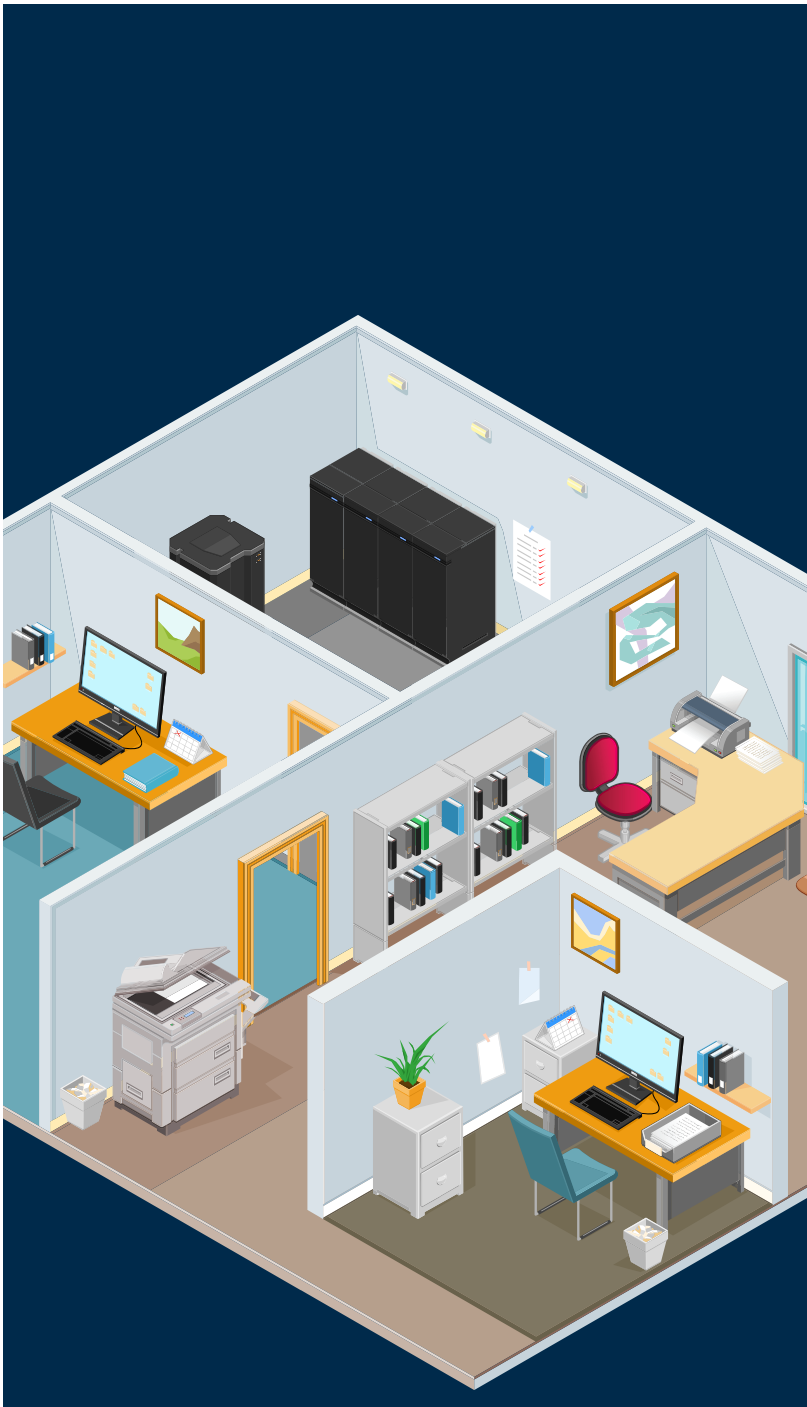
CLOUD **VS.** ON-PREMISES



VERACODE

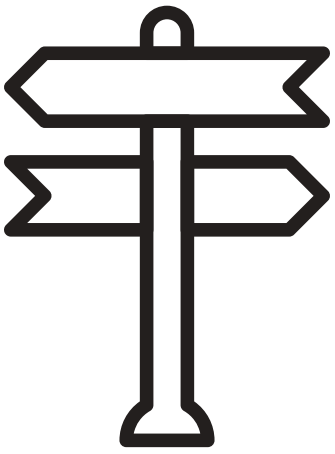
ON-PREMISES OR CLOUD-BASED APPLICATION SECURITY, WHAT'S RIGHT FOR YOU?

Once an enterprise decides to embark on an application security program, its next step is to determine what type of solution will work best for its requirements. In addition to the many techniques enterprises can use to assess the security of their applications, enterprises must also decide whether on-premises tools or a cloud-based service best fits their needs.

