



ALWAYS LEADING

# Who's Accessing Your Network?

Security should always start with zero trust – assume NO ONE is trusted to access your network. Sentinel's Zero Trust Workshop assists customers in identifying their highest areas of risk for workplace, workforce, and workload.

The COVID-19 pandemic has pushed many organizations to significantly expand their work from home capabilities. In the rush to support mass amounts of remote workers, organizations often compromise their cyber security standards and protection. Cyber criminals are acutely aware that security has been weakened in order to address the immediacy of access, and use the chaos as an opportunity to breach your systems, often without detection.

## Workshop Overview

- Initial Risk Discover - Experts will perform a comprehensive analysis of your network & security posture
- Workforce Overall Security & Controls -Who is my workforce? What happens from a user & device access perspective?
- Workload Security & Controls -Where do critical assets reside? Is my data secure?
- Workplace Threat Protection & Controls -Has my environment already been compromised? How do I contain threats?
- Report - Sentinel will provide recommendations that align with the strategic goals and business objectives of your organization

## Benefits

- Provide remote workers with in-office levels of security
- Rapidly identify areas of risk within your remote access infrastructure
- Significantly improve the security posture of your organization
- Assessment results presented with your overall risk score and zero trust readiness



[www.sentinel.com](http://www.sentinel.com)

1.800.769.4343 (main)

1.800.297.4853 (Incident Response Emergency)

[infoSENter@sentinel.com](mailto:infoSENter@sentinel.com)