IT Security Services for State and Local Government

Enabling citizen-centric services, powered by transformative IT solutions

Lack of expertise, visibility and control, limited budgets, outdated/aging infrastructure, legacy systems and spending priorities are big factors causing state and local municipalities to fall victim to cyber-attacks.

According to a 2015 Ponemon Institute report:

- Cybersecurity practices are not clearly defined, according to 71% of state and local respondents.
- 50% of state and local governments experienced 6 to 25 breaches in the prior 24 months, and 12% experienced more than 25 breaches.
- Most state cyber budgets are between 0-2% of their overall IT budget, compared with an average of more than 10% in large companies.

Today's threats are accelerating and becoming more sophisticated, insidious and dangerous. Your security infrastructure is getting more complex, yet most environments have separate, single-point products to address the wide range of threats. These separate products can leave gaps in your defenses, increase costs and complexity, and lengthen response times.

Identifying Your Gaps

Understanding your security gaps is key to addressing regulatory obligations and protecting your organization from breach. OneNeck can help by conducting assessments designed to identify vulnerabilities in your IT systems and gaps in your security program, followed by a thorough gap analysis that will leave you with a roadmap to remediation and compliance.

OneNeck Security Assessment and Strategy services include:

- Cybersecurity assessment
- Framework assessment and implementation
- Policies and standards
- Penetration testing
- Vulnerability management

Closing the Gap with OneNeck, Your Trusted Cybersecurity Partner for State and Local Government

State and local governments face a challenging new reality when implementing today's emerging technologies — a looming threat to constituent data security. Technologies such as mobility and the cloud are creating new — almost daily — opportunities for advanced, targeted attacks. It makes today's prevention strategies nearly inadequate for tomorrow.

At OneNeck, we recognize threats can enter the network in a variety of ways. We understand that having comprehensive protection requires a multi-tiered and pervasive approach to keep threats out as well as detect and isolate any breaches quickly. We can assess your infrastructure for its strengths and weaknesses, then recommend and implement a solution that will keep your critical data safe.

OneNeck®
IT SOLUTIONS
a TDS® Company

Our solutions include:

- **Network Security**. End-to-end solutions from design architecture and deployment to configuration review related to all aspects of network security including firewalling, intrusion prevention sensors, VPNs and traffic encryption/decryption.
- **Secure Application Delivery.** Protect your applications from external and internal threats with traffic managers and web application firewalls that offer SSL/TLS visibility and control, deep packet inspection, federated identity and DDoS protection.
- **Web and Email Security.** The top two attack vectors for malware continues to be email and web browsing. You need a solution that uses advanced tactics to block malicious websites and emails whether on the corporate network or off.
- **Public/Private Cloud Security.** Protect your resources from incurring outages and your data from exfiltration through proper design, system segmentation and access control. Identify shadow IT and public cloud risks by implementing a cloud access security broker (CASB) solution.
- **Identity and Secure Access.** Don't sacrifice security for user access. Provide authorized and secure access to your network with identity and secure access solutions.
- **Endpoint Security.** Running anti-virus with an encrypted HD isn't enough these days. You need a next-gen solution to prevent endpoints from being breached and to remediate them if they are.
- **Secure Enterprise Mobility.** Enforce mobility policies, regulate behaviors, contain costs and manage risks across multiple device platforms with an MDM solution to address BYOD risks.
- **Security Monitoring and Threat Hunting.** When a security threat is in progress you need to respond in time to protect against it. And since no security solution is 100% effective, you need a comprehensive SIEM solution in place to reduce your time to detection and breach remediation.
- **Security Assessments.** Security assessments using best practice or other industry standards like HIPAA or PCI are essential to identifying security and compliance risks and keeping your security program on track.

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 wholly owned 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.

OneNeck®
IT SOLUTIONS
a TDS®Company

Call 855.ONENECK | Visit OneNeck.com