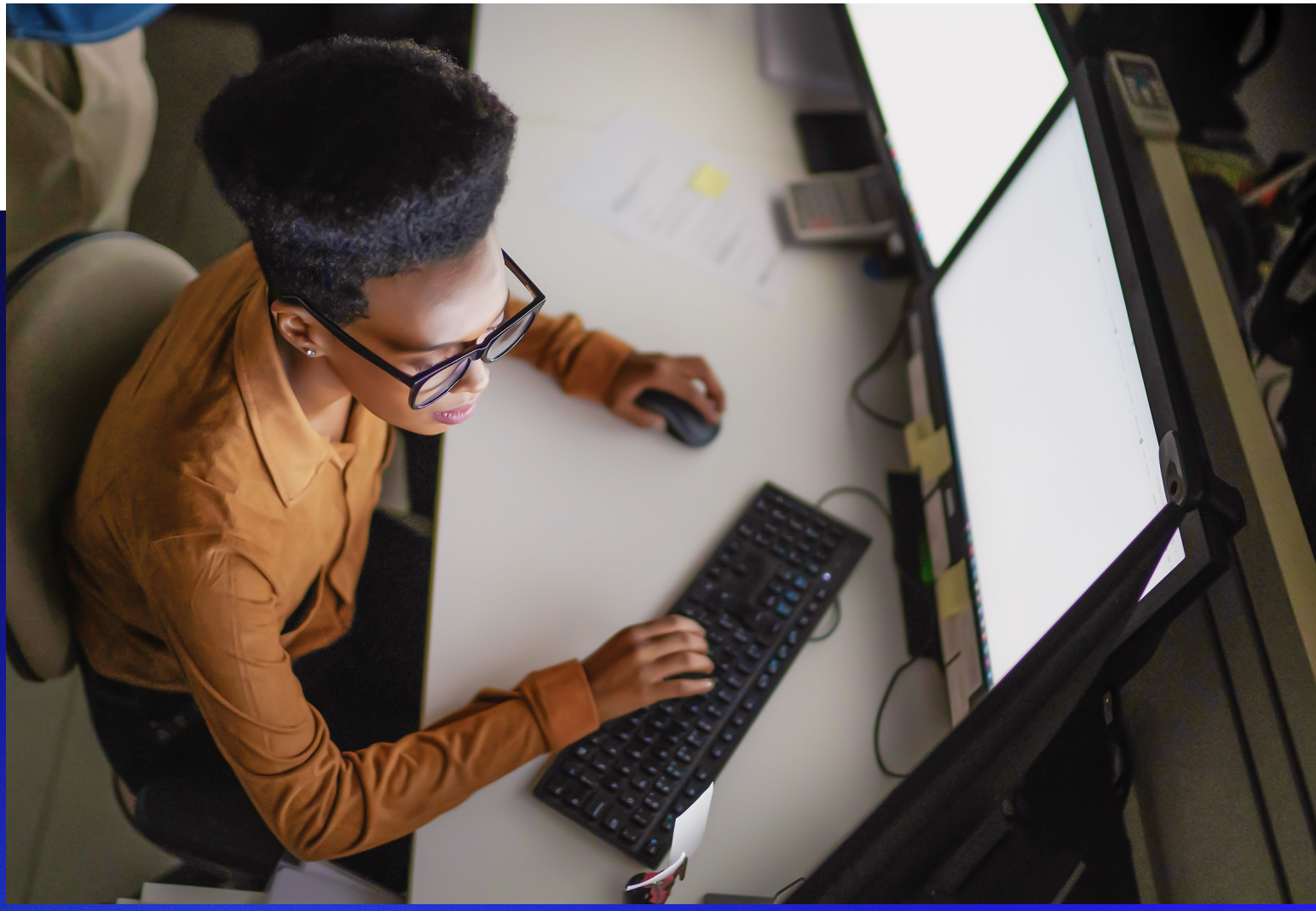
Secureworks®

WHITE PAPER

10 Questions to Ask When You Inherit a Cybersecurity Solution

Ensure Your Security Solutions Align With Your Organizational Strategy



When you're new to a company, there's always a learning curve involved. For those in the security organization, this curve can be steep, particularly when you are inheriting an existing solution. There are several key issues to address and questions you'll want to ask if you find yourself in this situation. Approaching this challenge in a formulaic, strategic manner is the best way to ensure your organization stays protected while you evaluate the current security solutions.

There are a few scenarios that would lead to an organization inheriting a cybersecurity solution. A merger or acquisition is a common one, and a situation in which you would likely be inheriting more than one solution, one from each company. In some scenarios, the decision rests with the Board who may choose a provider they have familiarity with despite what the security team has identified. Other reasons might be that you're new to a company or new security leadership has joined. In some cases, a company may have simply discovered an older legacy platform that had been long neglected due to organizational sprawl and security stack complexity. Whatever the scenario, a previously implemented security solution needs evaluation in the context of the overall security program.

Inheriting a cybersecurity solution presents a number of challenges to the business. The primary obstacle is that when you inherit a solution, it requires a revisit of your strategy. Maybe you had plans to migrate to the cloud but now you have to use a hybrid or on-premise solution for the foreseeable future. This may cause frustration with the existing solution if it doesn't align with the strategy and security roadmap you had in mind. Further complicating things, if a CISO lacks confidence in a solution, this attitude will likely translate to the analysts who use it and other C-suite leaders who may require a view into it as well.

