Looking for a New Security Technology? Choose a Partner, not a Vendor



Previously, I borrowed the concept of carcinization from convergent evolution and applied it to security to talk about how security tools have evolved over time so that product categories are no longer clearly defined. When the walls between endpoint detection and response (EDR) tools and network security technologies begin to crumble, and when categories like extended detection and response (XDR) and threat detection, investigation and response (TDIR) platforms collide, everything starts to sound the same.

How can teams cut through the noise and confusion to find a solution that best meets their needs?

An important area of differentiation to evaluate when you make your next security investment is the vendor’s effectiveness when it comes to customer success. Great customer support is the foundation and includes responsiveness and timeliness, but

knowledgeability is also important to help you get the value you expect.

Buyer beware

When you start to evaluate solutions, here are three considerations:

1. Start with the process. Technology should not dictate how things should be done. What's more, the team may not have the skills or capabilities to use the technology effectively, or they may not like the approach being used.

A lot of companies focus on selling technology, but as a buyer you don't have to lead with that, nor should you. Instead, focus on the outcome you are trying to achieve, which is to improve your security operations, and the steps to get there. Sure, technology is important, but remember it's part of the people, process and technology triad. As such, it is one component of an overall offering that should enable your processes and improve your people, not drive process and create complexities for your people. For example, some cybersecurity solutions may require security teams to change frameworks or risk scoring mechanisms to model and assess threats, which can hamper implementation and security effectiveness.

Instead, start with the process that the technology should enable and make sure the technology has the flexibility to support that. It still may require some user training (which I'll get to later), but it shouldn't require an entire redesign of workflows and processes to make the technology successful in your organization. That level of effort and retraining significantly delays time to value for the organization and it won't help your staff grow and scale as individuals.

2. Look for quick wins. Achieving faster time to value requires understanding the end goal but also the steps to get

there. When you eat the elephant in chunks you can get quick wins which help build momentum and trust within the team and also help with internal communication and reporting on the return on the investment. You're getting value from the tool but also building confidence and goodwill among other stakeholders within the organization.

Start by containing the scope and defining specific use cases. For example, if ultimately you want to integrate with six different tools because the value of the tool is not just with your team but with others in your company, choose a use case where you integrate with one to start and show the value. Then integrate with the others after. This could be integrating threat feeds into your security operations platform to normalize and prioritize data for action. And then, after that, integrating with your firewalls for proactive protection.

3. Understand the training options. Going back to the classic triad, we've already talked about technology and process. Now it's time to talk about people and training, which is critical and should be part of a vendor's customer success offerings.

Training should be available in multiple formats and form factors: instructor-led/in-person or instructor-led/virtual, depending on what works best for your business model. Self-service should also be offered, which is not only great for initial training but can be utilized on demand when there is turnover or your team grows. Additionally, follow-on training on more advanced capabilities helps ensure the organization derives increasing value from the investment and staff continues their professional development, working towards credits or certifications.

Customer success should be on every security team's checklist when evaluating new security solutions. Ultimately, you're looking for a partner, not a vendor, and a solution that enables people and process; not a technology that dictates how

things need to be done. As you work through these three areas – the process you're enabling, how you'll achieve quick wins, and the training available – you'll know pretty quickly if you've found the right partner.

https://www.securityweek.com/looking-for-a-new-security-technology-choose-a-partner-not-a-vendor/