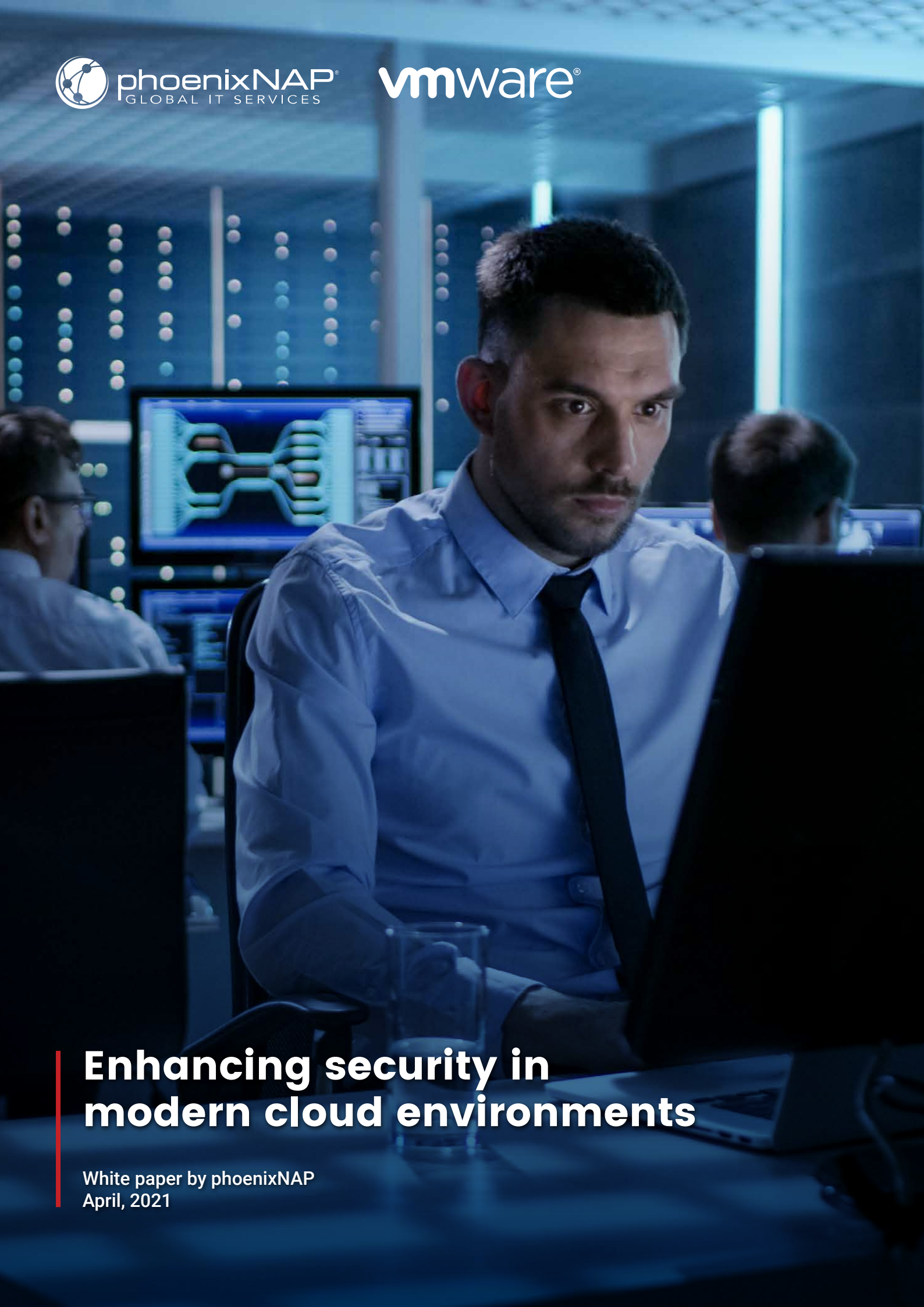


Enhancing security in modern cloud environments

White paper by phoenixNAP
April, 2021

I – INTRODUCTION: The Rising Challenge of Cybersecurity

Cloud computing is the future of business IT. Its adoption has been steadily growing for years, and the COVID-19 pandemic further validated its role in accelerating digital transformation. Synergy Research Group reports that all three major cloud models – SaaS, IaaS, and PaaS – grew substantially during Q3 of 2020[1]. According to Gartner[2], the proportion of IT spending that is shifting to the cloud will further accelerate in the aftermath of the COVID-19 crisis. The cloud is projected to make up 14.2 percent of the total global enterprise IT spending market in 2024, up from 9.1 percent in 2020.

However, as cloud adoption continues to grow, so does the concern about its security. Cloud security risks have evolved rapidly in recent years and new, more advanced threats are emerging at an alarming pace.

Research from McAffee[3] shows that 83 percent of organizations store sensitive information in the cloud, and that one in four companies using public cloud services has experienced data theft by a malicious actor. An additional one in five has experienced an advanced attack against their public cloud infrastructure.

93% of information security professionals are moderately to extremely concerned about cloud security.

With most modern organizations using cloud services today, security remains a top concern. A 2019 survey by Synopsis[4] that included 400,000 information security professionals revealed that 93 percent are moderately to extremely concerned about cloud security. The biggest concern is data loss and leakage (64 percent), followed by data privacy/confidentiality (62 percent), legal and regulatory compliance (39 percent), accidental exposure of credentials (39 percent), data sovereignty (35 percent), and incident response (29 percent).

Considering these risks, developing a cloud security strategy and implementing modern, reliable, and secure solutions to protect company workloads is one of the top business priorities. Recognizing the challenges in achieving that, this white paper provides guidelines and best practices for ensuring data security by leveraging phoenixNAP's Data Security Cloud platform.

---

[1] **Synergy Research Group, COVID-19 Boosts Cloud Service Spending by $1.5 Billion in the Third Quarter**

[2] **Gartner, Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021**

[3] **McAffee, What is Cloud Security?**

[4] **Synopsys, 2019 Cloud Security Report**

Businesses looking to enhance their infrastructure security will learn:

- What the best practices in cloud infrastructure security are.
- What features to consider when choosing a cloud provider.
- 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 organizations protect their security-sensitive workloads.

II - Vital Steps in Building a Rock-Solid Infrastructure

As organizations accelerate their digital transformation efforts by moving their workloads from an on-premises to a cloud environment, they need a modern security solution that protects business-critical data against emerging security threats. Companies that are reluctant to implement an adequate cloud protection strategy leave their infrastructure unprotected and vulnerable, facing many risks.

The most common cyber risks include:

By implementing a comprehensive cybersecurity strategy and multi-layered data protection, businesses can eliminate these risks and ensure business continuity in case of an attack or disaster. Recommended best practices for infrastructure protection are outlined below.

1. Create a Data Governance Network

To reduce cybersecurity risks, companies are implementing data governance networks—systems that define authority and control over sensitive data assets. These systems include employees, procedures, and technology solutions to determine decision rights and accountabilities for information-related processes. Once implemented, the data governance framework provides a streamlined approach to managing, utilizing, and protecting sensitive data.

2. Double-Check Cloud Configurations

Misconfigurations of cloud security settings are the leading cause of cloud data breaches. Cloud strategies that organizations rely on to improve their security posture are often inadequate or insufficient to successfully protect their cloud-based infrastructure.

Cloud security should not be a provider-only concern. It is an aspect of the shared responsibility model that is partly in the organization's hands. Businesses should pay special attention to cloud configuration as extra measures could significantly reduce the chances of their data being publicly exposed. Measures that businesses can take to improve security posture include:

1. Restricting access to least privilege
2. Disabling cloud resources your teams don't use
3. Encrypting data stored in the cloud by volume or tag
4. Blocking inadvertent uploads or cross-region copies
5. Enforcing data security governance policies
6. Preventing access to privileged accounts when MFA is disabled
7. Ensuring encryption keys are rotated and stored safely

3. Utilize Data Loss Prevention Software (DLP)

To ensure that a business's sensitive data is not stolen, misused, lost, or accessed by unauthorized users, companies deploy a set of tools and procedures known as data loss prevention (DLP). DLP software protects an organization's confidential and business-critical data by carefully classifying it and identifying policy violations. If a DLP software identifies a violation, it performs preventive actions to make sure that confidential data is protected. Data loss prevention solves three common business challenges:

1. Protecting personal information (compliance)
2. Protecting intellectual property against exfiltration
3. Data visibility and tracking data movement across endpoints, networks, and cloud

4. Implement a Reliable Backup Solution

No one is immune to cyber-attacks. With hacking attempts becoming increasingly sophisticated, even the most secure cloud infrastructures are at risk of being breached. A vital part of a cloud

security strategy is a reliable backup solution that allows businesses to quickly recover their data, restore business operations, and avoid downtime and other destructive consequences of a disruptive event.

5. Use Two-Factor Authentication (2FA)

A simple yet very efficient step in enhancing infrastructure security and improving an organization's cybersecurity posture is enabling two-factor authentication (2FA). Coupled with role-based access control (RBAC), which is essential in hybrid environments where multiple people have access to the infrastructure, multi-factor authentication is an integral part of identity access management. Both RBAC and 2FA add an extra layer of protection to the classic username-password combination, ensuring greater control of access to critical systems. 2FA is usually implemented as:

1. Fingerprint authentication
2. Email address or SMS code confirmation
3. Security question

6. Conduct a Detailed Cloud Security Assessment

The continually changing cloud environment makes it very difficult to detect and respond to threats rapidly. The most efficient solution to identifying and mitigating cloud computing security risks and improving systems safety is performing an exhaustive cloud security audit that gives a clear picture of security capabilities.

III - Key Considerations When Choosing a Cloud Provider

The cloud can benefit businesses of all sizes and in all industries. However, migrating entire operations to the cloud is a decision that must be thoroughly researched and analyzed. There are five critical factors businesses must consider before choosing a cloud provider.

SCALABILITY

Scalability is one of the main forces driving increased cloud adoption. Scalability in cloud computing means that an organization can quickly increase or decrease required IT resources to meet changing needs. If demand for IT resources grows, organizations can rapidly scale up while ensuring maximum performance.

SECURITY

Cloud providers use multiple applications, procedures, and technology solutions to bulletproof their infrastructure against internal and external cybersecurity threats. For businesses that are moving their mission-critical workloads to the cloud, reliable cloud infrastructure is vital. Trustworthy cloud security policies should be clearly outlined in an SLA to ensure the provider is able to protect access to your data and that your workloads are safely stored.

COMPLIANCE

Meeting compliance standards is extremely important for businesses operating in heavily regulated industries like healthcare or finance. Compliance requirements are industry-specific and ensure protection of sensitive data (e.g., GDPR, PSI DSS, HIPAA). For organizations operating in these industries, it is essential to choose a compliance-ready cloud infrastructure provider. It is vital to understand the compliance requirements, each party's compliance responsibilities, and the compliance aspects that a cloud provider covers.

COSTS

Apart from scalability, virtualization is all about cost-optimization and right-sizing infrastructure to eliminate unnecessary spending on IT resources. Cloud environments include pay-per-use billing options to help businesses reduce their capital expenditures. 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. This also eliminates the need to suffer through extensive maintenance windows or service outages.

AVAILABILITY / UPTIME

As businesses move toward 24/7/365 operations, ensuring data availability and preventing costly downtime become their absolute priority. Modern businesses need fast and highly available resources to maintain business operability. Cloud computing offers companies the ability to avoid or minimize spending while leveraging the flexible nature of the cloud infrastructure to meet growing business needs. You should choose a cloud provider that offers high uptime to ensure the highest possible levels of business continuity.

IV - High-Performance Cloud Infrastructure – Unparalleled Security

phoenixNAP's Data Security Cloud is designed to address common infrastructure security concerns by providing a 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 advanced built-in security components. Powered by the latest generation of hardware and advanced hypervisor technologies, Data Security 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 businesses in various sectors peace of mind in delivering redundant and security-centric apps to their customers.

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

Data Security Cloud Architecture Overview

Data Security Cloud was built using strict virtualization and segmentation controls, leveraging advanced hypervisor technologies. The modern networking fabric allows for the creation of logical security policies that can be applied to a virtual machine regardless of location (cloud or on-premises). The micro-segmentation capability of VMware NSX hypervisor helps isolate virtual machines, ensure zero-trust security between virtual machines, and contain a potential impact of a cyber-attack.

Data Security Cloud's flexibility and deployment simplicity makes it easy for organizations to create hybrid cloud solutions between their on-premises and Data Security Cloud implementations. The platform is also supplemented by a 24/7 security operations center (SOC) that takes immediate action to mitigate cyber threats before they make an impact.

Directly integrated into Data Security Cloud, threat intelligence provides organizations with continuously 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 businesses to keep their customers' data protected at all times. Data Security Cloud is integrated with an industry-leading backup solution that mitigates potential damage and ensures operability and availability even in case of a disaster. This ensures that organizations can restore a fresh copy of their workloads and quickly recover from a potential ransomware attack or other types of cyber-attacks.

