phoenixNAP GLOBAL IT SERVICES

vmware

CLOUD SECURITY SURVEY 2023:

Infrastructure Protection Best Practices

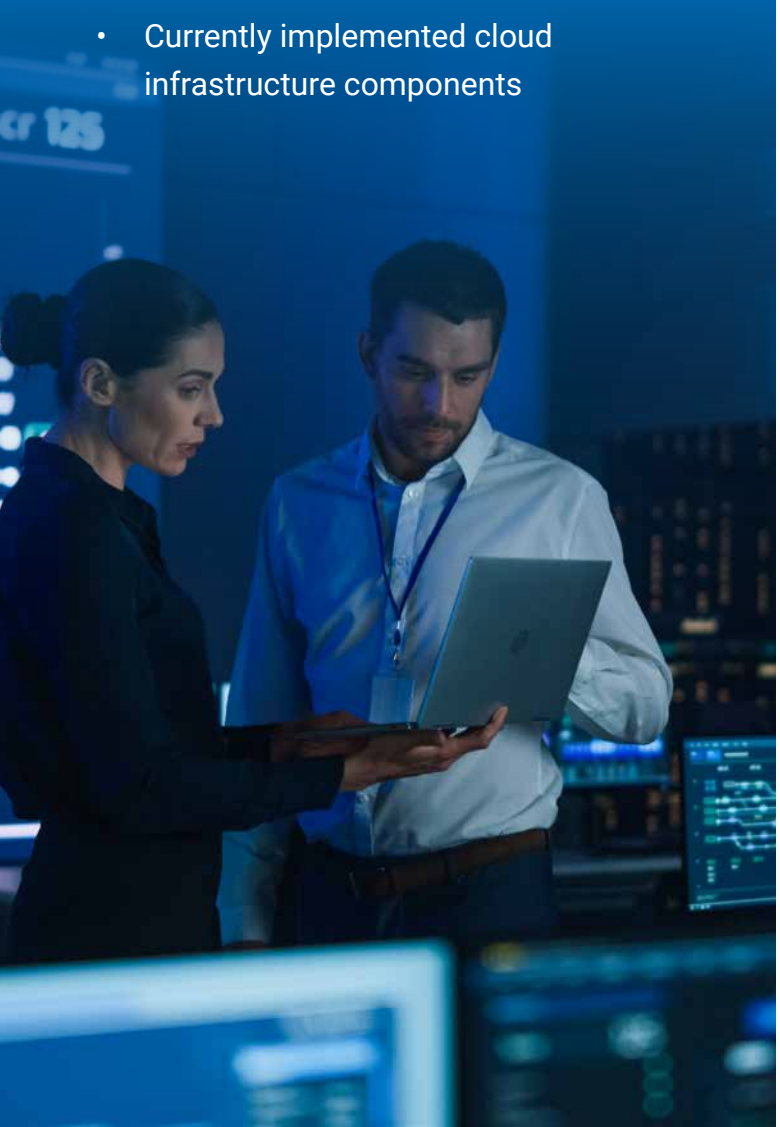
White paper by phoenixNAP
September, 2022

Survey Summary:

We surveyed 289 security and IT administrators, architects, and decision makers from SMBs and enterprises operating in more than 19 verticals including FinTech, SLED, Healthcare, High Tech, manufacturing, and services.

Topics:

- Cloud security concerns
- Data loss/breach experiences
- Confidence in current security posture
- Cloud security challenges
- Currently implemented cloud infrastructure components



INTRODUCTION

In the post-pandemic world, we spread data everywhere. As remote and hybrid workforce models become the norm, multi-cloud deployments evolve into the de facto computing standard for distributed workloads. This expands the attack surface well beyond the walls of a traditional data center and overextends already understaffed security teams. As a result, organizations struggle to combat the growing number of insider and outsider threats targeting their invaluable digital assets.

To better understand current cloud security challenges, phoenixNAP and VMware conducted a global survey involving close to 300 respondents.

According to our latest findings, **85%** of IT system administrators and decision-makers **are moderately or extremely concerned about the security of their organization's data.**

We asked IT decision makers about their data loss experiences, their organization's security posture, and the challenges they face while implementing infrastructure security components.

