OneNeck®
IT SOLUTIONS
a TDS® Company

OneNeck White Paper

Security and Compliance within OneNeck's Cloud and Hosting Solutions
Security by Design – The ReliaCloud® Difference

CLOUD COMPUTING

"Cloud computing" is a concept that has moved to the forefront of the market in recent years. As companies deal with increasing demands for IT services and decreasing budgets, cloud computing solutions have gained significant traction. More and more industry experts see cloud computing as a viable solution in managing IT applications and infrastructure. Security concerns, however, must be carefully considered and vetted as part of your transition to the cloud.

> "In order for organizations to move computing resources and applications to the cloud, **the value must exceed the risk**.
>
> The risks of cloud migration are largely captured in one word – '**security**'. Half of the organizations that are not adopting cloud computing cite security as the reason."
>
> As cloud adoption moves to the mainstream and expands from tactical uses to strategic platforms, enterprises will need to address cloud security and compliance issues more holistically.
>
> This will be especially true as organizations look to use cloud in cases where highly sensitive data is involved, where rigorous compliance requirements apply, or for business-critical applications."
>
> Forrester Research, Inc. *"Security and the Cloud"*

COMMON CLOUD SECURITY CONCERNS

How will a company make sure that confidential information remains protected? Could a company's proprietary data be accessed by a cloud provider, or another cloud user, even worse, a competitor? How comfortable companies feel in the cloud will determine their degree of engagement and what kind of information they will share and what services they will contract. When choosing a cloud provider, it is important to explore security processes and procedures thoroughly and not focus just on technology. Do they have the certifications in place? Do the controls apply to the cloud architecture? Is a fully staffed security operations center (SOC) part of the solution? Does your organization require specialized industry compliance (i.e.: PCI-DSS, HIPAA, etc.) and does the offering in the cloud provide the necessary regulatory compliance. Every cloud provider should be able to articulate security policies and procedures in a formal security policy document that can be provided to prospects and customers.

RELIACLOUD: SECURITY BY DESIGN

OneNeck® IT Solutions answers our customer's cloud security concerns with our ReliaCloud framework. The ReliaCloud framework encompasses our cloud and hosting solutions that are built and managed to strict best practices that provide a level of operational excellence achieved thru rigorous ITIL process and procedure, best-in-class technology, concurrently maintainable data centers and truly remarkable engineering talent. Our technical security controls are designed to industry consensus best practices by a team of senior security engineers with multiple security and vendor certifications. Our ReliaCloud infrastructure was designed with our customers security needs in mind. Only OneNeck meets the stringent facility, technical and operational requirements to be ReliaCloud certified.

OneNeck's ReliaCloud Delivers:

Scale: Consolidation of knowledge and expertise from numerous discipline.

Talent: Leverage our vast Pool of Technical Talent working in concert.

Simplification: We have invested millions in standardization and automation tools to ease common, repeatable tasks and limit human error and overall security risks.

Focus: Centralization of security capabilities with our SOC while other resources worry about integration, availability, capacity.

Intelligence: Security Information & Event Management solutions can greatly enhance your environment's protection.

RELIACLOUD VS. SELF-MANAGED

Security Attribute	ReliaCloud	Self-Managed Considerations
Physical Security	OneNeck owns and operates robust, physically secured data centers with digital camera systems, 24/7 on-site personnel, biometrics/badge access systems, multiple points of access challenge to the facility and policy based restrictions on access to computing systems to only those resources absolutely necessary.	Customers rarely have access to their own equivalent data centers to match what OneNeck offers. Customers can gain similar benefit by colocating their infrastructure in a robust 3rd party data center.
Network Security	OneNeck handles network design and architecture for its cloud and managed hosting customers. This includes security design and management for the network. Proper firewalls, VPN concentrators, content accelerators, load balancers, SSL offloading, etc. are deployed for customers and managed by OneNeck. Backups of network device configurations, log management and archiving, patches and upgrades to network devices, and best practices from a team of certified network engineers are included.	Customers often struggle with the large capital investment to get the correct gear and certified engineering resources. Toolsets for management and review of log entries for security concerns can be an involved and arduous responsibility requiring knowledgeable IT security personnel.

