Getty Images

SECURITY > THREAT MANAGEMENT

Protecting Your Environment with Open Source Security Tools

Open source security tools have come a long way and can be as effective as propriety tools. However, there can be disadvantages to using just open source tools, so a mixed model may be the best route to go.

Karen D. Schwartz | Jun 20, 2020

While open source tools continue to become a more integral part of many

answer is yes, but it's complicated. It depends on how experienced your IT staff is, how much you're willing to spend and your tolerance for risk.

In most cases, open source security tools are as effective or nearly as effective as proprietary tools, said Owen Pendlebury, chair of the global board of directors at the nonprofit Open Web Application Security Project (OWASP) Foundation and senior manager of penetration testing at Deloitte. That's because, unlike proprietary tools, open source tools are maintained by an active and involved community, many of them experts.

In fact, open source security has come a long way in a short time. Over the past decade, vendors have banded together to promote open source security, often collaborating with consortiums. One of these consortiums, the Open Cybersecurity Alliance (OCA), continues to push the envelope. With a mission of improving interoperability in the cybersecurity ecosystem, the OCA in February introduced an open source messaging framework for security tools to help with data and command sharing between cybersecurity software. There are other active organizations as well, such as the nonprofit and global CERT community, which is funding the development of open source security tools.

All of these factors taken together have changed the open source security landscape. There are more and better tools, and they are only getting better.

"We have seen a fairly rapid evolution in both the number and quality of open source security tools compared to even 12 or 18 months ago," said Jason Keirstead, chief architect of threat management at IBM Security. "I would have given you a very different answer 24 to 36 months ago."

There are many benefits to using open source security tools. Because they are

release schedule, which means there is a risk of backdoors being inserted by bad actors.

Although the code is typically reviewed by many people, it can still contain vulnerabilities. In fact, open source tools are subject to the same types of vulnerabilities as proprietary tools. The sheer size of code bases with millions of lines of code can make them difficult to detect, for example. Vulnerabilities also can be introduced as part of poor coding practices building on legacy code bases that may have been developed without security in mind, or using third-party libraries that have known vulnerabilities or misconfigurations, Pendlebury said.

And it's not always cheaper. Although open source tools are free, that doesn't mean there isn't a cost; it's important to factor in the time it takes to integrate the tools into your environment and continually maintain them.

"When you are using purely open source tools, a lot of the support, integration and maintenance falls on you, the implementer," Keirstead said. "We have data that shows that cybersecurity teams are hiring as many people to integrate the tools they have as they are hiring to actually do security operations. If that's already the case using existing supported commercial tools, imagine what increased workload there is when there is no commercial support for those tools and it's all community-based and you have to figure it out for yourself."

While there are plenty of security functions ideal for open source tools, it may pay to pick and choose. One area that may not be a good choice is anything around desktop or endpoint security.

"In most other places on the network, open source and paid products will do roughly the same job. A firewall is a firewall; it will either let someone in or it won't

What to Choose?

There are plenty of areas where using open source security tools can make sense, however. Firewalls are a good example. Many small and medium-sized companies, for example, use open source tools such as pfSense. The same is true of security information and event management (SIEM) systems like OSSIM and log aggregation tools like Graylog.

These tools can get definitely get the job done, but they don't come with all of the features of paid tools. For example, an open source firewall is perfectly functional, but getting a dashboard and more automation usually requires the paid Pro version.

"If you use open source security tools, you have to do more work, so you are basically exchanging your budget for hands-on time and work in configuration," Gargiullo said.

As an example, Gargiullo points to the well-regarded intrusion detection and prevention tool OSSEC. While the tool is excellent and has plenty of features, it requires someone to manually add changed information to the configuration file. For example, a Windows update would require someone to update the configuration file with the new correct value for the files.

If none of this dissuades you, this might: There are more open source security tools than you might think, so it can be hard to find the right one for your organization. There are some good rules of thumb to follow, however.

"It takes a lot of research. First make sure you have a clear understanding of your

One way to tell if you have found a good tool is if it is supported by support companies. The most successful open source projects, Gargiullo said, have huge support communities around them.

Best of Both Worlds

Most companies will have the best success mixing and matching open source security tools with vendor tools. That's especially true of vendor tools that have been built on open source tools. In a way, it's the best of both worlds, Keirstead said. "You have

greater operational freedom and independence but also the stability and support of a major vendor that has built on open source and integrated it into their ecosystem," he said.

In most cases, it comes down to what your IT team is comfortable with, how much money you have to spend and how much risk you're willing to tolerate.

"If you have a reasonably technical IT team, you can probably do 90% or more of your security configuration using open source tools. In theory, you could do 100%," Gargiullo said.

Regardless of whether you choose open source, a mixed model or proprietary software, it's most important that you find the right tool for the job, Pendlebury said. Key questions to ask include:

- Does the solution do what I am looking for, and is it the primary or secondary

- What are the staffing requirements to manage and maintain the tool?

Once you have chosen your tools, make sure to document the control environment, create a log of libraries used, subscribe to threat bulletins and updates, and document the tools' functions so your security team can use them effectively. Other important tasks include developing processes for auditing and testing the software, receiving vulnerability and update information, and providing feedback to the community to keep the tools as effective as possible, Pendlebury said.