8 Signs You Need to Consolidate Your Cyber Protection

CYBERLEAF
Managed Cybersecurity Service

Cybersecurity can feel like a game of catch-up — every time a new vulnerability or attack vector is discovered, you have to find a solution or an expert to protect you from it. It's not an illusion; recent research from Check Point and Dimensional Research confirmed that 91% of global security leaders agree or strongly agree that cyber threats have grown more sophisticated over the past three years. It's easy to end up with lots of disparate tools in a configuration that's difficult to maintain.

The most effective action to take in this situation is to consolidate your environment and, if it makes sense, move to a cybersecurity-as-a-service solution.

To find out what's best for your business, look at the pain points listed below. If they sound familiar, it might be a good time to change the way you manage your cybersecurity practice.

☐ You're constantly training staff on how to use your solutions.

While figures vary, HackerOne found that mid-sized businesses use up to 60 different security tools. The more tools you have, the more difficult it is to onboard new team members, and the more likely it becomes that someone will make a mistake.

☐ You're creating policies across multiple solutions and products.

Creating security policies is a requirement for top-tier cyber protection. However, if you have too many security components in use, it can quickly become a headache. Defining workflows and standardizing policies across products from multiple vendors can prove difficult and time-consuming, and it's a recurring issue. Every time standards change (not to mention products), you have to figure out how to get all of your tools to act accordingly, slowing down the business and hampering your ability to react to threats.

☐ You're drudging through complex deployments.

The more tools you add to your environment, the more difficult it becomes to add the next one, especially when they come from different vendors. And a simple misconfiguration can easily leave part of your environment exposed, meaning that there isn't a way around this one. Then multiply that headache by the number of other tools that have to cooperate and collaborate with each other to truly secure your environment; it's a tough challenge to overcome.

☐ You're having to perform difficult, manual integrations.

This problem goes hand in hand with complex deployments. Vendors don't always build their solutions to play well with others, which means your team has to spend time teaching them to. Vendors advertise APIs, SDKs, and integrations, but each one has fine points that may not be readily apparent. Different terminology, design points, data formats, and methods complicate the effort. As with deployment, this also increases the risk of human error.

☐ Total Cost of Ownership (TCO) is too high.

Buying and maintaining the latest tools can put a massive dent in your organization's budget. And the purchase of the tools is only the beginning of the problem. Once purchased, you have to install, integrate, operate, train, and maintain, meaning that the majority of the Total Cost of Ownership (TCO) doesn't become clear until after the purchase. A high TCO is one of the best indicators that you need to consolidate what you have — if the cost of cyber protection is getting out of control, you need to find a way to lower it in order to keep doing business without risking a devastating cyber attack.

☐ Procurement is difficult.

If figuring out what you need for cyber protection is hard, making it actually work is Mount Everest. You might think purchasing a single vendor solution simplifies your life, but "Vendor lock-in" is practically a curse word in cybersecurity. Some vendors design their products to work together in an attempt to sell more to their customers, but can they really do everything well? That means you may not get what you need from your vendor, forcing you to choose between forgoing complete cyber protection or going through the hassle of figuring out how to acquire, implement, and integrate another tool into your environment.

☐ Compliance monitoring is hectic.

If your business faces regulatory requirements or deals with confidential information, especially in the form of PII, you have to adhere to a set of compliance standards. In a consolidated environment, you can quickly figure out whether or not your systems are compliant, but if you're part of the 98% of organizations surveyed in the aforementioned Dimensional Research study that uses multiple consoles, it can become a challenge.

☐ Your threat response is getting slowed down by your system.

A consolidated security approach makes it easy to respond to threats as they appear. If your system is cluttered or disjointed, the process is slowed down. Figuring out where a problem began becomes exponentially more difficult as you add tools to your cyber protection.

Conclusion

Less is more when it comes to cybersecurity. The more consolidated your tools are, the easier it is to manage and improve your practice. One way to reap the benefits of a robust cybersecurity practice without running over budget is to use a Cybersecurity-as-a-Service (CSaaS) provider like Cyberleaf.

Cyberleaf offers the highest levels of protection to customers from day one. Our experts do the heavy lifting of integrating world-class solutions together under a singular SIEM platform, and they can incorporate what you've already invested in to make sure your needs are met. If you're interested in an efficient, defense-in-depth approach to cybersecurity that's built for performance and ROI, sign up for a free assessment today.