SecurityScorecard

Because Trust Means Everything

4 Four factors to consider when evaluating a cybersecurity partner

How Should You Evaluate a Partner You Work With?

Cybersecurity risk is no longer just the security team's concern; in fact, there's a growing call for executives and boards to have more cybersecurity experience and take on more responsibility to improve their organizations' cyber posture. Leaders need solutions to address threats while also making investments in automation and other technologies to improve their cyber resilience. But how do you know you can trust the people, the technology, and the data?

This guide can help you make informed choices about business partners, through evaluating four critical areas:

TRUST

Can you trust the data you are using to make decisions is transparent, actionable, trusted, and guaranteed?

TRUSTED LEADER

Does this company have notable relationships with experts in your industry, recognition from key publications and analyst communities; well as positive peer reviews?

TRUSTED SOLUTION OF CHOICE

Is this company proven in the field and helping to transform organizations with complex cybersecurity challenges?

TRUSTED METRICS

Does your partner help promote trust and provide value to the C-suite and board by translating cyber risk into easy-to-understand KPIs; while shoring up additional investments and resources to protect an organization's cybersecurity posture?

[1] U.S. Securities and Exchange Commission, Cybersecurity.

Key Factor 1
Do you trust the data?

When evaluating a company to work with, one of the most important factors to consider is how trusted, reliable, and accurate the data is. Companies should look for partners that use trusted industry methods such as scanners, web crawlers, machine learning, honeypots, and other in-house tools to ensure data accuracy and, more importantly, data ownership over the signals being collected. A partner that can constantly refresh and scan for new digital assets gives you the most accurate information to help boost your cyber resilience.

Beyond how the data is sourced, it's important to know how a partner maintains credibility to surface reliable and accurate insights about your overall cybersecurity risk. A trusted partner will make detailed information easily available about the methodology, formulas, and collection mechanisms behind their data. This includes being transparent about accuracy, how scores are calculated, and more.

Furthermore, when considering working with a partner, find out whether or not it stands by the data it delivers. Does the partner provide a guarantee against incidents should your organization suffer from a cyber event? If so, will your organization be eligible for free digital forensics and incident response services to help minimize the impact of a breach.

Your organization has large amounts of cybersecurity data that make it impossible to sort through manually. To scale this process, you need a partner that can help reduce these manual tasks, find vulnerabilities so you don't have to, and provide the right level of transparency so that you can make informed decisions based on real-time information to stay one step ahead of threats.

Key Factor 2
Are you working with an industry leader?

A good indication of a trusted company is that they have **recognition from key publications and analyst communities**

Everybody calls themselves an industry leader, but how can you know for sure? Being able to externally validate the security data and services offered by a partner you are considering is another important factor. Does this company have notable relationships with experts in your industry? A good indication of a trusted company is that they have recognition from key publications and analyst communities, including: Forrester, Gartner, Forbes, and InfoSec publications; as well as positive peer reviews on websites such as G2.com or Gartner Peer Insights.

Another indication of competency is finding out they work with Information Sharing and Analysis Centers (ISACs). ISACs can greatly enhance trust and validation within a company by providing a collaborative platform for organizations to share and exchange vital information related to cybersecurity threats and vulnerabilities. This collective effort aims to support the collective supply chains they form. By actively participating in an ISAC, companies demonstrate their commitment to cybersecurity and their willingness to collaborate with industry peers. This proactive approach not only enhances their own security posture but also establishes a sense of trust among customers, partners, and stakeholders.

True industry leaders understand the value of integrating with existing investments to extend the reach of your security stack; therefore, it's key to have a partner that can seamlessly integrate with other technology providers. A reputable cybersecurity partner understands the importance of collaboration and actively seeks partnerships with the most innovative technology organizations. By joining forces, they can collectively enhance their offerings and provide a more robust security solution to the companies they work with.

Key Factor 3

Can your partner help you quantify and translate your organization’s risk?

In order for your cybersecurity program to get adequate funding and stay effective, you need to be able to quantify risk and easily communicate it to the C-Suite and Board of Directors. Cybersecurity concerns are being treated more seriously than ever, especially in the face of new and anticipated government regulations (U.S. Securities and Exchange Commission regulations and the White House Cyber Strategy). Using cybersecurity ratings to not only quantify risk, but predict potential breaches, can help your company become more cyber resilient.

As you evaluate a partner, consider one that can:

- ✓ Automate and scale many of the functions of vendor risk management programs
- ✓ Managed cyber risk experts conserve valuable resources by helping you quickly discover and respond to incidents
- ✓ Contextualize cyber risk data into understandable terms to present to stakeholders

When regularly communicating cyber risk, your company can also demonstrate the value generated from existing security investments, which reinforces the importance of ongoing funding and support. When the Board comprehends the tangible benefits of security measures and sees how they align with business objectives, they are more likely to provide the necessary resources and budget to bolster cybersecurity defenses.

Key Factor 4

Is your partner proven in the field?

Whether it's working with partners in the public sector to assess the health of their cybersecurity environments, assisting companies as they audit their third-party vendors, or responding to cyber incidents, it's key to look for a partner that's always seeking to evolve, innovate, and enhance your organization's cyber resilience. Does the partner work with governments globally to protect critical infrastructure and assist regulatory agencies to make operations safer?

SecurityScorecard is the trusted must-have standard for measuring cybersecurity. Customers choose us not only for our approach and experience, but because we are the clear solution of choice in the marketplace. SecurityScorecard has over 50,000 customers worldwide in nearly every industry, and that number continues to grow.

We enable faster, better decisions and are trusted by:

- **70%** of the Fortune 1000 companies
- **8 out of the top 10** largest insurance companies in the world
- **9 out of the top 10** banking institutions
- **14** information Sharing and Analysis Centers (ISACs)
- **93** technology and integration partners

We'd love to help you transform the way you understand, measure, communicate, and reduce risk.

Learn how you can evaluate a partner you can trust

Trust means everything

FIND OUT MORE

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

United States: (800) 682-1707
International: +1(646) 809-2166