Defend 360™ Cybersecurity Assessment

A Clear, Practical View of Your Organization's Cyber Risk

Defend 360 is a comprehensive cybersecurity assessment designed to help organizations understand their true risk exposure—not in abstract technical terms, but in practical, real-world scenarios that reflect how modern attacks actually occur.

Rather than focusing on a single tool or control, Defend 360 evaluates both external exposure and internal network risk to identify where attackers could realistically gain access and what impact that access could have.

External Exposure: What Attackers See First

External exposure represents the vulnerabilities visible from outside your organization. These are the paths attackers most commonly use to gain an initial foothold.

- Employee credentials exposed on the dark web
- Email authentication gaps that allow impersonation and phishing
- Employee susceptibility to phishing and social engineering
- Public-facing systems with outdated or insecure configurations

Most breaches begin here. Stolen credentials or a single successful phishing email often provide access without triggering alarms or advanced security defenses.

Internal Network Risk: What Happens After Access

Once inside a network, internal controls determine how much damage an attacker can cause. Defend 360 highlights weaknesses that increase the likelihood of data loss or operational disruption.

- Passwords that never expire or are reused across systems
- Default credentials still active on servers or devices
- Unsecured file storage containing sensitive or regulated data
- Excessive user permissions and limited access segmentation

In many environments, attackers rely on simple misconfigurations rather than sophisticated exploits. Correcting these issues can significantly reduce overall risk.

Why These Findings Matter

Cybersecurity risk is ultimately business risk. The issues identified through Defend 360 can translate directly into financial loss, downtime, regulatory exposure, and reputational harm if left unaddressed.

- Higher likelihood of ransomware or data theft

- Potential regulatory or compliance penalties
- Operational downtime that disrupts revenue and productivity
- Loss of customer and partner trust

Moving Forward with Clarity

The majority of risks uncovered through Defend 360 are both visible and fixable. The assessment provides a prioritized view of exposure so organizations can make informed decisions about remediation, investment, and long-term security strategy.

Next Step: Review your Defend 360 findings with a Get IT Sense security advisor to discuss prioritization, remediation options, and ongoing risk management strategies.