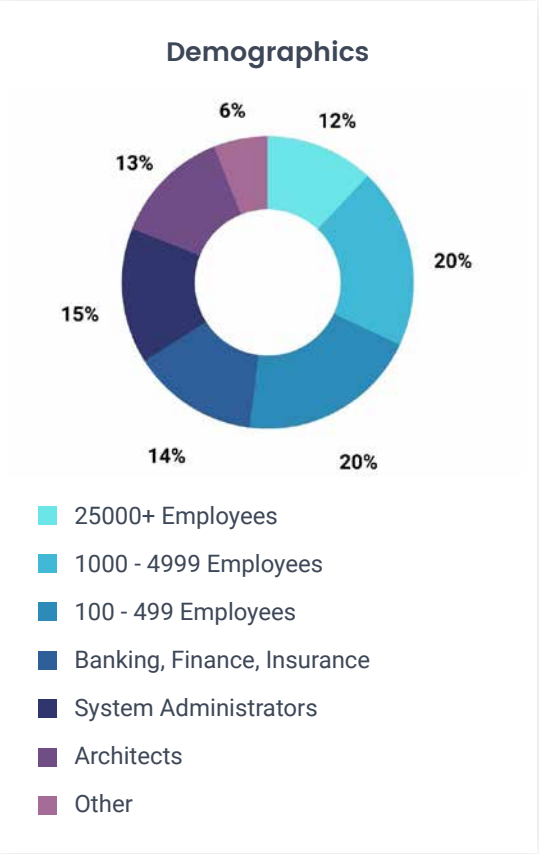
This white paper presents our latest findings on cloud security and asset protection. It also gives an overview of emerging cybersecurity trends and recommends best practices for ensuring cyber resilience and advanced data protection in modern IT environments.

I - Survey Methodology and Demographics

This survey was distributed by VMware User Group (VMUG) to their user base between July and September 2022. The responses were analyzed by the phoenixNAP team and key findings are presented in this document.

Regarding the survey's respondents, there was an almost equal number of people who work in large organizations and those employed in small to medium businesses. Most were system, network, or virtualization administrators, software architects, and managers.

The results of this survey confirmed our views on the state of security in modern environments and gave us a deep understanding of the challenges organizations face on their road to cloud adoption.

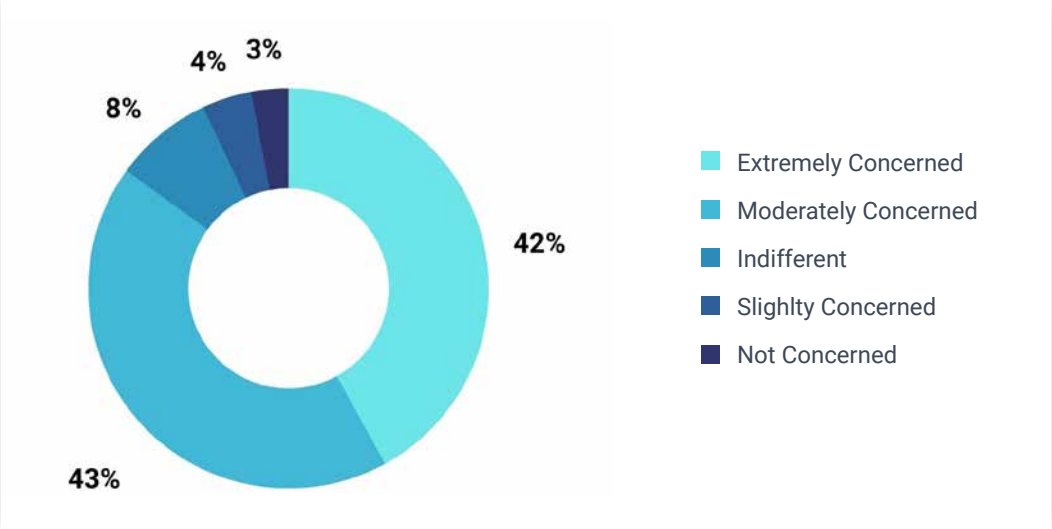


Key Findings: No Respite for Organizations and IT Security Teams

Today's typical enterprise is heterogeneous. Modern workloads consist of anything from legacy on-prem software to microservice-based applications and run across public and private clouds. Such complex hybrid environments make detecting and preventing breaches more difficult than ever. To make matters worse, the distributed workforce and clients demand constant and optimized access to vital services from any location and platform. All these factors take their toll on an organization's security.

