

PROS AND CONS:

On-Premises vs. Cloud-based Cybersecurity

Depending on your environment, there are lots of reasons you might think an on-premises cybersecurity solution is still the way to go. But, as business and IT needs change, there are a lot of reasons the cloud offers better scalability and flexibility, especially for managed service providers (MSPs). Here are some basic considerations for on-prem vs. cloud.

THE ON-PREMISES CYBERSECURITY MODEL



Customization

An on-premises solution provides IT teams with complete control over meeting compliance mandates.

Asset Awareness

Since data and applications are stored on servers in-house, IT teams always know the location of their data and assets.

IT Control

Organizations can fully customize and integrate systems to meet their specific business needs.



Scarcity of Talent

Security experts are in high demand.

Cost to Maintain a Security Team

Qualified security professionals earn up to \$98,350.¹

Limited Capacity and Scalability

On-prem systems often lack storage capacity, processing power, and scalability.

Resource Usage

On-prem solutions usually have a set fee, regardless of how much the business uses.



THE CASE FOR GOING CLOUD-BASED

Major Cost Efficiencies

Companies can engage the resources and expertise of a cloud-based security solutions provider, paying only for what they use.

Better Return on Investment

Cloud-based solutions allow organizations to take advantage of an OpEx model to reduce capital expenses, helping them realize greater cost benefits throughout the year.

More Flexible Solution Development

Businesses can rapidly adjust cloud computing capabilities to scale to the volume of internal and external threat information.

Greater Data Security

Cloud-based solutions can enable safer information sharing by combining analytics from multiple sources without compromising data security.

¹US Bureau of Labor Statistics, 2018