Examining the security of cloud-based vs. on-premise deployments

Is your data more protected in a cloud infrastructure?

Despite being several years into the cloud computing paradigm shift, there are still many businesses that are uncomfortable with the idea of a cloud-based infrastructure. This is understandable—every other week seems to bring a news story about a data breach. In a report published by KPMG, 30% of global senior executives said they have concerns related to the loss of data and privacy, while 26% are concerned with general security risks.\(^1\)

Still, it’s hard to deny the benefits of cloud computing. From cost savings and freedom from hardware constraints, to agility and always-current functionality, it’s no wonder that enterprise cloud adoption is on the rise.\(^2\)

Yet the question of security continues to be debated. Is it actually safer to entrust your mission-critical data off-premise? Read on for a point-by-point exploration and decide for yourself.

---

1. Examining the security of cloud-based vs. on-premise deployments
2. 30% of global senior executives have concerns related to the loss of data and privacy.\(^3\)
The following are viewpoints to consider as you explore migrating to a cloud infrastructure.

**Point**

On-premise infrastructure is more secure because it’s on-site.

If a company maintains a traditional in-house data center—replete with physical servers, chassis racks, and cooling fans—its IT team has complete control over the data. If an administrator chooses, he or she can keep data from ever leaving the server room.

If my servers are physically accessible, I can better protect them from viruses.

New security threats are not a large concern when your data center is housed on-site. The application of new security patches and software updates is completely under the control of your local IT staff, who can verify that virus signatures are kept up-to-date.

On-premise data centers are more reliable, because we can resolve all issues ourselves.

By owning and maintaining your own servers in your company’s own buildings, you can better ensure system uptime, which depends entirely on your maintenance. Your team can perform system checks at any time. If servers are farmed out to a third party, there may be a long queue if you ever need support.

**Counterpoint**

Most breaches are inside jobs, and a cloud system actually offers greater protection.

Security breaches due to unauthorized physical access to a cloud host’s data centers are incredibly rare. The most costly breaches come from within a company’s own firewalls, often from employees. Cloud hosting companies protect customers and alert them immediately about any disturbance. Plus, secure servers hosted in a variety of locations safeguard data better than the risks of a single location.

Cloud providers can rapidly deploy a fully-tested virus response to all customers—without your staff’s help.

A cloud provider that hosts hundreds of customers offers fast, thorough protection from emerging threats that you would never be able to feasibly manage on your own. Because the cloud host takes care of the time-consuming, tedious task of ensuring that virus signatures are up-to-date and security patches have been applied, your IT staff can focus on more profit-driven activities.

Cloud systems can better guarantee uptime because they experience fewer service disruptions and have 24/7/365 monitoring.

An IDC study of companies using cloud services showed that the benefits of the vendor’s scale and size led to significantly fewer disruptions and lower costs. In discussing leading cloud provider Amazon Web Services (AWS), IDC said: “End users benefited from fewer service disruptions and quicker recovery, reducing downtime by 72% and saving nearly $32,600 per application per year.”
Conclusion

Cloud vendors typically offer a much higher level of data center and virtual system security than most organizations can or will build out on their own. Leading cloud providers have made massive investments in the most advanced security tools and procedures available, which companies that choose cloud deployment can benefit from.

It’s telling that the world’s most security-obsessed organization, the U.S. Central Intelligence Agency (CIA), has a $600 million contract for cloud services with AWS. The agency rarely reveals what drives its security priorities; but from that evidence, one can conclude that cloud technology satisfies the highest possible security demands.

The bottom line? Cloud-based computing is often more secure than on-premise computing for businesses. It’s like upgrading your data’s vault from a hotel safe to the Federal Reserve.

“Using cloud services means that your data is better protected than if most of us tried to manage it on our own...Large-scale services are all much better than we are at avoiding data loss from gear failure, keeping software up to date, upgrading hardware, and constantly improving security.”

—Frank Gillett, Forrester Research
Actionable advice

- Only enlist a cloud infrastructure vendor with the highest level of verifiable security. Criteria include ISO 27001 certification; validation by the Payment Card Industry Security Standards Council; and U.S. Federal standards like FedRAMP.

- Be honest about your own IT team’s expertise and capacity. By delegating responsibility for cyber-attack response to full-time specialists at a cloud vendor, organizations can spare themselves a major source of cost and distraction.

- Make sure your cloud applications are compatible with the cloud infrastructure your vendor supports in terms of login credentials, authentication, and data encryption. Gaps can undermine the integrity and security of your applications. The more frequently your application vendor and cloud vendor have worked together, the less likely it is that there will be gaps.

Most progressive enterprises are knowledgeable about all of the different cloud service models (IaaS, PaaS, and SaaS), have researched the major vendors, have started executing on their cloud strategy.”

—Mike Kavis, Forbes

For more information please visit Infor CloudSuite ›