concerns for privacy, regulatory compliance, continuity and recovery, and even vendor viability. Staying secure in the cloud is, however, a "shared responsibility." It requires partnerships, especially between the customer and their infrastructure service provider. Nobody needs to be convinced that data breaches are frequent, and often due to management or operator neglect. Customers are becoming tired of their data being disclosed and then used against them. Most recently, abused via an email-based threat vector, where the bad actor quotes a breached user ID and password, as a way to convince the target recipient to perform an undesired action, behind the mask of perceived authenticity.

Any organization that accepts Personally Identifiable Information (PII) of its customer base establishes with that customer, an implied social contract to protect that information. At phoenixNAP, we have demonstrated leadership in the infrastructure space on a global scale, through partnerships with customers, solution aggregators, and resellers. We have created innovative solutions to meet the unique challenges faced by businesses, going above and beyond to achieve the goals desired by the target organization.

Use of Reference Architectures

One of the benefits of a cloud-based, secure infrastructure such as our Data Security Cloud, is the ability to implement battle tested reference architectures that in some cases go above and beyond the standard capabilities of what's possible in the physical environment.



In what we would consider an extreme case; an architecture as depicted above creates multiple layers of security with various gateways to get to the prized databases that most bad actors are after. Let's not ignore the bad actors that want to take control of the web infrastructure to infect visitors with infectious payloads; however, the real prize sits inside those databases in the form of PII, PHI, or PCI data. While the various levels of defensive components are designed to make it difficult for the bad actors to storm the castle, the 24×7 Threat Monitoring will undoubtedly catch the multiple attempts and anomalous behavior, triggering an investigation and response activity. Through a robust combination of tools, technology, services, and a cost model that's supportive of the needs of the SMB space, we believe we have demonstrated our leadership, but more importantly, we have created a solution that will benefit you; our SMB customer.
We aim to have created a complete security solution that you can take forward as you further define your cloud strategy.

Our Promise

We have assembled a world-class team of highly experienced and skilled leaders, who are passionate about cloud security. As global thought leaders, we design for the world and implement locally. We create sustainable solutions, understanding a customer's appetite and limited budget. Let us show you how we can benefit your goals through our solutions offerings. Keeping with our promise to "do the right thing" as it involves finding the best solution for you.

Notes from the Authors: Elements of a Strong Security Strategy

Over the years, we have learned many important lessons when it comes to creating solutions that are secure and reliable. Here are some final thoughts to ponder.

- There is no substitute for strong architecture. Get it right and you have a stable foundation to build upon. Get it wrong and you will play whack-a-mole for the rest of that life-cycle.
- Have detailed documentation. Implement policies and procedures that make sense. Documentation that supports the business process. Security policy cannot burden the users. If it does, it just becomes a target for shadow IT. It needs to be supportive of the existing process while implementing the control it absolutely needs. A little control is better than no control due to a workaround.
- Plan for a breach, plan to be down, plan for an alien invasion. If you plan for it, you won't be caught in a state of panic when something undoubtedly happens. The more off-the-beaten-path a scenario seems, the better you can adopt for when real-life scenarios arise.
- You can't protect what you don't know you have. Asset management is the best thing you can do for your security posture. If it's meant to be there: document it. If it's not meant to be there: make certain that you have a mechanism to detect and isolate it. Even to find out who put it there, why and when.
- Now that you know what you have: monitor it. Get to know what normal behavior is. Get to know its "baseline."
- Use that baseline as a comparative gauge to detect anomalies. Is this system showing inconsistent behavior?
- Investigate. Have the capability to see the alert triggered by that inconsistent behavior. Are you a 24/7 operation? Can you afford to ignore that indicator until the morning? Will your stakeholders, including your customers accept your ability to detect and respond to the Service Level Agreement (SLA) you extend to them? Can you support the resourcing needed for a 24/7 operation, or do you need to outsource the Threat Management component at least in a coverage extension model? The greatest SIEM and monitoring tools are useless without someone actioning the alerts as soon as they pop up. Machine learning helps, however, it cannot yet replace the operator.
- Mitigate the problem or be able to recover the environment. Understand what your Recovery Point Objectives (RPOs) and your Recovery Time Objectives (RTO). Do your current solutions meet those goals? Can those same goals be met if you have to recover into a facility across the country, with no availability from your current staff due to the crisis being faced? How will you communicate with your customers? Do you have a crisis communicator and incident handler as part of the response team?
- Take your lessons learned, improve the process and do it all over again.

No single vendor can provide you with a "silver bullet." Any vendor that tells you so, is someone you should shy away from. Every customer's needs are unique. Each situation takes a unique blend of solutions to be effective. Hence your vast network of partner relationships, to provide you with the solutions you need, without trying to make you fit onto one of their offerings.
The offer is always on the table. At phoenixNAP, we will gladly take the call to discuss your concerns in this area, and provide advice on what our thoughts are on the topic of interest. Promoting and supporting properly secured environments is part of our social responsibility. It is part of our DNA and the core philosophy for building products in this segment. Let us be your partner in this journey.

GLOBALLY CONNECTED.
LOCALLY AVAILABLE.

2.35 Tbps Bandwidth Capacity | 20,000+ Servers Available Worldwide

100% Network Uptime with World-Class Carrier Blend