LOOKINGGLASS

The Silent Threat:

SUPPLY CHAIN & THIRD PARTY CYBER RISK

TABLE OF CONTENTS

As companies rely on an ever-widening ecosystem of suppliers and third-party providers, cyber risks and attacks are multiplying. While being more interconnected creates efficiencies and strengthens business operations, it also increases one's attack surface and potential attack vectors.

Executive Summary

The December 2019 SolarWinds compromise, which was discovered not by the company itself, but by FireEye as they conducted an internal investigation on a breach in their systems, has proven to be a wake-up call, not just to cybersecurity companies but to business and government executives around the world. The wide-ranging impact of this attack—from companies from Microsoft to organizations like the U.S. Department of Homeland Security and Treasury—has demonstrated that *"check-list security"* for supply chain and vendor risk management will no longer be sufficient. Now more than ever before, knowing one's vulnerable supply chain network dependencies must be a critical component of any cybersecurity program.

> Without a view into supply chain security, your organization cannot effectively put the right protocols in place to defend your organization from its next potential attack.

In this white paper, we will discuss what supply chain and third-party risk is and why it can be so difficult to understand, manage and mitigate. Next, we will share why layering threat intelligence onto your ecosystem's external network footprint is critical.

Organizations can stay a step ahead of an exploit by leveraging solutions that combine continuous, external infrastructure monitoring with contextual threat intelligence to enable them to identify and mitigate risks and vulnerabilities of any asset connected to the internet—whether it is theirs or their supplier's.

— **Gilman Louie**, CEO
LookingGlass Cyber Solutions

A Common Ailment: Supply Chain Risk

By many measures, SolarWinds was an outlier. The damage it caused to organizations across the globe was also far above that of prior malicious software. The incident impacted some of the largest organizations in the world, including significant portions of the U.S. Federal Government. The truth is, SolarWinds was just an acute case of a very common ailment: supply chain risk.

Today, no organization is an island. Businesses and organizations rely every day on a complex web of software and services to operate—from climate control and physical access to managed services providers, as well as cloud-based storage and applications, and, more and more, Internet of Things (IoT) connected devices to streamline operations and service (even fish tanks.[1]) Unfortunately, as that web of third-party software and service providers expands, so do the risks they pose to enterprise operations and business continuity by providing actors with additional vectors to attack to gain access to your organization's network or data.

> Supply chain attacks and compromises are potent because they exploit a common, non-technical vulnerability in almost every modern organization: a lack of visibility into the security of their supply chain.

Organizations that evaluate third-party providers have many options to assess that organization's offerings, financial health, and leadership. But they have no easy way to assess the cybersecurity posture of the organization including its product and service offerings, internal operations, and public-facing infrastructure. The level of effort to assess the supply chain is large-scale and complex and typical methods are reactive, under-resourced, and focused on non-cyber aspects.[2] To fully comprehend the entire attack surface of your ecosystem, you need continuous situational awareness of your supply chain.

THE SUPPLY CHAIN VISIBILITY GAP

Why is it so difficult for organizations to discern between supply chain providers that observe cybersecurity best practices and those that don't? For one thing, traditional information security practices draw a strong line around IT assets and

[1] https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

[2] https://www.mckinsey.com/business-functions/operations/our-insights/supply-chain-risk-management-is-back

services that are owned versus those that belong to their supply chain or third-party providers.

For security monitoring, legacy security controls at most organizations were designed and deployed to manage threats to physical IT assets and perimeterized IT environments. The typical castle and moat approach. From network and application firewalls to gateway and desktop anti-malware detection to intrusion detection and data leak prevention tools, the goal of most IT security products is to detect and block threats to IT assets that are owned and managed by the organization. This protection model works for many, common threats. Attackers who are attempting to take over a critical web application server using Structured Query Language (SQL) injection attacks are readily stopped by application firewalls. Email messages containing ransomware disguised as email attachments might be blocked by an email gateway, or execution of the malware could be thwarted by desktop anti-malware products.