If you've inherited a cybersecurity solution and are facing similar challenges, this list of questions will help you address them in a measured way.

Once you understand what drives the business and ensure your team is aware of the expectations of their role, you can ask yourself whether there's room for the program to go from purely tactical or reactive to transformative and proactive.

10 Questions to Ask When You Inherit a Cybersecurity Solution

1. What drives your cybersecurity program?

Knowing the driving factors behind your cybersecurity program is an essential step in understanding the strategy and business decisions behind the existing solution. Is your organization's security program primarily driven by regulatory and compliance needs? Or is it one where business and risk conversations are happening simultaneously in real time? Once you understand what drives the business and ensure your team is aware of the expectations of their role, you can ask yourself whether there's room for the program to go from purely tactical or reactive to transformative and proactive.

2. How does the cybersecurity solution fit into your current strategy?

The answer to this question often depends on the age of the solution and the state of the business at the time it was first implemented. Since that time, perhaps your organization has started its journey to adopt a culture of digital transformation, or you're planning to migrate to the cloud and embrace a growth mindset. Having a complete picture of your current and future business and cyber strategy will help you evaluate the solution's long-term value.

3. What does the solution mean for your future roadmap?

Inheriting a solution often makes a cybersecurity program more reactive, with ad hoc processes and planning. It can also complicate an already complex tech stack that an organization may have been trying to streamline. Often, organizations struggle with analysts who may have a good grasp of security tools, but lack deep understanding of security fundamentals. This may cause issues if your talent is tied to a tool, but not connected to your larger vision. If your existing security solution was not built with the flexibility to grow with your future plans, it may not be the right fit for where you're headed as a business.

4. How will people utilize this solution?

It's important to know whether you have the internal resources who understand how to use and support the existing technology. If a tool requires a lot of administration or management, it could pull your tactical talent away from more critical tasks. When it comes to those who are managing the day-to-day security operations, changes to tools and processes can be very difficult. You may get pushback from someone on your team who's a champion of the legacy solution. On the other hand, if you don't have experts knowledgeable on a particular solution, that may be a sign that you're not using it to its full capacity and that it's no longer providing enough value to your security program.

5. What are the processes that are going to be supported by the solution?

Take a look at your processes to ensure they are compatible with and can "talk" to the solution. For example, if you're documenting standard operating procedure (SOP) for a process that doesn't address what the solution will do, that's a sign of a disconnect.

6. How does the solution correlate to my existing stack?

You must understand the interdependency of the solution with the rest of your stack. For example, consider a data loss prevention (DLP) tool: Do you have a tool that tags your information? If not, how is the tool that protects the information going to know if something is a confidential document? Lack of tool correlation could mean more manual work for analysts, and with it, the potential for missed threats. Knowing how one tool depends on the others will tell you where your gaps are so you can begin fixing them.

7. Would getting rid of the solution negatively impact the business in some way?

This is a risk management exercise that should be done with careful consideration with input from cross-functional stakeholders. It's possible that an inherited solution is embedded in a business process that's critical for running your operation. Understand the repercussions of phasing out a solution, compared with the challenges of keeping it, and make a risk-based and data-informed decision.

8. How would the solution impact your internal and external customers?

Beyond the impact to your security team, you must also think about how an existing solution is used by or affects the rest of your company staff, as well as your customer base. If the solution enables you to fulfill your obligations and responsibilities to certain parties, this holds some value.

9. Can I justify this solution to the rest of the business?

Cybersecurity must have a role and voice at the leadership table. A CISO should have a strong enough understanding of the solution in order to adequately communicate its benefits (or risks) to the Board, C-suite, or other leaders throughout the business. These stakeholders may also want a less technical explanation, so being able to relay how a solution affects the bottom line is another important consideration. If analysts are struggling to report on the solution, or the CISO feels they're not getting what they need to report up, that indicates an issue.

10. What are some signs that incorporating the inherited solution into the business may be more trouble than it's worth?

Aggregating your answers to the questions above should allow you to see whether keeping an existing solution is the right decision. If the solution creates more work for your analysts due to administration or a barrage of alerts, this could be a red flag. Further, if it doesn't sync with your company's future culture and strategy – or have the flexibility to grow into this vision – that's a strong indicator of trouble.

How a Managed Security Services Provider (MSSP) Can Help

Making sense of an inherited solution and how it may or may not fit into your business is a big undertaking, particularly if you already have a complex security stack. Partnering with a trusted vendor can help your organization make the tactical adjustments you need. An experienced MSSP can provide a holistic assessment of your security program, including all the tools and technology you've inherited. They should also be able to offer advice on how to consolidate your stack and streamline your security operations to best fit your organizational needs. This can lift a huge burden off the shoulders of your in-house resources if they are being spread thin chasing alerts or wasting time on non-critical tasks. An MSSP may be able to bring in artificial intelligence (AI) and machine learning solutions to complement your existing infrastructure.

As much as security relies on tools, having the right people to manage them is just as important. Finding the right security partner that understands your goals and can help you identify risks and opportunities in your program will help improve your overall security and provide benefits throughout the business.

Ultimately, when you inherit a solution, remember not to make any knee-jerk reactions without fully considering the business implications. Try to understand why it was implemented in the first place, rather than immediately looking for reasons to discontinue it. Cybersecurity works best when all related stakeholders embrace it. Whatever solutions you decide on need to be made with the entire organization in mind.

Cybersecurity works best when all related stakeholders embrace it. Whatever solutions you decide on need to be made with the entire organization in mind.

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