Physical Security

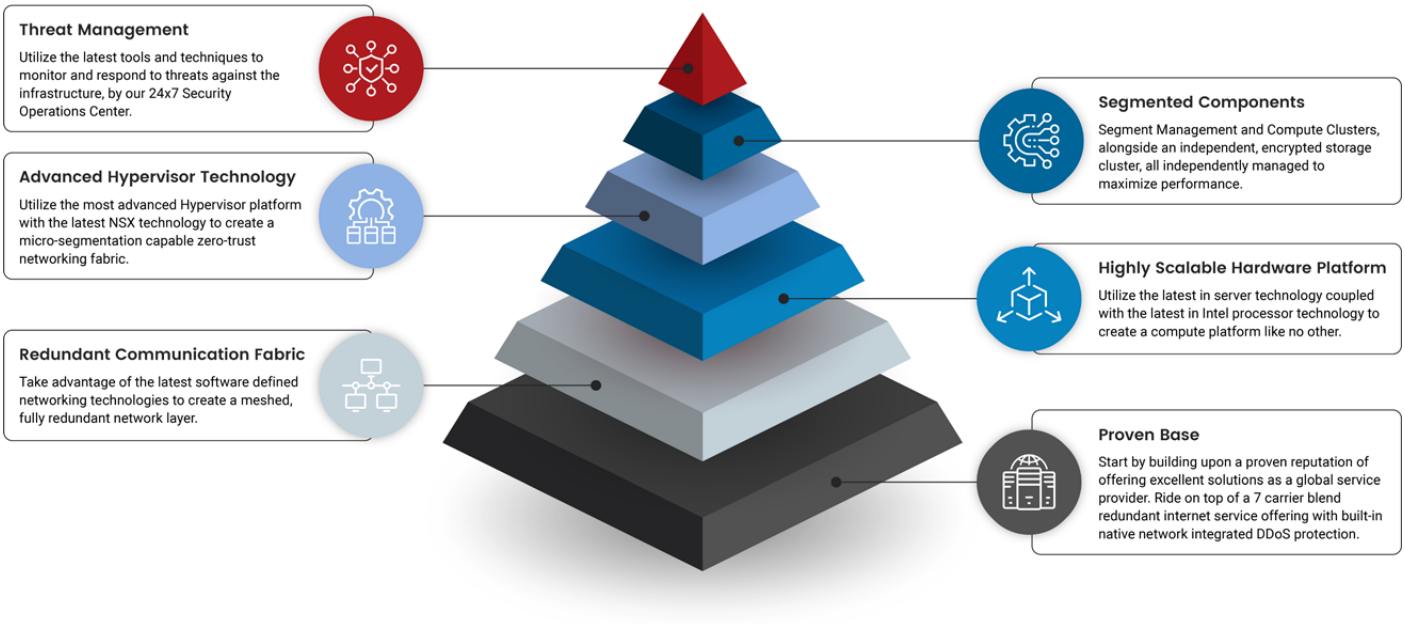
The phoenixNAP data centers that house the Data Security Cloud infrastructure are SOC-1, SOC-2, and SOC-3 audited. These certifications establish a baseline for physical and logical access control, data security, and business continuity procedures. On top of that, PCI-DSS certification allows financial and legal businesses to process sensitive payment data without worrying about compliance.

Advanced Performance

Along with advanced security, Data Security Cloud enables modern businesses to deliver fast, responsive, and high-performance services across the globe. This is thanks to the latest generation of processor technologies that power the infrastructure at its core. Businesses can rely on stable performance even under peak load, which directly translates to greater customer satisfaction. As the number of customers increases and the need for computing power grows, organizations 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.

Layer After Layer of Protection

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 layer. In building this type of infrastructure, phoenixNAP was guided by the notion that a layered approach creates a secure and stable solution that can easily be scaled laterally as needs and customer bases grow.