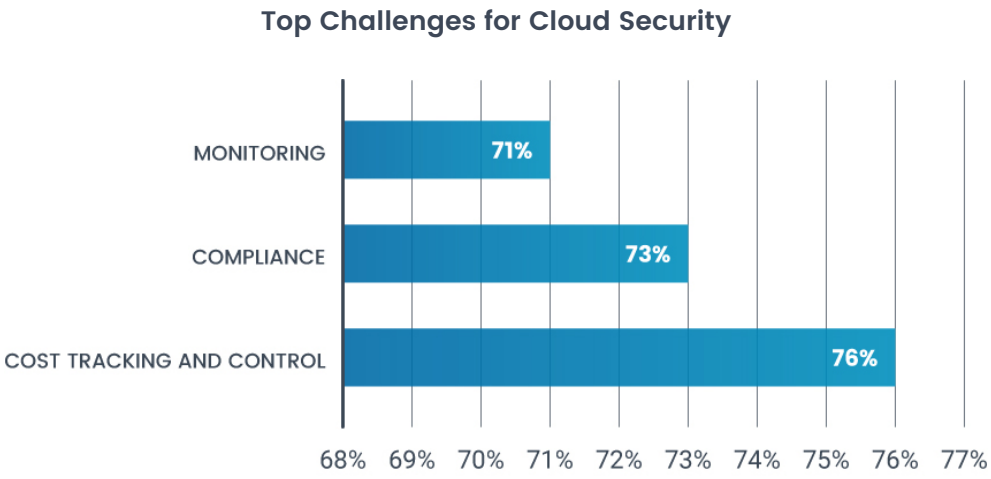
Only 19% of respondents felt extremely confident their organization's cloud assets were sufficiently protected. The rest were not so optimistic:

In fact, **42% of respondents were greatly concerned about the security of their organization's cloud data:**



Finally, our survey showed that **23% of organizations suffered a data loss due to a breach, disaster, or human error** in 2021 and 2022. What we can learn from this data is that disasters and breaches can happen anytime to any organization, causing stress and concern that can negatively affect its productivity.

When it comes to security challenges, organizations are faced with skills shortages, lack of advanced tools, and complexity of management and monitoring. The following three were identified as the top 3 cloud security challenges:



In addition, **70% of respondents found cloud waste optimization to be a major hurdle**, while **68% reported a lack of IT staff** as one of the critical concerns in cybersecurity management.

With breaches and outages being more a matter of "when" than "if", no organization is safe. Only with

proactive, multi-layered infrastructure protection and optimal incident response can organizations stay safe from the consequences of data loss and compliance violations.

III – Best Practices for Protecting Your Infrastructure

1. Take a Holistic Approach

Protecting your digital assets requires looking at the big picture and addressing all levels of cloud infrastructure:

Physical

Your data center, servers, security staff, and physical access controls.

Network

Your first line of defense against intruders.

Application

Your software development practices, pipelines, and protocols

Data

Your invaluable, business-critical digital assets

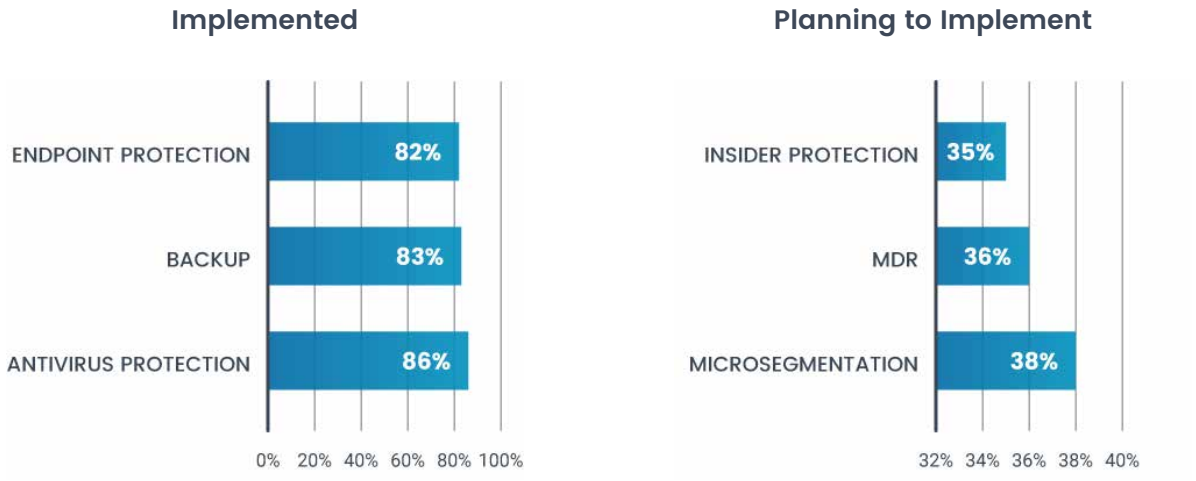
People

Your staff and customers, often the most difficult layer to manage

2. Ensure Multi-layered Security

According to our survey, most organizations currently implement endpoint, backup, and antivirus protection into their infrastructure security. However, while some plan to introduce additional layers such as micro-segmentation, managed detection and response (MDR), and insider protection, most do not have them in place. Currently, only 37% of organizations use micro-segmentation, and the same number of organizations deploy DRaaS. 41% use insider protection, while MDR is used by 45% of organizations.

