The LookingGlass™ Supplier Cyber Attack Surface Analysis provides organizations with a detailed, measurable way to examine their third party vendors' security posture across five categories of cyber risk. Each report is reviewed and analyzed by expert intelligence analysts in the LookingGlass Special Investigations Unit.

Five Categories of Cyber Risk:

- **Evidence of System Compromise or Infection:** Identifies evidence of live or recent infections on your suppliers' network from botnets, viruses and malware.
- **Compromised User Accounts:** Identifies account credentials stolen from your vendors among billions of breached records.
- **Vulnerabilities in Externally-Facing Applications:** Maps your vendors' public facing Internet footprint and itemizes the type, number and severity of vulnerabilities available to an outside threat actor.
- **Domain Portfolio and Spear Phishing Risk:** Analyzes registered domain names for fakes and look-alikes to identify likely vectors for spear phishing.
- **Online Indications and Warnings:** Examines feeds, posts and online chatter from more than 6,000 known actors and groups, as well as hacker channels and the dark web.

Unlike other risk assessment reports currently in the market, the Cyber Attack Surface Analysis extends beyond vulnerabilities and network issues to provide actionable intelligence on your suppliers' risk from threat actors, spear phishing and possible data breaches.

**Leverage Supplier Cyber Attack Surface Analysis to:**

- Minimize your attack surface by providing a deep dive evaluation of your vendors’ security vulnerabilities.
- Save valuable man hours evaluating your vendors’ security posture.
- Gain insight into vendor application vulnerabilities to inform more effective supplier management.
- Proactively look for potential leaks, theft of sensitive data or other holes in your vendors’ security posture.
HOW THIS BENEFITS YOUR ORGANIZATION

Analysis from Trained Experts
This isn’t a pushbutton scorecard based on automated scans. The LookingGlass Special Investigations Unit reviews and analyzes every report in all five cyber risk areas to explain the meaning of the data and the specific risks identified.

Breadth of Sources
By combining structured data from LookingGlass ScoutVision™; proprietary LookingGlass tools, systems and databases; and threat intelligence from the surface, deep and dark web, your organization will have a single, unified view of your vendors’ cyber risk footprint. You can quantifiably assess and measure their security posture as threats continually evolve.

Inform GRC (governance, risk and compliance) Policies and Activities
Quickly and cost-effectively identify holes in your third party vendors’ security posture to streamline vendor procurement and renewal processes, as well as ensure compliance with various industry regulations.

Clear Methodology
No “black boxes” here. Each of the five areas of cyber risk include a clearly detailed methodology section so you can understand exactly how sources are examined and determined to be a cyber risk.

ABOUT LOOKINGGLASS CYBER SOLUTIONS

LookingGlass Cyber Solutions delivers unified threat protection against sophisticated cyber attacks to global enterprises and government agencies by operationalizing threat intelligence across its end-to-end portfolio. Scalable threat intelligence platforms and network-based threat response products consume our machine-readable data feeds to provide comprehensive threat-driven security. Augmenting the solutions portfolio is a worldwide team of security analysts who continuously enrich our data feeds and provide customers unprecedented understanding and response capability into cyber, physical and 3rd party risks. Prioritized, relevant and timely insights enable customers to take action on threat intelligence across the different stages of the attack life cycle. Learn more at https://www.lookingglasscyber.com/.