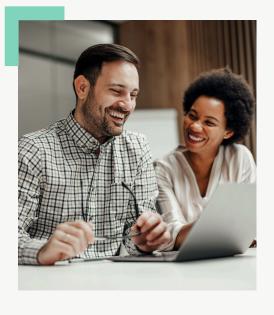# Why A Network Assessment Protects Your Organization

Why This Assessment Matters

Your business runs on technology. Every application, user account, and device is a potential doorway, either to productivity or to a breach.

A StrataDefense Network Assessment gives you clarity on where vulnerabilities exist and how they impact your operations, compliance posture, and long-term growth strategy.

This is not a technical exercise for its own sake. It's a business tool that answers key leadership questions:

- Where are we exposed?
- How does that risk affect our ability to operate, serve clients, and grow?
- What steps will reduce exposure while aligning IT with our strategic priorities?

Why This Matters for Leadership

Reduce the likelihood of costly security incidents.

Build a foundation for scalability and future technology adoption with confidence.

Strengthen compliance readiness across frameworks like NIST, HIPAA, and PCI DSS.

What a Network Assessment Can Reveal

Our process examines your IT environment holistically: hardware, software, user access, and configurations. We uncover risks that matter most to your business and provide actionable insights to address them.

Examples of What You'll Learn

OVERALL SECURITY POSTURE

A consolidated risk score that reflects the health of your IT environment. Example: A grade of D signals critical gaps that need immediate attention.

KEY RISK DRIVERS

Unsupported or aging operating systems, critical software vulnerabilities, and weak access controls such as inactive accounts or non-expiring passwords.

COMPLIANCE SNAPSHOT

Identify gaps against standards like NIST and HIPAA, reducing risk of fines, audit failures, and reputational harm.

OPERATIONAL WEAKNESSES

Unsecured endpoints, inconsistent device configurations, and lack of visibility into user activity.

Why It Matters for Your Business

Unchecked vulnerabilities do more than create IT headaches, they pose real business risks:

OPERATIONAL DISRUPTION

A single attack can halt productivity and impact client trust.

REGULATORY EXPOSURE

Compliance failures invite penalties and reputational harm.

FINANCIAL IMPACT

The average cost of a data breach in regulated industries exceeds $4 million.

STRATEGIC LIMITATIONS

Insecure infrastructure slows your ability to scale confidently.

Your Next Step

The first step to addressing these risks is knowing where they are. A StrataDefense Network Assessment provides clarity, delivering actionable insights, prioritized remediation strategies, and a roadmap for resilience.

Schedule your Network Assessment today and take control of your organization's security and compliance posture.

Strata Defense

info@stratadefense.com
(715) 842-7665

stratadefense.com