Protecting your infrastructure requires optimally stacking layers upon layers of physical and virtual security.



2.1 Protect the Physical

Physical protection is as important as virtual, and your data deserves nothing less than a top-tier data center service, including:

- 24/7 on-site security personnel
- Perimeter security with video surveillance
- Biometric and multi-factor authentication barring entrance to secure areas
- Access to enterprise-grade server hardware supporting the latest security technologies
- Disaster-free location
- Redundant cooling, power, and network

Hosting your servers in a secure facility helps prevent physical threats such as malicious intent, theft, or accidental damage, all of which can have a devastating effect on your business.

2.2 Secure the Network

Your network needs to be designed with cyber resilience and attack prevention in mind. Best practices include the use of:

- Enterprise-grade hardware
- Advanced, custom firewall configuration
- Intrusion detection and prevention systems (IDPS)
- Threat Management and Response Systems (MRS)
- Endpoint Protection
- Log Management

Zero-day threats and weaknesses keep getting discovered and network security needs to stay one step ahead and continually improve. Just as your servers need to be constantly monitored for file integrity, access control, and security patches or updates, your network also requires constant vulnerability and penetration testing and monitoring.

Mobile devices your teams use should also be strictly protocolled and monitored since they are frequently used to access corporate systems and sensitive information both inside and outside the organization's network.

2.3 Trust No One

Threats were traditionally viewed as coming from the outside. Staff, devices, or applications inside the perimeter tend to be granted excessive access and permissions by default. As a result, modern threats such as insider or account takeover attacks manage to get inside the network undetected. That is why implementing a **Zero-trust security strategy** is one of the most important steps in building a secure cloud infrastructure.

This broad approach to security rightfully assumes that any digital transaction is potentially dangerous. As such, it focuses on threat hunting and incident response, offering all-around visibility in case of a suspected breach.

Additionally, it offers robust identity, access, and attribute management for every interaction on both the user-resource and resource-resource level. By limiting permissions and granting access only to resources necessary for a specific use case, you minimize the impact a successful breach can have on your organization.

2.4 Perform Network Segmentation

While malicious actors rarely gain immediate access to their targeted resources, they commonly enter your network via phishing or social engineering attacks and then move laterally through the system. In fact, VMware's *Global Incident Response Threat Report* for 2022 states that **25% of all attacks involve lateral movement**.

Leveraging network virtualization and security platforms such as **VMware's NSX®**, you can segment your entire network from a single pane of glass.

This hypervisor lets you create multiple virtual networks with specific requirements or enable any network topology in a matter of seconds. By doing so, you can isolate virtual machines, ensure zero-trust security between them, and contain a potential cyber-attack.

The platform's micro-segmentation features include:

- Dynamic creation of security groups and policies beyond IPs, ports, and protocols
- Policy attributes, including:
  - Layer 7 (application-level) user information
  - Machine name and tags
  - OS types
- Active Directory-based policies
- Security all the way down to the user level of a single remote or virtual desktop session

Infrastructure Security Challenges VMware NSX Solves:	
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 endpoints (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 and device.
Lack of in-house security talent	• 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.

2.5 Build Applications with Security in Mind

While plenty of monolithic applications are still running on-prem, organizations increasingly embrace cloud-native software development principles and break apps into microservices. Even though this approach accelerates deployment and increases reliability and portability, it often focuses on frequent releases and rarely addresses security beyond the software testing phase.

That is why implementing DevSecOps into your organization's DevOps culture is vital. This approach helps you simplify vulnerability detection and management and improve the overall security of your workloads, applications, and services. DevSecOps tools can enable threat intelligence and updated vulnerability patches, securing the application throughout its lifecycle.

DevSecOps is the practice of integrating security into software development processes. To learn more about it, read phoenixNAP's **What is DevSecOps** Knowledge Base article!

