

Key Findings from a Network Assessment

Clarity on Your Cyber Risk Starts Here

Your organization relies on technology for every critical operation. If vulnerabilities go unnoticed, they can lead to costly breaches, compliance violations, and downtime that impacts your reputation and revenue.

A StrataDefense Network Assessment delivers an objective, data-driven view of your IT environment. It identifies gaps that put business strategy, operational resilience, and regulatory compliance at risk.

This isn't a compliance checklist. It's a strategic tool for making informed decisions that strengthen your business today and position it for secure growth tomorrow.



Why This Matters to You

Reduce the likelihood of costly incidents before they disrupt your business.

Build confidence that your technology investments support growth, not risk.

Gain clarity on compliance gaps that can lead to fines or reputational harm.

What This Assessment Can Reveal

Our assessment goes beyond surface-level scans. It pinpoints the hidden risks in your infrastructure, then translates them into actionable insights for business leaders. Here's what you can expect to uncover.

OVERALL RISK SCORE

A single, consolidated score that reflects the security posture of your environment.

Example: Grade D – High Risk

What this means: Critical vulnerabilities and configuration gaps require immediate attention to prevent business disruption.

TOP RISK DRIVERS

Outdated Systems: Devices running unsupported operating systems or nearing the end of life.

Critical Vulnerabilities: Software flaws with active exploits, increasing your risk of ransomware and data breaches.

Weak Access Controls: Inactive user accounts or non-expiring passwords create easy entry points for attackers.

COMPLIANCE SNAPSHOT

Gaps against frameworks like NIST, HIPAA, and PCI DSS signal exposure to regulatory penalties and reputational damage.

Example: Non-compliance across multiple categories, including password policies and encryption standards.

OPERATIONAL WEAKNESSES

- Inconsistent security configurations across devices.
- Aging hardware jeopardizes performance and long-term scalability.

Why It Matters for Your Business

Unchecked vulnerabilities don't just create IT challenges; they affect your bottom line:

- **Operational Disruption:** Downtime stalls productivity and damages customer trust.
- **Financial Loss:** The average cost of a breach in regulated industries exceeds \$4 million.
- **Regulatory Penalties:** Compliance failures result in fines and a loss of client confidence.
- **Growth Limitations:** Weak infrastructure hinders your ability to scale and adopt new technology securely.

Turning Insight Into Action

StrataDefense transforms findings into a roadmap for resilience and growth:

- **Prioritized Remediation:** Focus on the most impactful risks first.
- **Continuous Protection:** 24/7 monitoring and layered defense to stop threats before they escalate.
- **Strategic Alignment:** Technology decisions that support compliance, scalability, and operational goals.

OUR APPROACH

We act as an extension of your team—bringing deep expertise, practical solutions, and the responsiveness you need to stay ahead in an evolving threat landscape.