

Third Party Manor



A haunted tour of the vendors you already let in



CHAPTER ONE

The Pumpkin Patch



The pumpkin was the finest in the patch on the day it was picked, and it looked the same every night after. Inside, it was quietly rotting, and only a lantern that shines beneath the skin could tell.

Vendors that change after approval

A vendor tends to look its best on the day it is assessed. The questionnaire has just been answered and the certificates are current, because its security team had a reason to tidy up, and that snapshot stays on file until the next annual review.

In the months between, the vendor keeps changing. It might fall behind on patching, or move to a new host and leave a certificate expiring on a subdomain nobody remembers, and none of it reaches the questionnaire. Catching it earlier means looking at what the vendor exposes on the internet today and comparing it with what it reported when it was approved.

HOW PANORAYS LIGHTS IT

Panorays keeps testing the external assets of the vendors you monitor and alerts you when a vendor's cyber posture rating drops.

Panorays Continuous Monitoring

CHAPTER TWO

Ghosts in the Cloud



The great hall was empty when the lights went out. By midnight four ghosts were drifting between the curtains, one hugging a laptop and another clutching a company card, and nobody had let them in. A light swept across the room was the only thing that found them.

Shadow IT nobody onboarded

Nobody invites shadow IT in. A team starts a free trial on a Tuesday, or someone installs an AI note-taker that ends up joining every meeting, and because neither went through a vendor review, neither appears on the vendor list.

These tools spread because they solve a real problem faster than the approved route, which is why a policy rarely keeps them out on its own. The exposure sits in what they connect to, since a single sign-in grant can give an unknown supplier access to mail and files. The useful question is which suppliers already hold company data, and that list tends to run longer than the vendor register.

HOW PANORAYS LIGHTS IT

Panorays Supply Chain Discovery detects Shadow IT across your supply chain, and you can drill into the evidence for how each third party was detected.

Panorays Supply Chain Discovery

CHAPTER THREE

The Wolf in Vendor's Clothing



GENUINE

Self-assessed questionnaire, every box ticked



GENUINE

New contact this month, confirmed in writing



GENUINE

Temporary admin access, booked in advance



THE IMPOSTOR

Lookalike address, asks for every key and new bank details

Four guests came to dinner hoping for Dracula's castle key. Three of them looked strange, and one looked perfect: a polished gentleman from the payroll company. Only when the moonlight reached his gloves did they begin to split.

Suppliers that aren't who they say they are

Impersonation works because trust attaches to a name, and a name is the easiest thing to copy. An attacker borrows a real supplier's identity, writes from a lookalike address and asks for more than the real supplier ever needed, such as new bank details for the next invoice.

Appearance is a poor guide, because genuine suppliers also change in ways that look alarming, from a new contact after someone leaves to temporary admin access for a scheduled update. Telling the two apart depends on one record of which third parties you actually work with, who your contact is at each of them and what their contract covers.

HOW PANORAYS LIGHTS IT

Panorays Inventory consolidates all your third parties in one platform, even before you've defined their tiers, and tiers each one using Internal Questionnaires and a Cyber Posture Rating.

Panorays Inventory

CHAPTER FOUR

Something Brewing in the Stack



The Trusted
Crystal



The Poison
Mushroom



The Leaking
Vial



The Binding
Thorn



The Unmarked
Jar



The Memory
Honey

The witch was approved to cook from the old recipe, and for years the brew tasted the same. Then new jars began appearing on her shelf, and each went into the pot without a label. Only a taste under the lamp showed which ones had turned the brew.

AI added to your tech stack

A new AI tool rarely arrives as a new vendor. More often a supplier approved years ago switches on an AI feature in a routine release and starts sending customer data to a model provider you have never assessed, with the change noted only in an updated subprocessor list.

The approval on file then describes a product that has quietly changed. The risk depends on what each tool keeps and what it can reach, so a tool that remembers everything can be acceptable once you know who reads it, while a familiar plugin can ask for every system when it only needs one.

HOW PANORAYS LIGHTS IT

Panorays identifies and labels the suppliers using AI, even when vendors don't explicitly disclose it, and tiers each third party by its AI exposure.

Panorays Third-Party AI Risk Assessment

CHAPTER FIVE

Skeletons in the Server Closet



Something in the tower bedchamber had been rattling for weeks, and the owner swore the wardrobe was empty. When a lantern finally caught the gap in its door, two skeletons tumbled out. They had been in there far longer than anyone admitted.

Incidents nobody disclosed

An incident a vendor has not disclosed often leaves traces somewhere else first. A supplier can answer its annual questionnaire honestly and still leave out last spring's breach, while leaked credentials or the company's name on a ransomware group's leak site surface during the vendor's own investigation.

The vendor's account tends to arrive later, shaped by contracts and legal advice, so a program that only hears about incidents from the vendor hears about them on the vendor's schedule.

HOW PANORAYS LIGHTS IT

Panorays checks hacker forums and dark web marketplaces for mentions of your vendors, and alerts you to breaches and security changes in your third-party network.

Panorays Dark Web Insights

THE FINALE

The World Wide Web



Below the manor, the dungeon is strung with silk, and everything you met upstairs hangs from one web. In the dark the threads look separate. Hold up a light and every strand runs back to one spider at the center.

The suppliers behind your suppliers

Every vendor you assess depends on suppliers of its own, and many of them share the same few. A cloud provider or a single open-source library can sit behind dozens of your vendors, so one failure several steps down the chain can look like twenty separate incidents on the day it happens.

These fourth and Nth parties rarely appear in a contract and almost never fill in a questionnaire, which leaves them out of any program built on what vendors report about themselves. Mapping the shared dependencies is how a program finds the strand the whole web hangs from.

HOW PANORAYS LIGHTS IT

Panorays maps the hidden 4th and Nth parties behind your vendors and their relationships, and monitors them for cyber threats.

Panorays Nth-party discovery

MAKING IT OUT BY DAWN

Every risk came in through an open door



Third Party Manor



*Every vendor you let in brought
something with it. Panorays helps you see
what came through the door.*

ABOUT PANORAYS

Panorays is a leading provider of third-party cyber risk management solutions, helping businesses optimize their defenses for each unique third-party relationship. Trusted by the most complex supply chains in the world, Panorays goes far beyond the generic third-party risk management solution with its AI-powered platform making assessments adaptable and more personalized.



panorays.com