Other security practices that should be implemented at the application level are:

- Data encryption at rest and in transit
- Multi-factor authentication (MFA)
- Log Management
- Vulnerability testing
- Code reviews

Coding with security in mind prevents the appearance of code flaws and fortifies the application against possibly devastating zero-day exploits.

2.6 Secure the Entire Data Lifecycle

Data is most vulnerable while being transferred or shared between services, data centers, and providers. Protecting it while in transit is vital, but this does not mean it is completely safe inside the walls of the data center. On the contrary, malicious actors can access it as soon as they penetrate the previous security layers of your infrastructure.

One of the most important steps is to **encrypt data at rest and in transit**. Even when data is stolen, strong encryption makes it useless to anyone without the encryption key.

Another crucial step in protecting data is implementing **continuous cloud-based backups**. By copying or replicating your business-critical data or even entire VMs on a cloud server at a remote location, you can easily restore your assets even when your system has been compromised. Modern third-party cloud backup solutions often support advanced features such as **insider protection and immutability**, helping you add yet another layer of protection to your critical assets.

A sound data security plan also needs to include **organization-wide data retention, archival, and destruction policies**, especially in organizations following strict compliance or regulatory procedures.

2.7 Never Underestimate the Human Factor

According to Verizon's 2022 Data Breaches Investigations Report, **82% of breaches involve the human element,** including social attacks, errors, and misuse. This fact places a level of urgency on implementing Zero-trust policies but also highlights the necessity of including cybersecurity awareness training into your defense strategy. Employees need to be regularly updated on possible security threats and taught how to recognize them and react adequately. Apart from awareness, the following practices can help you keep human errors to a minimum:

Policies and procedures – Clearly defined and documented guidelines on who can access sensitive data and when, how it can be handled, and the consequences of not following policies.

Passwords and Multi-factor Authentication – Users need to learn how to create passwords that are difficult to breach. These should be combined with other authorization factors such as security questions, fingerprints, or SMS confirmation codes to further protect their accounts.

Bring Your Own Device (BYOD) Policies – As more and more workers opt for remote or hybrid work models, personal laptops, smartphones, and tablets are used to access the applications and data needed for performing daily tasks. Since these endpoint devices can be stolen or compromised, it is vital to create device access policies and systems that protect them.

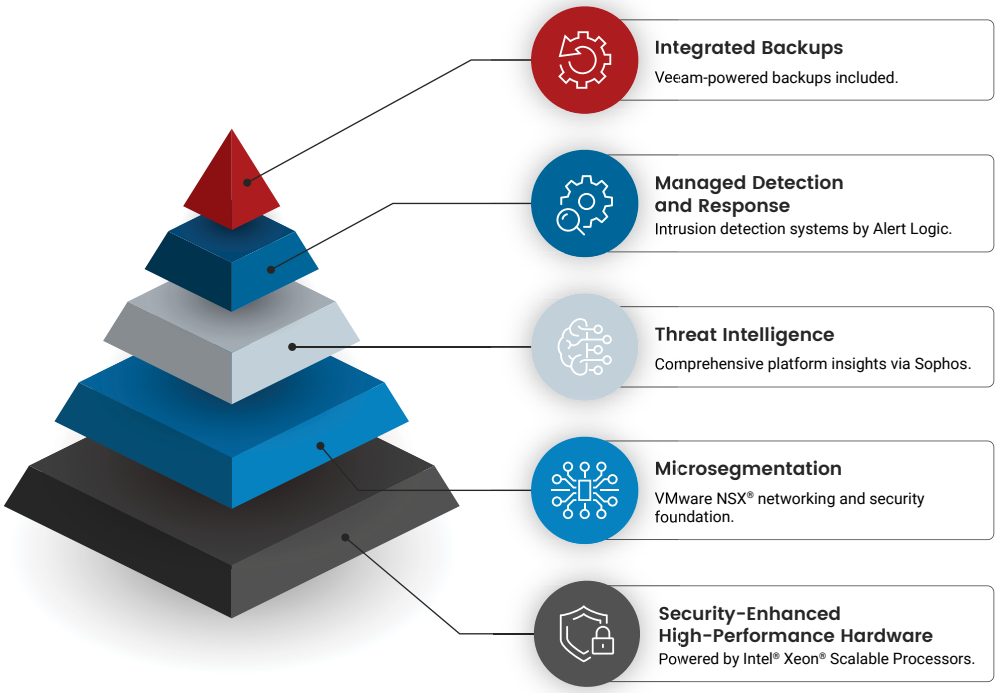
Policies can be regularly tested through periodic ethical hacking performed by the organization's security team. This can help identify the weakest links in the teams and identify areas where further education or policy enforcement is necessary.