With on-premises tools, the enterprise's security team installs and maintains an application security tool and manages the application assessment process in-house. With a cloud-based service, there is no equipment on-site, and a third party manages the enterprise's application security assessment via the Internet.

Although the trend is toward cloud-based application security and away from on-premises tools, some organizations continue to use on-premises tools, or a combination of on-premises tools and a cloud-based service. This more traditional approach typically appeals to organizations uncomfortable uploading code to the cloud to be assessed, or that want or need the control afforded by on-premises tools.

In addition to the many techniques enterprises can use to assess the security of their applications, enterprises must also decide whether on-premises tools or a cloud-based service best fits their needs.



WHAT YOU GET WITH ON-PREMISES APPLICATION SECURITY TOOLS

An on-premises solution is the best bet for organizations that:

- Need extensive customization: For organizations that need extensive and complicated system customization and integrations, some cloud solutions cannot address their needs. Most cloud solutions are configurable, but not necessarily able to be heavily customized and integrated with existing systems. Although, the ability to customize and integrate cloud-based services is improving.

- Have to keep data on-site due to regulations: For some large organizations, their industry, clients or business mandates where corporate data is held, and moving any data to the cloud might not be an option. Some organizations also feel that the cloud is less secure than an on-premises tool and want to keep their data on-site. However, it is risky software, rather than the where data is stored, that adds unnecessary risk when using a third party, and organizations should be more concerned about the security of the development processes of third party partners rather than the security of the cloud. Regardless, for some organizations, keeping their data on-site remains a priority.

The cons of an on-premises solution include the following:

- Need in-house security expertise: On-premises tools typically require specialized expertise to install and run. The security experts who can install, configure and maintain these tools, as well as respond to the information they return, are expensive and in short supply.

- Cumbersome to scale: When an on-premises application security program needs to be scaled, enterprises frequently need to track down more of these hard-to-find security specialists, in addition to installing more servers.

- Not ideal for remote/disparate teams: Today's workforce is rarely located in one place, and the on-premises model makes it challenging to work seamlessly and consistently across disparate teams.

- High upfront costs: On-premises tools require significant upfront implementation and equipment costs.

WHAT YOU GET WITH A CLOUD-BASED APPLICATION SECURITY PROGRAM

A cloud-based service lets enterprises start immediately, without hiring more consultants or installing more servers and tools. It also allows enterprises with large and distributed development teams – even those that incorporate outside software companies – to more easily incorporate application security into their processes.

In addition, unlike an on-premises tool, a cloud-based service is continuously gathering more information, learning and improving. With this feature, it's less likely developers will get bogged down with false positives because the platform is continuously learning to adapt to evolving threats.

Finally, a cloud-based application security service allows an organization to easily scale its program to address its entire application landscape, even as it rapidly expands and evolves.

The following chart expands upon some of these differences between cloud and on-premises solutions.

CONSIDERATION	CLOUD	ON-PREMISES
IT Resources	Upgrades managed by vendor, reducing need for dedicated internal resources.	Internal IT support/sys admin needed, upgrades handled internally.
Software Investment	License fee, plus one recurring payment per month.	License fee, plus 20-25% per month for maintenance/support.
Hardware/Infrastructure Investment	Reliable Internet connection. For companies without sufficient bandwidth, cloud services will not be feasible.	Server hardware, software, data backups, storage, disaster recovery, remote access, network connectivity. Servers also need to be upgraded approximately every five years.
Scalability	Seamless and simple – no additional resources required.	Involves significant resources – a recent Forrester Research study that examined the Total Economic Impact® (TEI) of switching from an on-premises to a cloud-based application security found that an enterprise would spend an additional $5 million (including the addition of 15 FTEs) over three years to expand an on-premises application security solution to match the scale of a cloud-based solution.
Remote Location Support	Built-in.	Can be costly if lacking the network infrastructure to support multiple sites or geographic locations. Forrester Research found that one enterprise reduced its application security costs related to outsourced development from $70 per vulnerability to $10 per vulnerability when switching from an on-premises to a cloud-based application security solution.
Mobile Access	Available.	Not always possible.
Customization/Integration	Typically able to configure rather than heavily customize.	In-depth customization and integration possible.
Location of/Control Over Corporate Data	Must trust third party with data. Regulations in some industries will not allow data to be kept off-site.	Local control of corporate data.

For more details on this subject, check out our video survey of security professionals to hear their thoughts on cloud vs. on-premises solutions: Video Survey: Limitations of On-Premises Software Versus Cloud Solutions.