SIDEKICK SECURITY

DATA SHEET

THIRD-PARTY & SUPPLY CHAIN RISK MANAGEMENT

KEY BENEFITS

Align your security program to the risks and opportunities that truly matter to your organization. In short, start actually reducing risk instead of finding things you can't do anything about.

Drive compliance requirements since TPRM exists as a basic requirement in almost every major control framework.

Identify risks across your whole ecosystem of third party suppliers and SaaS tools, including the points of interconnection between them all where visibility typically slips through the cracks.

YOUR CHALLENGE

Your organization relies on third parties to scale, innovate, and operate. Questionnaires and SBOMs trying to answer the question, "Is this company safe to work with?" are not helping, it's also wasting time and presenting you with data you can't do anything about. This problem cuts across SaaS tools, vendors, COTS tools, and more. Ultimately, you need to address risks that are directly in your control.

OUR SOLUTION

Sidekick's Third Party Risk Management flips the script on the traditional approach of questionnaires and assessment of the vendors themselves. Instead, our approach starts by understanding how you actually use a vendor, the data they access, your operational reliance, integration complexity, and so on. Our program systematically focuses on applying security that is within your control to vendor solutions, taking actionable steps to reduce and manage risk. Our team helps you plan, assess, implement, and operate a program built for scale.

To us, security is all about enabling your mission. Third parties are a necessary part of that mission, so we think about their risk in two main ways:

AT THE VENDOR

Part of the risk rightly lies within the vendor environment or tool directly. This type of assessment can be streamlined and scaled.

IN YOUR ENVIRONMENT

An outsized majority of the risk which is often ignored lies within the way you use, integrate, configure a vendor or their solution.

All of Sidekick's services are designed to scale and ultimately be connected to everything else you do. We believe that point solutions create more work and problems than they solve.

Why Choose Sidekick?

Sidekick's clients benefit from a diverse pool of experts, including former CISOs, Directors, Staff Engineers, Architects, Privacy, and GRC Leads. We have worked with organizations of all types, from government agencies to publicly traded international companies to startups. We have also worked across a diverse set of industries, giving us insight into the unique challenges posed by regulation, org structure and complexity, resource constraints, and threats.

Pair that expertise with a chief focus on your success. That starts with an understanding of your business, needs, and goals so that we can integrate effectively. You can rely on your team at Sidekick to ask the hard questions, get strategic guidance as well as tactical remediation advice, work closely with your teams, and help make you successful through your cybersecurity program.

Our bigger picture is your organization's strategic mission.

Who Needs These services?

- **Organizations** that want to move past the standard questionnaire-based approach that plagues teams across the world start truly managing their risk and becoming resilient.
- **Security teams** that are looking to start bringing real security practices to third parties and tool deployments in their organization so they are ready to harden and deal with incidents.
- **Compliance teams** that need to independently attest to their third-party and supply chain risk management programs to a customer or key stakeholder.
- **Executive and Board teams** that are looking to manage the strategic risk of their third-party ecosystem, avoiding some of the massive disruptions that have occurred from recent third-party breaches and exploited risks.

Deliverables

Our deliverables are not standardized because your needs and organizational context aren't standardized. There are several throughlines in our engagement model:

- **Maturity assessments** are performed as part of the independent program attestation process.
- **Incident and Continuity Plans** are jointly developed to make sure that you are prepared for any disruption in your supply chain.
- **Full Spectrum Reports** about your key suppliers and partners so you have the insight you need to make effective decisions.
- **Capability** is where the rubber meets the road. When we step in to harden your portfolio of third-party applications we're taking your security controls and scaling them horizontally so you aren't operating with gaps.