Tracking and changing human behavior is not easy and requires continuous effort and vigilance. However, through regular education and strict policies, breaches relying on the human factor can be reduced to a minimum.

IV - Data Security Cloud: On-demand access to Enterprise-Grade Data Protection

Implementing all the steps mentioned above into your cyber security strategy can significantly strengthen your security posture. However, many organizations lack the time, staff, and money required to build a secure cloud infrastructure on premises.

phoenixNAP's Data Security Cloud is designed to provide organizations with a cost-effective way to address their infrastructure security concerns. This multi-tenant, virtualized cloud platform boasts a high-performance architecture that delivers reliability and advanced security on an OpEx model. With VMware NSX at its core, powered by Intel Xeon Scalable processors and integrated with leading security systems and technologies, the platform offers multi-layered software and hardware-based data protection.



The Anatomy of Data Security Cloud

Data Security Cloud uses strict virtualization and segmentation controls powered by the latest hypervisor technologies to ensure advanced data protection. Leveraging the latest networking and compute technologies, such as Software Defined Networking (SDN), the platform enables the creation of logical security policies that can be applied to a virtual machine regardless of location (cloud or on-premises). The micro-segmentation feature of VMware NSX lets you isolate VMs or ensure zero-trust security between them and prevent lateral movement to reduce the blast radius of cyber-attacks.

Secure Hardware Features	Built-in Security Ecosystem
• Root of trust module (TPM) • Built-in instructions for verification • Fast, high-quality random number generator (RDSEED) • Firmware assurance (BIOS Guard)	• Efficient provisioning and initialization (Intel PTE) • Scalable management with policy enforcement (Intel CIT) • VMware integration (NSX, vSphere, vCloud Director, vRealize etc.) • Integrated Enterprise Key Management • Trusted connectivity • Remote attestation for the secure platform Compliance and measurement at the core

Directly integrated into Data Security Cloud, threat intelligence provides organizations with continuously updated intelligence feeds, antivirus, and vulnerability scanning, endpoint protection, as well as machine learning and behavioral analytics.

This secure cloud platform comes with an integrated industry-leading backup solution for up to 100% of your storage, helping organizations ensure availability and quick recovery in case of data loss.

Data Security Cloud also gives you access to a state-of-the-art, HSM-grade Encryption Management Platform (EMP). Through integration and automation, EMP bridges the gap between on-prem and cloud environments, providing a single platform to unify all encryption, key, token, and secret management processes.

Hosted in phoenixNAP's enterprise-grade SOC-1, SOC-2, and SOC-3 audited facilities, Data Security Cloud gives you easy access to premium data center features, including:

1. **GDPR and Privacy Shield compliance** – for data protection requirements when transferring data between the EU and the US
2. **PCI-DSS certification** – for processing sensitive payment data
3. **24/7 on-site security** – with professional staff, video surveillance, MFA, and mantraps
4. **DDoS protection** – a network-wide free 20 Gbps DDoS protection against multiple threats
5. **Hybrid cloud compatibility** – for easy integration of on-prem infrastructure with Data Security Cloud using familiar VMWare tools.
6. **Easy migration** – phoenixNAP's engineers and security staff provide full support throughout the workload migration process.

As a fully managed solution, Data Security Cloud helps you meet regulatory and compliance requirements without the overhead of building and maintaining a secure in-house infrastructure. Through complete visibility into your environment, the platform lets you focus on growing your business while knowing your sensitive data is secure and available at all times.

CONCLUSION

As work models continue to evolve and turn further away from the traditional office, cyber threats increasingly exploit the expanded attack surface. As a result, a comprehensive data protection strategy requires developing a multi-faceted infrastructure defense system to cover everything from hardware and software stacks to end users. Achieving this requires businesses to allot the time, staff, and resources many cannot afford in the struggle between staying competitive and battling the ever-evolving threat landscape.

With managed solutions such as phoenixNAP's Data Security Cloud, organizations with limited budgets and staff gain complete control over their IT environment. Leveraging enterprise-grade hardware, software, and data center technologies on an OpEx model, businesses get easy access to multi-layered security ensuring compliance and rock-solid data protection.

Resources:

1. Cloud Security & Asset Protection Survey 2022, phoenixNAP and VMWare
2. Global Incident Response Threat Report for 2022, VMware
3. 2022 Data Breach Investigations Report, Verizon

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**