Cyber criminals, nation state hackers, and other malicious actors recognize that the lack of visibility into the supply chain provides an opening for them. By pivoting to the supply chain, they have found a gaping hole in the external attack surface, a way to circumvent gatekeepers—taking advantage of trusted business partners and suppliers. In the SolarWinds incident, attackers saw an opportunity in the supply chain to exploit trusted connections to deliver malicious code, gaining access to and exfiltrating sensitive information, such as organizational emails at the Department of the Treasury.[3]

This lack of visibility won't be solved by having a risk scorecard, one-time security assessment, or periodic audits of supply chain vendors and third-party providers. Organizations cannot act on 100,000-foot-high security ratings. To truly improve security down an organization's supply chain, one must have specific, actionable intelligence and continuous monitoring of supply chain practices and IT assets that expose their organization to risk.

Even with the assistance of continuous monitoring services, organizations are often are at a loss to identify the third-party IT assets that pose a risk to their customers and data. For example, security researchers like Chris Vickery have made a career of scouring cloud-hosting services like Rackspace, Google, and Amazon AWS for unsecured or lightly protected repositories of sensitive data. More often than not, the data was released to, and then exposed by, third parties providing narrowly targeted services like marketing, data analytics, and other business operations. As an attack vector, cloud-based infrastructure and the data it stores on behalf of customers has increased as more and more organizations move to cloud-based options. For example, data breaches from cloud infrastructure of customer sensitive data increased 50% in 2019 over 2018 as a result of under-trained employees, malicious insiders, compromised account credentials, and misconfiguration issues.[4]

[3] https://www.crn.com/news/security/top-treasury-email-accounts-exposed-in-solarwinds-hack-report

[4] https://www.securitymagazine.com/articles/94036-anatomy-of-data-breach-in-cloud-generation

APPLYING THREAT INTELLIGENCE TO THIRD-PARTY RISK

The expanding external attack surface requires companies to think differently about how they manage these risks and vulnerabilities. That's where threat intelligence comes into play, as it complements on-network and off-network security controls.

The information and data that is the foundation of threat intelligence might come from external sources or be extracted from internal monitors and detection tools. However, the intelligence itself is the end product of focused analysis of relevant pieces of data and other assembled information. Today, cyber threat intelligence services are an increasingly common element of comprehensive cyber risk and security plans, extending security monitoring beyond the corporate perimeter to encompass a wider range of potential targets and threats within the ecosystem.

Properly applied, threat intelligence services complement and augment existing controls. A company informed by threat intelligence is better able to mitigate risk to themselves. For example, a threat intelligence feed from an industry ISAC (Information Sharing and Analysis Center) could tip you off to a pattern of network scanning identified among peer organizations that might indicate the early stages of a hacking attempt or warn you about a sector-specific threat targeting a vulnerability in a common platform. That, in turn, might re-prioritize business operations to reduce risk, such as vulnerability scanning, patching, and remediation efforts internally. Or, an intelligence feed might identify stolen credentials for employees that might prompt extra scrutiny of ongoing or passed user sessions, while prompting a wholesale upgrade of password and authentication practices.

TUNE OUT THE NOISE & PRIORITIZE WITH THREAT INTELLIGENCE

Done right, threat intelligence is a powerful tool for identifying and addressing major risks to your organization from any third party with access to your assets. There can be, however, *"too much of a good thing."*

Done wrong, too much data runs the risk of overwhelming your IT security team with *"noise"* in the form of false alarms and security notifications that are not actionable or of limited operational application to your organization. That's increasingly common as organizations outsource multiple business critical functions to supply chain providers who might support thousands of other customers.

Vendors with deep expertise in threat intelligence know threat intelligence informs priorities and enables analysts combing through incidents to find the needles in the haystack most relevant to your organization. Leveraging a threat intelligence platform that can group or categorize your supply chain or third-party providers based on organizational requirements (i.e., all of the finance department's providers in one group and all of the communications department's providers in another) can help clarify and prioritize threat intelligence alerts. Threat intelligence should provide contextualization of risks to facilitate holistic, risk-based decision making and inform business operations and risk remediation efforts.

