Secureworks®

WHITE PAPER

Setting Expectations: Getting the Most from a Cybersecurity Vendor

How to Maximize Value from your Security Partnership

Cybersecurity's growth means more options for businesses to consider, but more doesn't always mean better. Partnering with a security vendor should strategically ease the day-to-day burden and help you scale your program. However, inefficiency and frustration can overwhelm the relationship if your needs don't align with your vendor's expertise. Unfortunately, the rate at which threats evolve and the lack of industry-wide standards increase the risk that businesses and vendors will end up in mismatched partnerships. Nevertheless, there are steps security pros can take to account for these challenges. Learn what you can do to ensure you're working with the right service provider and how to get the most from your partnership.

Cybersecurity's Primary Constant is Change

Getting optimal support from a cybersecurity vendor looks different today than it did 10 years ago. In fact, it looks different than five years – or even two years ago, and odds are, what works best for you today will look very different in a couple of years. Still relatively young, the security industry lacks the indelible rules and guidelines developed for well-established industries like manufacturing or finance. Cybersecurity playbooks perpetually change because business, technology, and the adversary change. Couple the evolving landscape with an oversaturated marketplace, and too often, security teams end up with a security services provider that simply does not match their needs.

Today, everything is more complex – more data, more threats, more attack surface, more choices, more integrations. There are infinite combinations of environments, needs, services, and technologies. This complexity is contributing to the increase in vendor-customer mismatches.

Tip 1: The reality is that not every business need can be addressed by any security vendor in the market, so getting aligned with your vendor at the start will create a more beneficial partnership.

In-House Security Tools – Should They Stay or Should They Go?

A challenge many organizations face when working with a vendor deals with tools and technology. When should you be open to new tools a service provider recommends or requires? When should you stick with what you've got? Security goals have to align with the vendor's capabilities, but they must also factor in the boundaries of the organization.

Sometimes – more often than you might think – getting the most from your vendor means adapting to recommendations that require you to change tools or technologies. That's not possible for every business, and in some cases, it isn't the right move or the right time. However, an organization's willingness and ability to be flexible is a key factor to netting more value from a trusted security partner. In short, when the service provider offers well-defined, measurable, and enforceable outcomes that align to your goals, you're likely to get more from your vendor by focusing on the results versus what tools are used to yield them.

Today, everything is more complex – more data, more threats, more attack surface, more choices, more integrations. There are infinite combinations of environments, needs, services, and technologies. This complexity is contributing to the increase in vendor-customer mismatches.

It's often instinctual to want your security vendor to work around your business, but a flexible partner doesn't necessarily translate to better results. The fact is, some industries don't benefit by adapting to the end user's preferences, and when that criteria is unnecessarily prioritized, it creates a breeding ground for bad disciplines. Some flexibility from your vendor is important, but when it becomes center stage, you could be leaving measurable value on the table.

Some industries don't benefit by adapting to the end user's preferences, and when that criteria is unnecessarily prioritized, it creates a breeding ground for bad disciplines.

Of course, sometimes changing tools is simply not an option, and in cases like this, it's better to have a vendor that can work with your tools. These scenarios may include:


Small or new security teams


Recent substantial investment made in new tools


Lack of dedicated security personnel


Awareness of a new risk the team isn't staffed to address


Prioritized relationship with existing tech provider

Tip 2: Mature security providers will often have a limited list of supported tools and technologies based on their ability to deliver consistent outcomes. It's worth considering the vendor's experience and keeping an open mind about their supported tools.

Recognizing Red Flags to Find the Right Relationship

It bears repeating that getting the most out of your cybersecurity vendor is dependent upon – at least in part – selecting the right partner that fundamentally understands your needs and has the accompanying skills to deliver the right support. The crowded marketplace presents buyers with endless choices, but navigating these options comes with its own challenges. Although the vetting process will vary depending upon your needs and timeframe, here are three red flags to consider when going through the evaluation process:

1. Overemphasis on Technology Solutions

There is no doubt technology plays an important role in cybersecurity today, but technology alone is rarely, if ever, the security silver bullet many claim it to be. Technology can be a tremendous asset to your team, but if vendor representatives answer all your concerns with, "Our tool does that" and offer no examples, then they could be overpromising. Similarly, pay attention to their use of the terms 'AI' and 'machine learning.' Again, AI and machine learning can help address security issues, but if the terms are used interchangeably or they cannot offer specific details or examples, you might wonder if it's a core competency.

