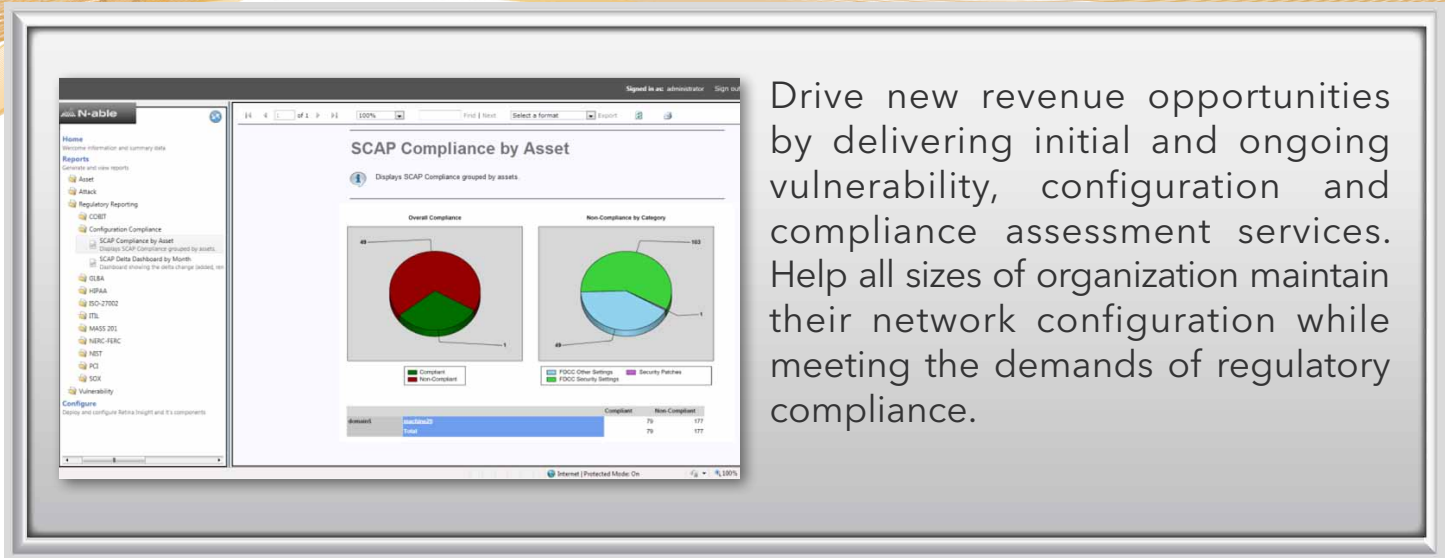




AUDIT MANAGER



Drive new revenue opportunities by delivering initial and ongoing vulnerability, configuration and compliance assessment services. Help all sizes of organization maintain their network configuration while meeting the demands of regulatory compliance.

Audit Manager is comprised of three complementary products:

- » Audit Manager | Vulnerability
- » Audit Manager | Configuration
- » Audit Manager | Compliance

Audit Manager | Vulnerability is an integrated end-to-end vulnerability and compliance solution designed to help organizations with protection and compliance by defining and monitoring relevant IT controls.

Audit Manager | Vulnerability monitors both patch and configuration vulnerabilities and compliance to pre-defined configuration baselines and provides automated notification of violations. The environment is assessed, capturing established security controls along with any vulnerabilities or configuration violations that impact the network. Detailed reports providing prescriptive guidance and recommendations are then forwarded and response is initiated to ensure that corrective action can be taken in a timely fashion.

Audit Manager | Vulnerability's management console is a fully integrated and rich internet-enabled application for security and compliance management.

Now you can simplify the management of distributed, complex infrastructures while protecting your mission critical assets from evolving threats with a single unified management system.

FEATURES & BENEFITS

REDUCE THE COST OF SECURITY and compliance by automating configuration auditing and vulnerability management

ENSURE THAT YOU ARE protected from the latest known vulnerabilities with intelligently updated audits database that include a 48-hour SLA for critical vulnerabilities

PRIORITIZE RESOURCES AND streamline remediation efforts through executive and task specific reporting offering risk scoring prescriptive and guidance on issues

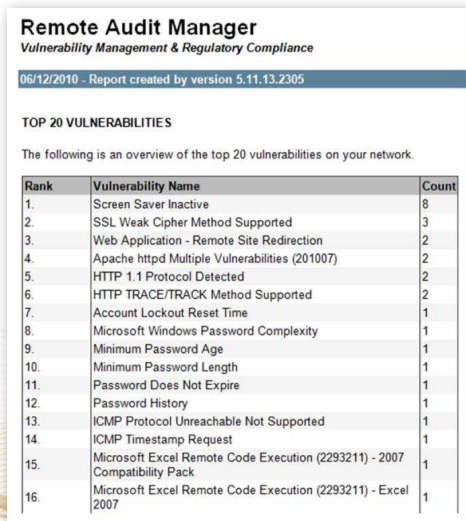
SIMPLIFY ASSESSMENTS AND lower cost with a single solution that provides non-intrusive, scalable remote scanning that will not impact business assets or operations

DISTRIBUTED SCANNING AND reporting of all discovered assets, compliance violations and vulnerabilities into a single management console

Audit Manager | Configuration allows you to prioritize and manage risk, audit configurations against internal policy or external best practice and centralize reporting for monitoring and regulatory purposes.

While many organizations focus on implementing strong controls over systems and applications, they often fail to formalize, automate, or optimize the business processes that keep their Windows environment secure. Ensuring that systems are configured according to policy is critical to reducing risk, improving security, and demonstrating compliance.

But this is often a challenge, with constantly changing networks and systems and time consuming monitoring and reporting. Organizations need to take corrective actions when changes or threats impact their security and compliance posture.



Audit Manager | Configuration simplifies configuration compliance with drag-and-drop templates for Windows operating systems and applications from FDCC, NIST, Microsoft and CIS. Prioritize and manage risk, audit configurations against internal policy or external best practice and centralize reporting for monitoring and regulatory purposes.

Audit Manager | Configuration is available as an add-on to Audit Manager | Vulnerability. With this module, a complete configuration compliance benchmark library keeps systems up-to-date with industry benchmarks including changes to benchmarks and adjustments for newer operating systems and applications. Automate configuration compliance and reporting to cut report creation and delivery costs, while maintaining control over data.

Audit Manager | Compliance adds comprehensive reporting packs to the Audit Manager | Vulnerability solution to help organizations assess their environment against the requirements mandated in a broad range of regulatory compliance specifications.

In a growing number of industries, businesses are under increasing pressure to comply with regulations mandating data security and network integrity. Accounting scandals and well-publicized security breaches have angered consumers, cost businesses vast losses in revenue, and have legislators looking for solutions. As a result, businesses finds themselves legally compelled to put in place rigorous controls and monitoring processes for risk assessment, compliance reporting, and vulnerability assessment.

Security regulations are continuing to evolve, and audits are becoming more frequent and more comprehensive. Compliance is about managing the security risks to your organization and safe guarding intellectual property and consumer data from fraud, theft, and misuse.