A HACKER'S VIEW OF THE SUPPLY CHAIN

How can threat intelligence be applied to supply chain networks and providers? The first step is to develop a detailed internet *"footprint"* of each member of one's supply chain. This provides a key baseline of the potential external attack surface for an organization.

Next, this footprint should be layered with threat intelligence to provide an adversary's view of the organization from the public-facing internet. During this information gathering process, key, public-facing IT assets are identified and analyzed for each asset, further assessment and analysis can determine whether it is running software with exploitable vulnerabilities or is otherwise a risk factor. Even more, this can be done passively and unintrusively, without direct engagement with one's supply chain.

Together, a supplier's internet topology layered with threat intelligence will provide an organization with a detailed map of the supplier's network infrastructure, including important cybersecurity details such as open ports, exposed services, existing vulnerabilities, and more. This threat-informed footprint gives organizations the visibility they need into assessing their exposure to threats from a supply chain member's vulnerabilities.

The pay-off is better visibility into the supply chain's security posture so one's organization can better protect and defend itself against third-party compromises. Much attention is paid to Advanced Persistent Threat (APT) actors such as nation-state groups. But the truth is, the most effective threat actors often succeed by attacking *"low-hanging fruit"* at victim organizations. For example, improperly configured and publicly addressable devices might exhibit inferred vulnerabilities such as expired digital certificates and open Telnet or File Transfer Protocol (FTP) ports that are easy access points for would-be attackers. External actors who can gain a foothold on these devices typically use publicly-available exploits to elevate their level of privilege on a system and move laterally to higher value IT assets and accounts.

This *"outside-in view"*, layered with critical threat intelligence, allows organizations to narrow their defense and remediation efforts from the deep sea of *"what's out there"* in the cyber underground to the much more important category of the *"supply chain risks directly impacting my organization."* ■

LookingGlass™ Supply Chain and External Attack Surface Monitoring

Supply chain risk tools should make your organization more informed and efficient, not less. That's why LookingGlass's scoutPRIME, a global attack surface management solution, captures more than just point-in-time information. Supported by customizable continuous risk monitoring, threat intelligence feeds, and tailored real-time alerts, security teams and executive management have constant visibility into risk factors across their operational ecosystem's attack surface, versus being reliant on yesterday's third-party provider scorecards.

SCALABLE, CONTINUOUS MONITORING

While it is useful to have a picture of your third-party risk exposure at a point-in-time, today's threats (and therefore risk) are ever-changing. A weekly or monthly risk report can prove useful in some scenarios, but it is only a snapshot of third-party risk at that moment. If, for example, such a report is issued hours before the disclosure of a critical, remotely exploitable hole in a common open source platform, that report is unavoidably out-of-date by the time it is read.

For Chief Information or Security Officers and IT security leads who need to translate risk to other C-level executives, corporate boards, or even Congressional members, intermittent scorecard-style risk ratings are unlikely to lead to productive conversations as they (by design) omit the information that is of most interest to those audiences: what is the organization's security posture at this moment? Beyond that, executives and other stakeholders want to understand what steps have been taken to mitigate identified threats. Equally important to them is to understand how those mitigations have affected the risk posture of the organization.

That's why organizations require continuous monitoring of each third-party vendor's network, including any domain names and IP addresses for indicators of compromise, infection, or illicit use that may increase the organization's risk.

Such outward indicators are varied and constantly evolve. Among other things, LookingGlass solutions monitor for risk indicators such as malware hosting or distribution from a monitored organization's network, including infection by computer viruses or botnet activity. LookingGlass continually assesses whether the monitored third-party organization's network or IT assets are part of a malicious Command-and-Control (C2) network associated with malware or botnets.

Beyond that, LookingGlass can also identify outward signs of vulnerability, even in the absence of malicious activity. For example, we scan public-facing IT assets for known vulnerabilities, exposed ports, or expired certificates that indicate poor cybersecurity hygiene.

REAL-TIME ALERTING AND DRILL DOWN TOOLS

Our solution offers unique drill-down capabilities allowing your teams to find the needle in the haystack in a very loud, cluttered environment. Security teams don't need one more thing that goes ding. What they need is knowledge around the immediate source of a problem and where it is. This enables teams to pivot from wasting hours determining *"where's the vulnerability"* and gathering context around it to doing actual work to fix a vulnerability.

LookingGlass' unique drill down capabilities enable the discovery of specific element details around the following threats:

EVIDENCE OF SYSTEM COMPROMISE

Malware Hosting/Distribution: Assets observed hosting or distributing malware

Virus/Botnet Infection: Assets infected by a virus or botnet

Command-and-Control (C2) activity: Networks with C2 activity or communication associated to malware, botnets, or ransomware

Malicious/Scanning Behavior: Network presence of malicious behavior or scanning activities

Spam: Spamming or other similar behavior

Questionable Asset Use: Assets being used to route our disguise the origination of traffic (e.g., Tor exit node, proxy, VPN, etc.)

Hosting Phishing Activity: Hosting of phishing activity, fake branded websites, etc.

SYSTEM VULNERABILITIES

Observable Application Vulnerabilities: Specific system flaws or out-of-date software versions with known security issues

Open Ports: Open system ports such as TCP and UDP

SSL Certificate Information: Status, currency, and other details of security certificates found on the organization's systems