At Secureworks, our philosophy is centered around customer success, and to deliver, buyers must understand what our technologies can do, what they can't, and when services and technology work best hand-in-hand.

2. Vague Process Descriptions

Yes, you want to understand capabilities, but it's just as important to understand how vendors function and how they'll work with your organization. If the way they operate is incongruent with your organization's structure and culture, you'll spend more time addressing frustrations than optimizing value.

Secureworks has been a highly rated services provider by industry analysts for 10+ years, and one of the main benefits is that organizations can and often do get primed on our capabilities from third party analysts before they speak with us, giving us more time with businesses to focus on compatibility.

3. Redirecting the Conversation

This one's pretty simple. If a vendor does not answer your questions with specificity, it might indicate a gap between what they offer and what you need. If the conversation keeps coming back to a solution that doesn't really address the problem, overtly bringing the conversation back to your needs may reveal a mismatch. That does not mean the solution is bad (although it might be). If a family of five opts for a minivan, it doesn't mean a sedan is a bad vehicle. It might simply mean you require specific features that can help narrow your search for something that better meets your needs.

The deep experience Secureworks has acquired across many IT environments for 20+ years has allowed us to find productive and flexible ways to work with diverse organizations, and we still may not be the right fit for every need for every business. Do we want to partner with you? Absolutely. Do we think we can provide better outcomes? We do. But if we discover a mismatch in the vetting process, it's a disservice to all involved not to address it candidly.

Tip 3: Selecting the right security service provider is like dating. The best thing you can do is know yourself first. Know what you need. Know your deal-breakers. Know where you're flexible and where you're not. With the option pool this large, you can't wait to be impressed and base your decision on a gut reaction.

Secureworks has been a highly rated services provider by industry analysts for 10+ years, and one of the main benefits is that organizations can and often do get primed on our capabilities from third party analysts before they speak with us, giving us more time with businesses to focus on compatibility.

Getting the Most From Your Cybersecurity Vendor

Once you have selected your security services provider, dividing the work in a way that boosts the support you get will enable your team to do more. By implementing these best practices, you'll set your team up for an effective partnership that will help keep you all moving in the same direction.

1. Map the division of labor based on your needs. Partner responsibilities will likely fall into one of the following three domains: security operations (SecOps), security engineering, or security architecture. Smaller teams may not have a division of labor that matches the provider's operations, but mapping the team members' skills based around these domains will help you get the most value out of your partner.
2. Regular communication is a cornerstone of a strong partnership. Security is an evolving industry that sometimes requires course correction. Structure plans for collaboration and work distribution with a regular cadence of checkpoints to gain and maintain alignment on the following:
   - Governance
   - Emergency response
   - Reviews and progress reporting
   - Service-level agreements
3. Take the time to adapt your team's operational procedures and responsibilities to best match the service from your vendor. You've hired a partner based on an informed analysis of your needs and desired outcomes. Continuing to do what you did yesterday and analyzing the differences between what you've done and what your partner recommends often leads to inefficiencies that reduce value.
4. By all means, ask questions if you have concerns. Business and security both get easily derailed by lack of communication and lack of transparency. When in-house or third-party security teams receive conflicting information, progress slows or worse – teams act in silos and create misalignment within the program.

Take the time to adapt your team's operational procedures and responsibilities to best match the service from your vendor. You've hired a partner based on an informed analysis of your needs and desired outcomes.

The Value You Get Shouldn't Change Even When the Industry Does

Cybersecurity is rooted in adversarial science. Unlike more established industries that have gradual and predictable changes, security providers are adapting to industry and business changes without losing focus on an ever-evolving adversary. In the last two decades, Secureworks has helped organizations of all shapes and sizes. We've seen adversaries evolve their tactics and motives, working collaboratively and backed by considerable resources. But historical context can be a valuable tool when preparing for the future. Each year, our security teams conduct 2,500+ consulting engagements and 1,300+ incident response engagements. Getting the most from a security provider means that as your business and security team change, your partner is agile enough to change with you so that you can operate uninterrupted.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp