

Should you BIY or BUY security?

Comparing build-it-yourself versus commercial IDS/IPS solutions for sustainable security



Contents

Executive summary	3
Creating sustainable cybersecurity solutions for your organization	4
Open-source intrusion detection and prevention solutions	5
Advantages of building your own IDS/IPS	5
Suricata	5
Bro	5
Considerations	6
Advantages of commercial solutions	7
Traditional commercial	7
Commercial open-source (Hybrid)	8
Conclusion	9

Executive summary

Creating sustainable cybersecurity solutions for your organization is challenging. Organizations building out security solutions often face the dilemma of build versus buy. Numerous open-source network security solutions are available, but what is really involved in building out a sustainable solution and is it the right choice for your team? This guide will help you evaluate various open source and commercial options and provide best practices and tips to get started, as well as guidance on how to plan and scope your project.





Creating sustainable cybersecurity solutions for your organization

Organizations planning out their security apparatus have much to consider, including: size of the organization, geographic diversity, type of information being protected and available resources. Inevitably, security organizations will be faced with the question of build vs. buy.

Generally, a security organization's goal should be to mitigate the most relevant cybersecurity risks facing the company. There is no one-size-fits-all approach. Successful teams will tailor strategy and programs to what their lines of business need. This guide will discuss some of the challenges that businesses are facing today when developing their security strategies.

At first glance, cybersecurity might look like a technical problem requiring technical solutions. However, experienced teams know that the technological components address only part of the equation. It is important to remember that tools don't solve problems, people do. In fact, many security organizations suffer from too much technology and not enough process and in-house expertise, as well as growing operational expenses.

As time goes by, these tools accumulate and so does the information and the data they produce.

Many security organizations underestimate the total cost of ownership when they embark on solving problems. The typical lifecycle goes something like this: A threat or risk is identified, and the security team tries to mitigate the situation through the procurement of a shiny new "tool." The team implements the new tool and attempts to operationalize it. Then, a new threat or risk is identified, and the same process is followed, rinse and repeat. Growing the number of people to manage these tools at a sustainable pace can be both costly and challenging, especially when there is a shortage of competent security professionals. Since you cannot accumulate your tool operators at a fast enough pace, corners are cut, and tools are not properly operationalized. Procedures and documentation are not defined or well thought out, maintenance items, such as backups and system monitoring, are bypassed. As time goes by, these tools accumulate and so does the information and the data they produce. You end up with a tremendous amount of technical debt. When it comes to the selection of appropriate mature intrusion detection or intrusion prevention systems (IDS/IPS) there are many choices on the market.

One of the first decisions you will need to make is whether to go with an open-source, commercial or hybrid solution. If you have more of a do-it-yourself mindset then your choice may seem easy, but if you are not sure, then it is time to consider the business drivers, the security organization's goals, your budget and how much support the initiative has from the key decision makers.

Open-source intrusion detection and prevention solutions

Although up and coming solutions such as Bro-IDS provide some complementary feature sets, most purists will use one of the two most popular open-source solutions as their core engine: Snort or Suricata.

Snort has been the de facto standard in this space for quite some time. In fact, many analysts still use the Snort rule signature syntax throughout the information security community. Suricata was born from the need to improve processing throughput beyond what Snort offers. Suricata allows for high-performance deployments through its 64-bit, multi-threaded architecture, its approach to integrating IP reputation signatures and how it natively processes signatures based on application (instead of the traditional network protocol and port). Suricata also offers other powerful capabilities, including extracting specific file types for further analysis from the network traffic it monitors and logging useful elements, such as SSL certificates and DNS requests. Both applications are good choices, but if performance and the ability to detect more advanced threats at a lower cost is a priority, Suricata should be at the top of your list.

Advantages of building your own IDS/IPS

Over the past decade, we have seen a convergence of the firewall and IDS. However, commercial firewalls can get excessively expensive, especially when you must pay for additional intrusion detection module licenses. If that does not noticeably constrain your wallet, try to scale out a deployment across other locations and/or internal areas of your infrastructure that may not benefit from full firewall capabilities.

Most companies place their firewalls at key egress/ingress points, such as the internet connection or partner choke points. However, companies seeking a full coverage solution will also want to consider monitoring what is happening at remote locations (such as retail stores, medical centers/clinics, branches, restaurants, etc.), and internally on their core networks in addition to the perimeter. All this adds up to having to procure a lot of features at high cost.

Many unified NGFW/IPS systems also suffer substantial performance degradation when IDS or IPS capabilities are activated. For example, if you need to inspect 10 Gbps of traffic and have a 10 Gig NGFW, the IPS performance may only operate at 2–4 Gbps. That means either dropped packets, limited traffic inspected or over-buying firewall capabilities to get the requisite IPS throughput; something to keep in mind if you are evaluating a combined solution.

If going the build-it-yourself (BIY) route, you should consider where you will need coverage, how many sensors you will need to scale to, and the full maintenance lifecycle including: signature updates, software updates, operating system patching, general system administration, etc. If you only need a small deployment, the BIY approach is likely a good fit. Here are some links to get you started:

Suricata — download directly from the Open Information Security Foundation (OISF) for the latest updates and documentation; <https://oisf.net>
The OISF also hosts training and conferences to help you get started or improve your Suricata deployments.

Bro — While focusing on network security monitoring, Bro provides a comprehensive platform for more general network traffic analysis as well; <https://bro.org/download>

Another resource is Security Onion, which is a combined Open-Source technology Linux distro package. It includes Suricata, Snort and Bro, amongst other technologies. It may be a solid option to get you jump started on a BIY project. Just beware of the fact that this is a packaged installer, not an integrated system. Each tool will still need to be managed and operated independently; [Security Onion Solutions. github.io/security-onion](https://github.io/security-onion)

Considerations

Before diving right into a BIY security project, take some time to define your strategy.