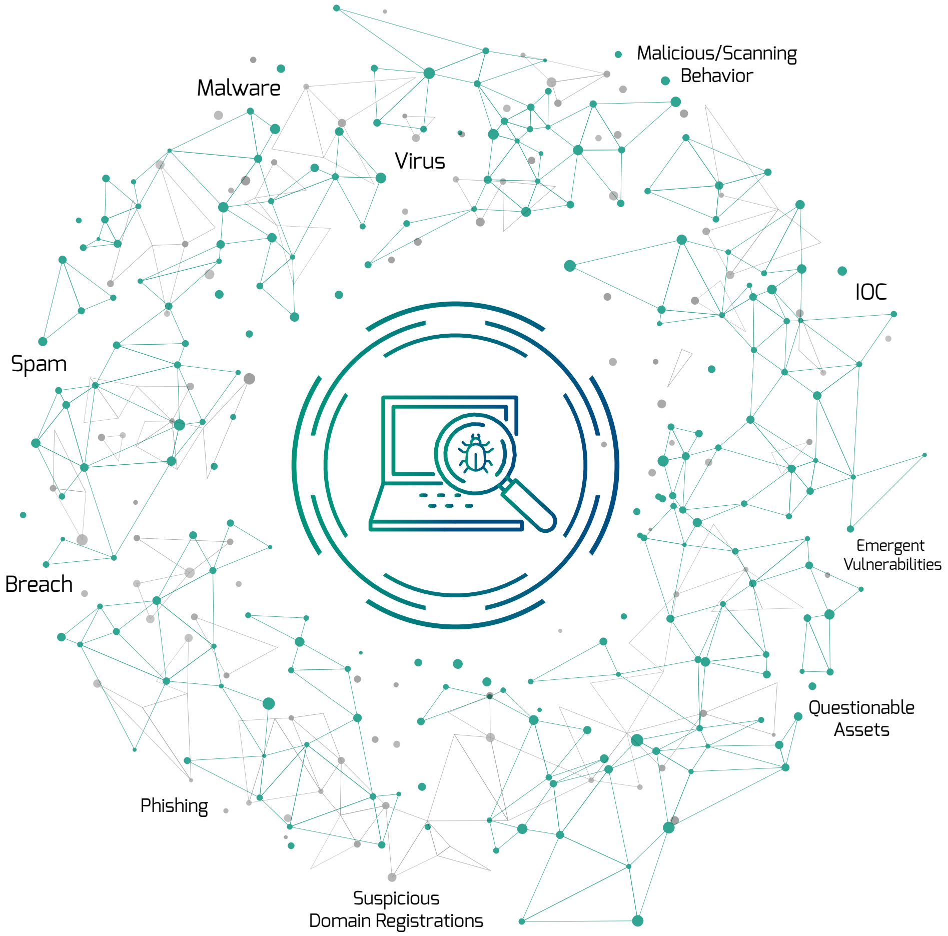
OPEN SOURCE INTELLIGENCE

Domain Portfolio and Spear Phishing Risk: Identify domain threats like typo-squatting and lookalike domains commonly used for phishing, social engineering, and Business Email Compromise

Reported Breach or Vulnerability: Near real-time alerts indicating if any third party vendor announces a data breach— publicly reported by the vendor (to a regulatory body) and claimed by the perpetrators

In addition, we provide customers with near real-time notifications of new threats and risks that appear on monitored networks. Alerting ensures that your IT organization is kept abreast of the latest developments as they relate to your organization's assets and risks.

LookingGlass's monitoring, notification, and investigation tools allow your team to move beyond alerts and warnings to identify and remediate the source of a threat to your organization's network, IT assets, data, and employees. Coupled with API-based connections to third-party investigation and incident response tools, your security team is notified of emerging and potential risks so they can immediately initiate effective response and remediation actions.



THREAT AND RISK REPORTING

Finally, LookingGlass provides customers with a wide range of reporting options that make it easy to collect and analyze third-party threat intelligence. These reports promote visibility into the work being accomplished by your teams, as well as accountability around what security responses are working, what aren't, and what could be improved upon.

Not to mention, built-in reporting makes complex measurements such as organizational threat posture easy to grasp, as well as aids in the process of informing decision makers, executives, and board members about third party risk. ■

