



BASELINE ATTACK SURFACE REPORT™

The First Proper Step For Vendor Risk Management

The LookingGlass™ Baseline Attack Surface Report is a cost-effective first step to determining which of your vendors pose the most risk to your organization. Your report will not only provide a historical analysis, but will also help you meet compliance and regulatory requirements when the occasion arises. Provided with an aggregated risk summary, your vendor benchmark opens the door for an easy conversation with your vendor or upper management, outlining “next steps” for proper process changes allowing your organization to quickly adjust to the outlined vendor risk.

Baseline Report Highlights

1. System Compromise:

Vendor network foot-printing is made possible with LookingGlass' Threat Intelligence Platform (TIP) ScoutVision™, allowing your security team to quickly identify:

- Malware hosting/distribution
- Virus/botnet infection
- Command-and-Control (C2) activity
- Sending/relaying spam
- Malicious/scanning behavior
- Questionable asset use
- Hosting of phishing or fraud sites

2. Compromised Company Account Credentials:

Leaked credentials pose a real problem in today's challenge to secure Personally Identifiable Information. Metrics are provided around:

- Total record count
- Unique user count
- Count of user identified with 10+ breaches
- Count of malware sourced leaks
- Count of reputation risk websites associated with total user set
- Highest total for an individual user

3. Network Hygiene:

Keeping the network running at optimal performance not only enables your business but impacts your bottom line. Review the main domain of a vendor or third party for common implemented protocols:

- DomainKeys Identified Mail (DKIM)
- Sender Policy Framework (SPF)
- DNS Security (DNSSEC)
- TLS/SSL enabled
- TLS/SSL expired

4. Hacker Chatter:

Monitoring all the corners of the Internet allows your organization to see beyond the surface for impending attacks or vulnerabilities by aggregating counts based on client inputs and public data on:

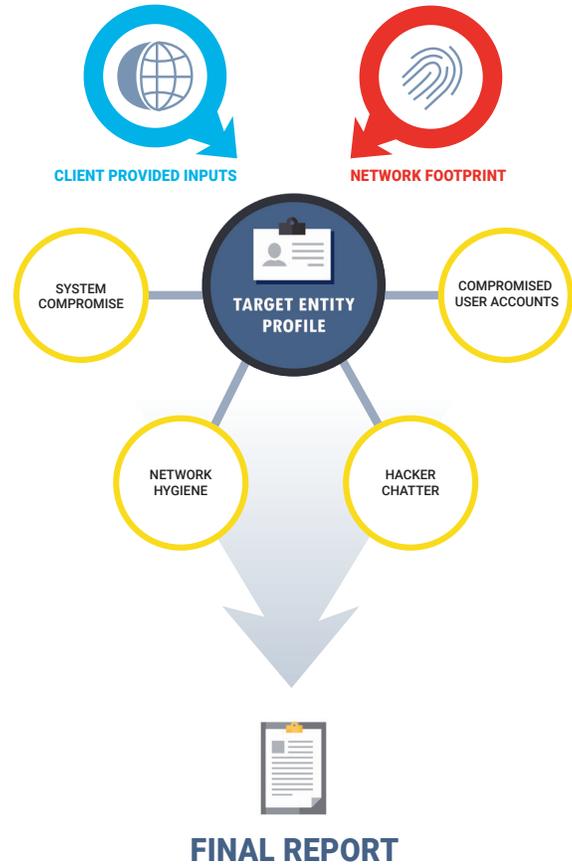
- Dark Web
- IRC/messaging networks
- Underground forums



How Do I Receive the Report?

Findings are delivered in a number of ways. The report is generated (in English) in PDF format, and then encrypted before it is consumed via email, FTP, or through a secure file sharing system.

FEATURES	BENEFITS
Cost-Effective	<ul style="list-style-type: none"> A low-cost way to receive a summary of the appropriate steps needed to remediate vulnerabilities in your organization. Designed to be simple, this report focuses on first steps for an organization looking to understand their vendor risk.
Compliance Ready	<ul style="list-style-type: none"> In the event of a vendor breach, both your vendor and business are now held responsible. Our reporting shows due diligence on your part as your company becomes compliance ready.



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 third 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/>.

Know More. Risk Less.