- Why are you building this and what do you hope to achieve?
- Define specific goals and consider what metrics you can use to measure success.
- Consider all the costs; look beyond the base hardware and ancillary software to project anticipated time required to deploy and manage the systems.
- What will you use for threat intelligence? Free tools are available, such as Emerging Threats Open, but the coverage is limited. For more comprehensive rulesets, there may be a fee involved.
- Who will keep the systems updated or repair devices that fail?
- How many people will ultimately use the solution? Consider upstream integrations like SIEM operators and security analysts. Who will manage technical support calls?
- Plan for sustainability; how critical will your monitoring system be to your security infrastructure, and what are the consequences if a device fails? What turnaround times will you need to assure management for system restoration, and do you have the resources available to execute properly?
- What expertise do you need to manage all those elements and who will be responsible for them?

Often initial success with these projects drives initiatives to invest more time into building it out. Eventually, the solution evolves to a more widely deployed and depended on tool and it is heavily integrated into other processes. In some instances, teams realize that scalability, performance and operationalizing certain aspects of the solution have become challenging or burdensome. Examples include optimizing the solution to keep up with the performance requirements in certain high-volume locations, or system administration and health monitoring for a large number of devices. Compounding the problem can be challenges around managing and deploying rules and policies, along with consistency around configuration management.





Quantifying the time, costs and operational requirements may give you the data you need to justify additional resources for the project to ensure its success.

Walking through the planning scenarios above will help you prepare for a more sustainable project and avoid major surprises down the road. Quantifying the time, costs and operational requirements may give you the data you need to justify additional resources for the project to ensure its success.

Advantages of commercial solutions

The advantages of commercial solutions versus open source vary, but some common things include:

- Integrated features
- Optimized performance
- Consistent and reliable updates
- Threat intelligence updates
- Usability enhancements
- Simplified deployment
- Centralized configuration, operation and maintenance
- Warranty
- Technical support
- Detailed documentation

At this point you might be trying to figure out which camp you fall into; commercial, build it yourself or hybrid (commercial open-source). Cost is often a driving factor, as is control over the platform (ability to customize and change things to suit your needs). The fact is there is no-one-size-fits-all, but here are some guidelines to help you determine if a commercial solution is a better option for you, and if so, whether a legacy system or hybrid solution would be best.

Traditional commercial

1. Reliable performance is a must-have
2. Minimize the number of vendors in the security portfolio
3. Centralized management
4. Highly proprietary infrastructure requiring seamless integration
5. Proprietary threat intelligence is preferred
6. Monitoring internal activity or remote locations is less important
7. IPS capabilities can be licensed from your firewall vendor and the costs and speeds to meet your requirements
8. Customization/flexibility is less important than conforming to existing infrastructure
9. Budget is not a determining factor

Commercial open-source (Hybrid)

1. Reliable performance is a must-have
2. Numerous locations to monitor
3. Centralized management and operation
4. Expand existing BIY solution and utilize existing tool knowledge
5. Building and constantly maintaining a large open-source deployment isn't realistic with existing resources
6. Minimize transitional pain by importing similar policies and configurations from existing open-source technologies
7. Flexibility/open standards to incorporate new detection methodologies and grow easily over time
8. Leverage open-source community intelligence while having the flexibility of adding additional threat intelligence feeds
9. Share threat intelligence internally or with industry partners through STIX and TAXII
10. Affordable VM and cloud options to expand the solution
11. Budget is a significant consideration

Experienced security teams that have already identified a need for an intrusion system evaluate several factors before they dive into the implementation phase of a solution. These considerations may include: hardware, operating system, signature and rule management, integration into existing security operating center workflows, troubleshooting, scalability around performance, centralized management and technical solution support.

They also periodically evaluate the skills they have and play to their strengths. Asking provocative questions such as:

- *What are we good at?*
- *Which processes are repeatable and might be good candidates for optimization?*
- *What are our prioritized goals?*
- *Should our security organization spend its time performing tasks that can be offloaded to automation, other internal teams, and/or an external business partner?*

Introspective approaches like this are important. They can provide clarity on what to focus on and which path(s) optimize resources and mitigate risk.

[Security](#)
[OpenText Blogs](#)

[Threat Detection
and Response](#)
[OpenText Solutions](#)

Conclusion

Some smaller organizations are better off building an intrusion system themselves and sustaining that for the long term. It might make sense for medium and large organizations to start off with an in-house solution, especially when a full solution commitment cannot be made from the start. However, as scalability becomes a priority, it is prudent to consider migration to a commercial solution.

It comes down to the total cost of ownership for any of these security tools and the goals you have in place for network monitoring and threat defense. Organizations should be encouraged to perform their due diligence before they dive into deploying any system. In most cases, a free trial or proof of concept deployment is available to evaluate different approaches and see what resonates with your team. Even if you are set on building it yourself, it never hurts to show that you have done your homework and evaluated different options. Who knows, you might be surprised to find a commercial solution has fairly commensurate costs, alleviates a lot of your issues and delivers a solution a lot faster.

About the author

Michael Newborn is the former Chief Security Officer for Bloomberg BNA. He is an expert in cyber program development and execution with more than 17 years of experience driving information security breakthroughs across various sectors. Newborn owns and serves as the Principal Consultant for Newborn Associates, a boutique firm advising small-, medium- and large-business clients on cyber program operations.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: [opentext.com](https://www.opentext.com).

Connect with us:

- [OpenText CEO Mark Barrenechea's blog](#)
- [Twitter](#) | [LinkedIn](#)