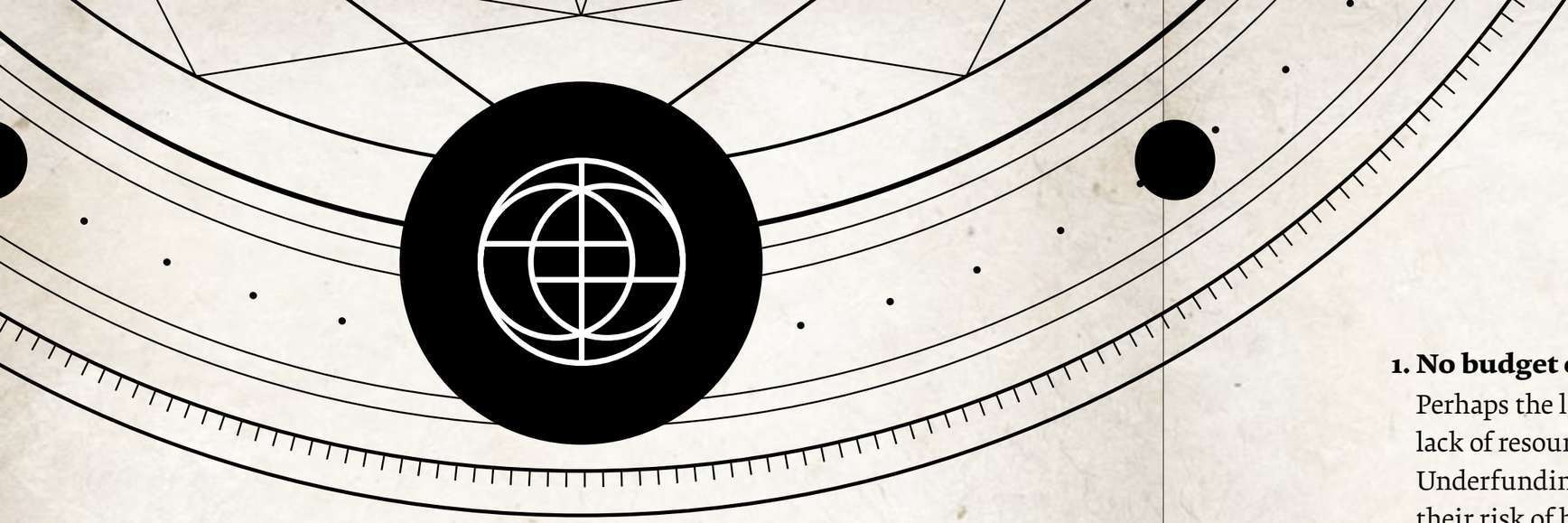
A WARLOCK'S GUIDE TO SELLING SECURITY SERVICES

ninjaOne

elcome to A Warlock's Guide to Selling Cybersecurity Services, a spellbook designed to help shopkeepers sell and build impactful security services using the vast power of magic. The world is full of monsters, many of which lie in wait for the chance to pounce at any vulnerability, leaving a wave of carnage in their path. As a **shopkeeper (MSP)**, you are able to provide important protection against potential threats with security services and inherent insight, all of which can be magnified with these mighty spells.

Cybercrime has grown immensely in the past few years, growing worldwide nearly 4x over the past six years, from 4.32 million attacks reported in 2016 to 16.81 million attacks reported in 2022. This also means that the estimated cost of cybercrime has skyrocketed over the past few years as well, increasing from $610 million in 2016 to a whopping $13.82 billion in 2022. Cybersecurity is something that every organization should invest in, but unfortunately, it's not always that easy.

Shopkeepers have a unique opportunity to protect a variety of businesses from these looming threats. But sometimes, it's not always as easy as putting together a solid portfolio of security offerings. Often, you'll need to build trust, communicate the importance of cybersecurity, and construct a solid defense system tailored to individual needs. The following spells are a must-have in every shopkeeper's back pocket.



Empathic Insight

LEVEL	SCHOOL	EFFECT
1st	Relationships	Trust

When first approaching a potential or existing customer on the value of cybersecurity, it's important to build an initial layer of trust. Many small businesses that you'll be working with have a unique set of pain points that prevent them from being able to invest their time and bandwidth into a comprehensive security plan.

With Empathic Insight, you gain an understanding of the pain points that these businesses struggle with. These pain points can impact the security services offered but can also help build a solid foundation of trust. Take the time to understand their needs and listen. Some of the pain points you may discover are:

1. **No budget or bandwidth for cybersecurity**
   Perhaps the largest obstacle for any small business is a lack of resources or bandwidth to devote to cybersecurity. Underfunding security is short-sighted and increases their risk of breach.

2. **Reactive rather than proactive**
   Small businesses often struggle with taking a proactive approach to cybersecurity, defaulting to a reactive stance. Unfortunately, this means they may overlook pressing security issues that could have thwarted a much more costly attack.

3. **Struggles with security system implementation**
   Tied to the lack of security resources, small businesses will often try to configure security systems without the guidance of an IT or security professional. These misconfigurations or deferred software patches can lead to easily exploited weaknesses.

4. **Lack of knowledge on current threats**
   With millions of attacks being launched worldwide every year, it's no wonder that investigating these threats is a full-time job. Many small businesses don't have the time to keep up with it all. Without a dedicated security resource, these businesses can find themselves in the dark.