ONENECK RELIACLOUD CERTIFIED CLOUD AND HOSTING SOLUTIONS VS. SELF-MANAGED

Security Attribute	ReliaCloud Certified Cloud and Hosting Solutions	Self-Managed Considerations
Server Security	OneNeck handles server security as part of ongoing administration and management of managed hosting customers. This includes virus and malware control management, hot fix and patch management of server OS and applications, server hardening, log management and archival and best practices from a team of certified system administrators. In fact, OneNeck's managed hosting customers gain the direct benefit and knowledge of over 250 certified, seasoned system administrators.	Similar to the challenges of network security, mid-market customers often struggle with this as well. Lack of capital to purchase the right tools and lack of operations budget to hire the system administrators in the different disciplines makes this a challenge for customers to do themselves
Security Personnel	OneNeck employs a dedicated security and incident management team. This team is responsible for establishing security policy, training for that policy for our service delivery staff and enforcement of the policy. These are highly skilled security specialist with the following certifications: CISSP, CPHIMS, GISP, GCIH, and GSEC.	It is not common for a mid-market organization to have dedicated security personnel or formal incident management in place.
Intrusion Detection Systems (IDS)	OneNeck has a robust Intrusion Detection System (IDS) that all managed hosting customers gain benefit from. The IDS scans all inbound network traffic and looks for attacks/security issues and notifies the security team of any issues.	IDS is commonly in place for the mid-market. When it is in place, it is often not actively managed due to lack of security personnel.
Intrusion Prevention Systems (IPS)	Similar to the IDS above, the Intrusion Prevention System (IPS) can scan traffic and make intelligent decisions on potential attacks and automatically block them in addition to the notifications to the security incident management team.	IPS is commonly in place for the mid-market. When it is in place, it is often not managed due to lack of security personnel.
Security Information and Event Management (SIEM)	OneNeck's SIEM solution correlates the logs from multiple sources including servers, applications and network devices. Our SIEM system will send notifications to our security incident management team and lead engineers when suspicious patterns are detected. The SIEM also serves as an external log aggregator for all computing devices that could have their logs wiped in an attempt to cover tracks from an attacker.	SIEM solutions are typically cost prohibitive for the mid-market. In addition, significant security expertise is required to properly configure and link up SIEM technologies to computer systems. Ongoing management of the notifications requires an investment in operational resources 24/7.
Encryption	OneNeck offers both data at rest encryption and data in transit encryption solutions as part of our cloud and hosting services. Our data at rest encryption meets or exceeds government regulatory compliance such as FIPS140-2.	Encryption technologies are commonly available for self-managed IT environments, however, only a rigorous operational process ensures their effective use and proper chain of custody.
Backups and Secure Destruction	OneNeck cloud and hosting services include comprehensive data backups and data archival solutions with secure storage and off-site rotation of certain datasets. Secure data destruction of data and physical media with chain of custody control is also available.	Backup technologies are widely available for self-managed environments, however, organizations don't often have the extensive policies, procedures or operational discipline to ensure the integrity and thoroughness of data backups required by the organization. Maintaining long-term retention and off-site storage can be costly for the mid-market. In addition, secure data destruction policies and chain of custody tracking are often not in place
Data Loss Prevention (DLP)	Worried about data leaving your organization and falling into the wrong hands? OneNeck's Data Loss Prevention (DLP) solutions will keep your information within your environment and under your control. Users will not be able to copy and/or extract data from your computing environment without your permission or knowledge.	DLP is commonly in place for the mid-market due to costs and complexity.

RELIACLOUD VS. SELF-MANAGED

Security Attribute	ReliaCloud	Self-Managed Considerations
Third Party Vulnerability Assessments	OneNeck's cloud and hosting services include third party security vulnerability assessments. This ensures that an independent organization has certified our customer environments are secure from external attacks.	Vulnerability scans are often subscription based services at a substantial costs for most organizations to do on their own , and not commonly in place for the mid market.
Security Policy Enforcement	OneNeck has a fully documented, mature security management policy that details how we properly secure our customers environments. Every employee attends continuous security training and must abide by the terms of our security management policy.	Documentation and enforcement of security policy is often overlooked in the mid-market.
SSAE16 Compliance/Auditing	OneNeck is Type 2 SSAE 16 (SOC 1) certified and is audited continuously across its security policies by a third party. This validation report is available to customers upon request.	Mid-market companies struggling with PCI-DSS, SOX, HIPPA, FERPA, etc. can benefit from the SSAE16 certification surrounding their IT management/infrastructure.

COMPARING RELIACLOUD TO SELF–MANAGED SOLUTIONS

There really is no comparison for our customers when it comes to our cloud and hosting solutions self-managed IT environments. This is largely because our customers gain the immediate benefit of maturity and scale around security management from our enterprise managed hosting operation, formal security operations center (SOC), years of knowledge and expertise from our expansive senior technical talent, and hardened best-practices in IT management. Self-managed solutions rarely match the scale and depth of our offerings.

RELIACLOUD: AUDIT READY

Audits are never fun and no one really enjoys being audited however they are an important component of maintaining security and operational compliance with many certifications. With OneNeck, audits are a breeze. We are already familiar with numerous industry standard audit processes and expectations including HIPAA, PCI-DSS, U.S.-EU Privacy Shield, ISO27001, FERPA and SSAE16. We know what your auditors expect. We designed our security controls and reporting outputs to be 'audit-ready' to streamline the evidence gathering process for most audits. We understand security, privacy and compliance and we stand ready to help with any audit requirements for our customers.

SUMMARY

Cloud computing doesn't redefine security practices and procedures, it refines them. Use your migration to the cloud to become more secure and more in control. OneNeck's ReliaCloud offers customers unparalleled security controls, risk management and privacy control difficult for most organizations to obtain via their own efforts alone, and not commonly in place for the mid-market.

ABOUT ONENECK IT SOLUTIONS

OneNeck IT Solutions LLC offers hybrid IT solutions including cloud and hosting solutions, managed services, enterprise application management, advanced IT services, IT hardware and top-tier data centers in Arizona, Colorado, Iowa, Minnesota, New Jersey, Oregon and Wisconsin. OneNeck's team of technology professionals manage secure, world-class, hybrid IT infrastructures and applications for businesses around the country.

OneNeck is a subsidiary of Telephone and Data Systems, Inc. [NYSE: TDS]. TDS provides wireless; cable and wireline broadband, TV and voice; and hosted and managed services to approximately six million customers nationwide through its businesses U.S. Cellular, TDS Telecom, OneNeck IT Solutions LLC, and TDS Broadband Service LLC. Visit tdsinc.com.