Secure at the Foundation

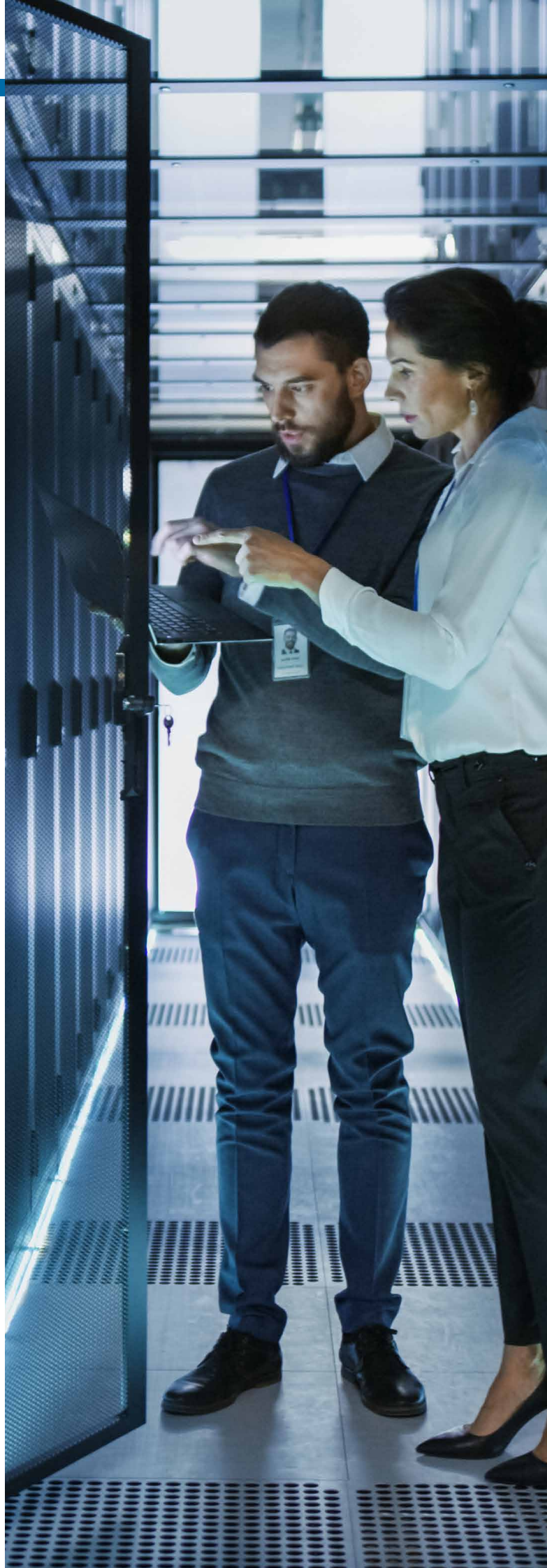
- Root of trust module (TPM)
- Built-in instruction sets for verification (Intel TXT)
- Fast, high-quality random number generator (RDSEED)
- Firmware assurance (BIOS Guard)

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

Integrated Backups – Ensuring Your Workloads Are Safe and Sound

phoenixNAP's Data Security Cloud environment includes backups up to 100% of storage. This means that copies of stored workloads and data are automatically created straight in the cloud, enabling businesses to quickly recover their operations in case of debilitating events like cyber breaches, natural disasters or accidental deletion.



Addressing Security Risks with VMware NSX

Providing micro-segmentation and virtualized firewalls, VMware NSX helps reduce operational costs, improve network performance, and secure East-West (lateral) traffic within the data center.

Addressing today's risks with VMware NSX	
Storing data within a VM in a hybrid cloud environment	• NSX is an important element in locking down your virtualized environment, regardless of where VMs run. • NSX can quickly identify and isolate problems before they spread.
Increasing attack surface with growing end points (mobility)	• NSX policies follow loads no matter where they reside and control access to images and production VMs. • Lateral traffic is continually monitored to prevent unauthorized access from any user, any device.
Missing internal security expertise	• Create security profiles that can be attached automatically to workloads as well as classifications of users.
Lack of insight into VM activity	• VMware vRealize Network Insight and NSX can quickly identify and isolate problems.

V - CONCLUSION

Cloud adoption is growing significantly as businesses of all sizes realize and embrace its benefits. At the same time, cybersecurity challenges significantly inhibit adoption, hampering businesses' digital transformation strategies. The lack of skills and budget to manage cloud security implementation and policies prevent many organizations from leveraging its full potential.

phoenixNAP's Data Security Cloud is an ideal solution for companies that have high security requirements but limited budget, IT resources, or staff. It gives them complete control over their environments, along with intelligent threat detection and offsite 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.

About phoenixNAP

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

Contact phoenixNAP at: **sales@phoenixnap.com**
or **855.330.1508 | www.phoenixnap.com**