Software for vulnerability scanning is an essential resource for any company looking to defend its data and systems against online threats. Vulnerability scanners assist companies lower their risk of compromise by finding and fixing vulnerabilities.

Software for vulnerability scanners has two primary revenue models:

Subscription model: To access the vulnerability scanner software, users must pay a monthly or yearly charge. The most popular business model for vulnerability scanner software is this one since it gives the provider a consistent flow of income.

Per-scan model: Users of the vulnerability scanner software must pay a fee each time they scan their systems. Although less prevalent, this business model may be a good fit for companies that need to scan their systems only sometimes.

Vulnerability scanner software providers have various more avenues for making money besides the two primary business strategies. For instance, some providers provide extra services like training and consultation for vulnerability management. Add-on modules with extra functionalities, including scanning cloud resources or containerized apps, are sold by other companies.

Below is a more thorough explanation of every business model:

Model of subscription

The most popular revenue stream for vulnerability scanning software is the subscription model. Customers pay a monthly or yearly subscription to utilize the program under this approach. This charge usually covers the cost of support and maintenance in addition to the software itself.

There are several benefits to the subscription model for providers as well as customers. Customers no longer have to pay upfront for software and hardware since the subscription model offers a predictable pricing structure. Vendors may invest in the creation of new features and capabilities because the subscription model gives them a consistent flow of income.

Model per-scan

Though less popular than the subscription model, the per-scan model may be a useful choice for businesses that need to scan their systems only infrequently. Customers pay a fee under this approach each time they use the vulnerability scanner software to scan their systems.

There are several benefits to the per-scan approach for vendors and customers alike. Because they only pay for the scans they require, consumers benefit from a more flexible pricing structure under the per-scan approach. For software providers, the per-scan approach can help them bring in more money from businesses who aren't currently subscribing to their services.

Further sources of income

Vulnerability scanner software providers have various more avenues for making money besides the two primary business strategies. For instance, some providers provide extra services like training and consultation for vulnerability management. Add-on modules with extra functionalities, including scanning cloud resources or containerized apps, are sold by other companies.

Vendors of vulnerability scanner software can reach a larger consumer base and increase revenue by providing a range of goods and services.