SCANTRON
TECHNOLOGY SOLUTIONS

SMART STARTS HERE

Managed Security Services

Assess, Plan, Implement, and Monitor Your IT Environment's Security

Regardless of your organization's size or the capacity of your IT resources, you'll be subject to attempted data breaches and many other security risks. Through our comprehensive environmental assessment, strategic planning, exhaustive policy review, and continuous monitoring, you can reduce risk and improve security without investing in a large security team and high-level security infrastructure.

Your business's well-being relies on effective and secure handling of information. Most firms are required to comply with privacy regulations such as HIPAA, FISMA, FFIEC, PCI-DSS, FERPA, GLBA, or more than one of these.

In a perfect world, you would have a full team to monitor for and detect threats, test your system's resiliency, and continuously adapt your policies and procedures to meet emerging threats.

In reality, you likely contract with various security consultants to meet basic needs. With ballooning cybersecurity costs, how can you assess whether you have enough mitigations in place throughout the organization, or whether these measures comply with industry regulations?

Managed Security Services

When you engage Scantron for Managed Security Services, you gain a trusted advisor. Our security engineers measure and improve the security of your entire IT environment using internal and external security scans, policy and regulatory compliance examinations, operational assessments, and budget reviews.

With decades of experience in serving highly regulated industries, our team of in-house experts stays current on the latest threats, the most effective devices and software, and the best methods to mitigate risk. We continuously apply this knowledge across all of our supported customers.

Key Benefits

- **Better compliance exam readiness and responsiveness**
- **Centralized operating approach to security for improved oversight and management**
- **Enhanced or new security policies**
- **Proactive detection and mitigation of items that could lead to a breach**
- **Larger security footprint**

Engagement Steps

Depending on your requirements, you may need the full suite of Managed Security Services. We configure a plan to address your most urgent needs.

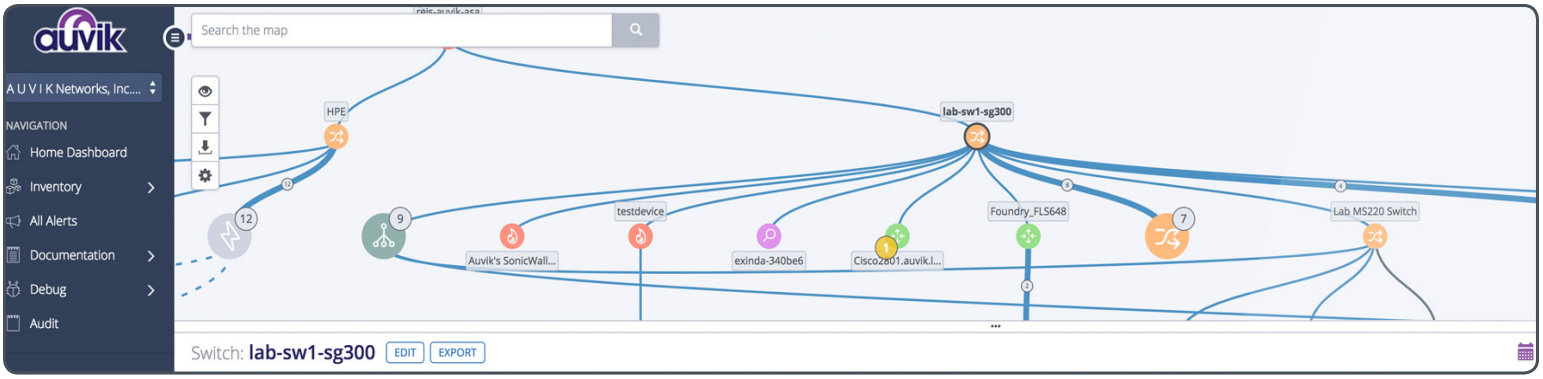
Security Audit, Policy Engagement, and Infrastructure Assessment and Engagement

Step one is typically a comprehensive assessment of your current security posture and a comparison to best practices and standards.

- **Capture current security practices to include policies, network topology, and user account permissions**
- **Planning and education: When is your next security audit? Do you meet training requirements for your industry? How do you prepare for current security risks and keep up to date on current market trends?**

On average, it takes a firm 191 days to identify a data breach. In 2018, the average per capita cost of data breaches was $233 and the total average organizational cost was $7.91 million.

Source: Ponemon Institute, 2018 Cost of a Data Breach Study: Global Overview



We use sophisticated network management tools for monitoring, reporting, alerting, and configuration management.

We examine your policies and procedures and baseline your IT infrastructure and its security posture. When necessary, we make recommendations to update and bring everything current, including development of new policies.

- **Policies include Acceptable Use, Access Control, Business Continuity, Change Management, Disaster Recovery, Encryption, Incident Response and Handling, Physical Security, Network Security, and many more**
- **Hardware and software inventory and procedures: What do you have and how do you handle patching and versioning? Who can access systems, information and applications?**
- **Networking device inventory (routers/switches): Check current security hardening**
- **Change management: What is your process for introducing new hardware, appliances, software, and processes into the environment?**

Strategic Security Planning, Continuing Education

We create a strategic plan that will both aid you in adapting to emerging and continuous security threats and better prepare you for regulatory oversight. This can include directly assisting you with responding to audits.

- **Which information are auditors requesting?**
- **Access reporting that your internal IT team can digest and supply to an auditor**
- **Adapt to current market trends in security**
- **Craft training measures and documentation to meet target security posture**
- **Ensure training requirements are compliant**

Vulnerability Scanning and Auvik Network Monitoring

Finally, for ongoing and proactive security, we periodically scan for vulnerabilities and deploy advanced network monitoring. Easy-to-use reporting and analysis will help you address exposures and gain valuable insights into the health and performance of your network over time.

- **Annual, semi-annual, quarterly internal/external vulnerability scan and findings report**
- **Audit remediation and reporting**
- **Guidance and remediation concepts powered by in-house security analyst**
- **Monitor and report on non-Windows devices**
- **Network and device discovery and real-time topology**
- **Device configuration backup and restore**
- **Configuration management and analysis**
- **Network evidence history and network traffic visibility insights**
- **Live & historic network performance data**

OPTIMIZE YOUR BUSINESS IT SOLUTION OPTIONS TODAY!

For a free consultation to meet your organization's goals, call **800.228.3628** or visit **www.scantron.com** to learn more.

About Us

Scantron Technology Solutions provides managed print and IT services you can count on. Our nationwide team of experts provide full-service packages and á la carte options to be your IT team or to support your current staff. Scantron solutions meet you where you are and help you get to where you want to be.

@ScantronTech Scantron Technology Solutions 07.2019