Conclusion and Recommendations

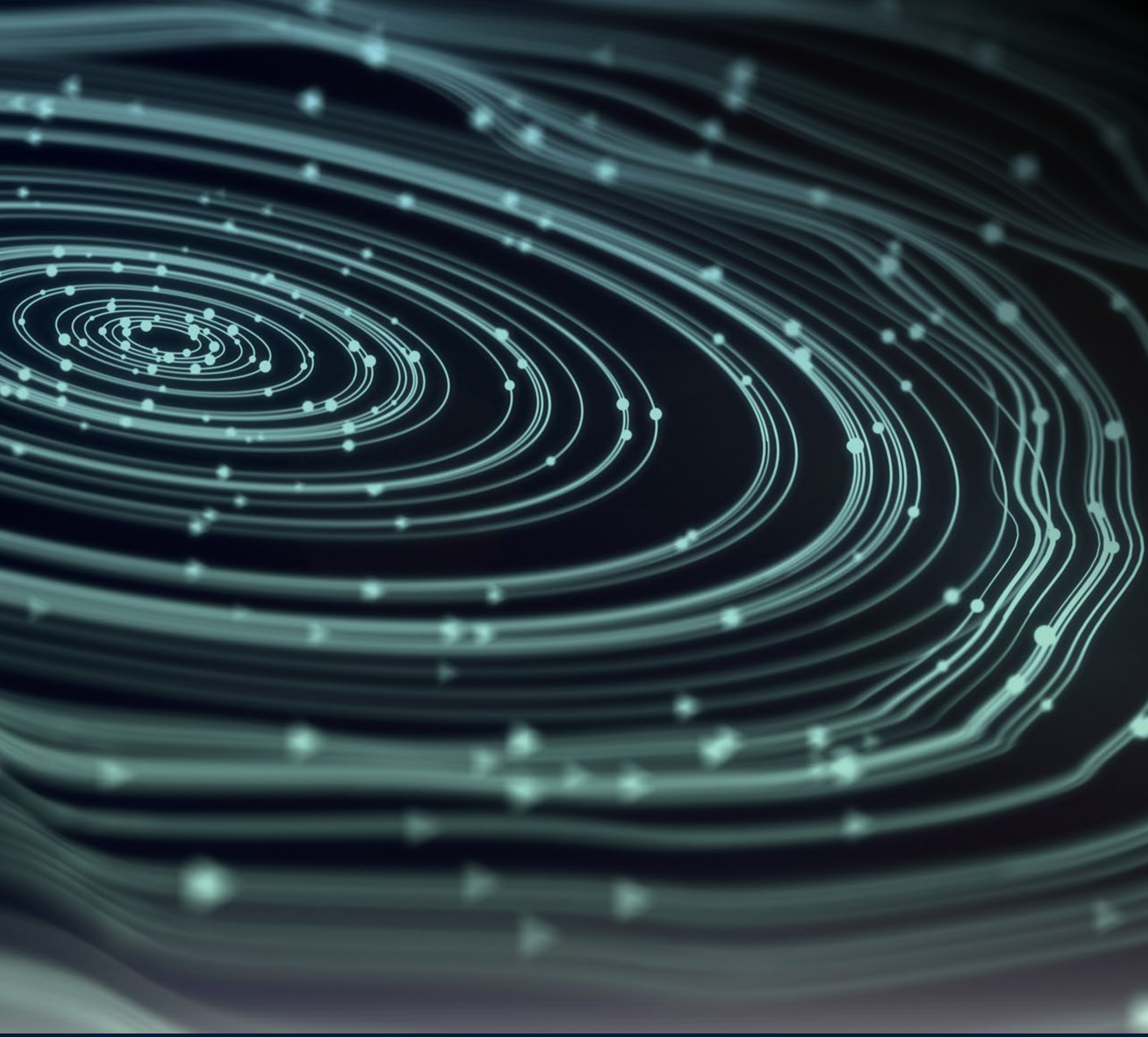
Managing information security requirements on its own is difficult enough. Extending that purview to the scores or hundreds of third parties that an organization transacts business with may seem like a Herculean task. Still, the unavoidable truth is that supply chain cyber risk is a real and growing threat to many organizations. It is no longer safe to simply ask suppliers, contractors, and other third-party providers to fill out a risk and security questionnaire, when your continued operations and mission objectives rely on their security just as much as your own.

With that in mind, monitoring one's supply chain and third parties for cyber risk should be a core component of every organization's information security program, regardless of industry. Organizations need holistic assessments of their supply chain that capture both the outward security posture of those entities and less easily measured indicators, such as the security of hosted and cloud-based IT assets and data. It's not enough to receive a point-in-time scorecard without the deeper analysis or actionable intelligence to remedy the risk and exposures.

Continuous monitoring and timely alerting that enables IT staff to respond within hours instead of days are now non-negotiable.

LookingGlass's platform is purposefully designed to provide just this mix of features so you can assess and manage supply chain and third-party risk information at scale. Our unique footprinting capability gives your IT security staff an *"adversary's view"* of your third parties, so you can truly understand any vulnerable supply chain network dependencies, allowing you to get ahead of third-party risks and breaches.

If you are interested in learning more about how LookingGlass can help you see your supply chain's vulnerabilities, **contact LookingGlass at** info@lookingglasscyber.com. ▪



LOOKINGGLASS

LookingGlass develops cybersecurity solutions that empower organizations to meet their missions with tailored, actionable threat intelligence and threat mitigation capabilities that move at machine speed. By linking the risks and vulnerabilities from an organization's external attack surface to customized threat actor models, LookingGlass provides a more complete view of cyber risk and enables systematic definition and deployment of mitigations to defend against the threats that matter. For more than a decade, the most advanced organizations in the world have trusted LookingGlass to help them protect financial systems, ensure telecommunications are cyber-resilient, and safeguard national security interests.

Learn more at **http://www.LookingGlassCyber.com/**