

Security Managed Services

As cyberthreats become more pervasive and more sophisticated, you need dedicated expertise to protect your company's data.

Data security continues to be the number one threat to businesses, and CIOs and CISOs are struggling to keep pace.

Damages from cybercrime are expected to reach \$6 trillion by 2021, and the number of security breaches is increasing at a rate of 27.4% annually. A Ponemon Institute study estimates that the average cost of a U.S. cyberattack is \$15 million.

Cyberattacks are becoming more sophisticated and more insidious. The number of ransomware attacks alone has increased 15 times over the past two years and it's estimated that by 2019 one business will fall victim to ransomware every 14 seconds. Phishing is another area of particular concern. One study shows that 78% of users understand the risk of phishing emails, but phishing attacks are becoming more believable and 45% of users clicked on phishing links anyway.

At the same time, 52% of organizations that suffered from a cyberattack in 2016 have no plans to change their security systems, and 45% are planning to keep the same budget for security. And due to a lack of available talent, there is expected to be more than three times the number of unfilled cybersecurity jobs by 2021.

Enterprise security and compliance are a growing problem that most companies can't adequately solve using existing resources. That's why more organizations are improving security and compliance and reducing costs by outsourcing to dedicated security professionals.

Choosing the Right Security Partner

When seeking out the best managed security services, making the right choice is largely a matter of trust. The level of engagement hinges on the degree of confidence a company has in security protocols, the types of information they are willing to share, and the services they will ask of a managed service provider. When it comes to talking about security, trust is paramount.

That's why OneNeck has developed a security framework based on the three core principles of the CIA: Confidentiality, Integrity and Availability.

Maintaining reliable data security and compliance requires expertise, dedication, and regimentation. That's why everything we do for our customers is built and managed according to strict best practices. We maintain a higher level of operational excellence through a combination of ITIL processes and procedures, best-in-class technology, top-tier certified data centers and exceptional security and engineering talent.

OneNeck excels at delivering security by design, which means we build security solutions from the ground up, customized to meet your organization's unique requirements. Every detail is analyzed and assessed for security and risk implications, as well as its impact on regulatory compliance.

Compliance is an ongoing concern for many of our customers, which is why we go beyond risk assessment to ensure security measures conform to all necessary privacy, secure data management, data storage and reporting protocols.

Our technical security controls are designed to comply with the most rigorous best practices, and our senior security team is made up of engineers and experts with multiple security and vendor certificates. It's our versatility, attention to detail and deep engineering bench that has made OneNeck a preferred IT compliance partner for companies of every size, in every industry from coast to coast.

Following are some of the security and compliance areas where OneNeck managed services excels.

Data Encryption

Data has become the currency of business, and sharing and securing sensitive data has become an ongoing concern for CIOs and CISOs. As data networks become more fragmented, transmission channels become harder to secure. Even though a hosted connection or network server is deemed secure, there is still a risk from malicious insiders as well as outside hackers.





Securing the data as well as the transmission channel protects information from both internal and external threats. We can help you develop data encryption strategies for data transmission, email, real-time communication and more.

Intrusion Detection and Prevention

Threats from external sources are growing at a geometric rate, so protecting your critical data requires vigilant intrusion detection and prevention solutions. Data traffic need to be continuously monitored to eliminate potential threats while allowing legitimate data traffic to reach its destination. The challenge for IT is sifting through the thousands of alerts to identify which ones are real threats and which ones are false alarms.

Working with OneNeck can prevent your IT team from running in circles. Our expert security team can assume responsibility for keeping intruder detection/intruder prevention devices up to date, and for continuously monitoring data traffic looking for anomalies. By shifting intrusion detection and prevention to OneNeck, your IT team can focus on more strategic initiatives.

Security Information and Event Management

Information security strategies such as authentication, encryption, and intrusion detection are a critical part of IT planning and implementation. It's not enough to see when your data is being accessed. You also need manage who has data access and what permissions need to be in place. And you need to be able to monitor for threats to your organization and identify points of weakness before they can be exploited.

Applying security information and event management (SIEM) provides a centralized point of view that makes it easier to spot trends and unusual data patterns that could indicate a security threat. OneNeck's managed SIEM offers scalable, real-time security monitoring and analysis to our customers to detect threats and meet compliance requirements.

Log Management

With more devices connected to the network, log management becomes a problem since each device generates its own log of ongoing activity. If each of these logs isn't monitored and analyzed, the real security threats can go undetected. However, the sheer volume of logs makes it impossible to perform a thorough analysis.

The OneNeck security team can not only monitor your logs for alerts, we can analyze logs from each device, looking for potential security

threats, and then prevent and/or mitigate those threats before they compromise your critical data.

Hosted and Managed Services to Lower Costs

Managing IT resources becomes harder when you have to justify every dollar you spend. Organizations are finding they need more security services but don't have the budget to expand.

OneNeck can save you money. Outsourcing security services can reduce operating expenses while improving data security. Every IT project requires a cost analysis, including comparing the costs of in-house resources against a service provider. You know the benefits of using security specialists, and when you evaluate the quality and cost of OneNeck's managed services against in-house services, we're confident you will find OneNeck offers more for less.

Why OneNeck for Security and Compliance

Everything we do for our customers is built and managed to strict best practices that provide a level of operational excellence achieved through rigorous ITIL process and procedure, best-in-class technology, top-tier certified data centers and truly exceptional engineering talent.

There are many reasons to rely on OneNeck for your managed security and compliance needs. Here are just a few to consider:

Uptime SLAs – OneNeck prides itself on providing reliable services. Our uptime SLAs are backed by security, power, and redundancy requirements that not only meet but exceed expectations. All of OneNeck's managed security services offer high performance and high availability, and are have financially backed SLAs.

Flexibility on demand – Our security and compliance services are fully customizable, tailored to meet specific business needs today, and changing business needs tomorrow.

Frees up valuable in-house resources – In-house IT resources are expensive, and are best used for strategic projects. OneNeck relieves your IT team from handling routine maintenance and troubleshooting, leaving them free to focus on mission-critical initiatives.

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.