

6 ways cloud computing can support your security capabilities

Embracing cloud computing forces organizations to decide between the cost-effectiveness, scalability, and convenience of using a cloud environment or the comfort of keeping your data and applications hosted securely on your own servers. But is on-premise really more secure than cloud computing? Many experts say no. The following six factors will show why you can feel comfortable moving to cloud computing.

1 Security is expensive

Security costs money. Ask yourself: how much can my company actually afford? Deploying the necessary security for your on-premise datacenter is actually cost prohibitive, especially for small-and medium sized businesses. Achieving a level of security close to what hyperscalers can offer their customers is impractical.

2 Security requires significant staff resources

Similarly, security also requires more staffing resources. The large-scale cloud providers employ 24X7 security teams and a full security operations center to continuously monitor IT infrastructure and physical hardware. For example, Microsoft Azure is protected by a team of more than 3,500 cybersecurity experts. Most organizations do not have the staff capacity to provide the same level of security as hyperscalers.

3 Cloud providers are in the security business

You care about security, but it is not your business. While security is one of your many concerns, it is one of the highest priorities for cloud providers. To stay in business, and remain competitive, cloud providers must deliver the highest possible level of security for their customers. For example, Google Cloud offers “secure-by-design infrastructure” with built-in protection and encryption by default.¹

Microsoft Azure helps identify threats “by analyzing vast sources including 18 billion Bing web pages, 400 billion emails, 1 billion Windows device updates, and 450 billion monthly authentications using machine learning, behavioral analytics, and application-based intelligence as part of the Microsoft Intelligent Security Graph.”²

Cloud providers must also meet the highest standards, including independent, internationally-recognized certifications and audits of security people, processes, and technologies through a range of rigorous programs. For example, Amazon Web Services (AWS) regularly achieves third-party validation for thousands of global compliance requirements. Most organizations do not have the time, resources, or budget to meet this level of security assurance.³

¹ “Trust and security.” Google, accessed 29 April 2022.

² “Strengthen your security posture with Azure.” Azure, accessed 29 April 2022.

³ “AWS cloud security.” Amazon, accessed 29 April 2022.

4 Advanced security tools

Cloud providers deploy a range of advanced security tools to protect customer applications and data. AWS provides fine-grain identity and access controls, continuous monitoring, threat detection, network and application protection, multiple encryption layers, automated incident response and recovery, and more. Hyperscalers offer access to hundreds of additional security solutions available in their partner marketplaces. Duplicating this broad set of advanced security tools in your own network and datacenter is virtually impossible. The cost, staffing, time, and effort required is too much commitment for a company that does not specialize in security.

5 Network segmentation

A security advantage inherent in a cloud environment is segmentation from user workstations. A common method of cyberattack is targeting specific users on the system via email and websites. In these cases, entry into the system comes through user workstations. In a cloud environment,

however, user workstations only have enough connectivity to allow the users to perform their jobs. The workstations do not have direct access to the corporate network. So even if a workstation is compromised, the attacker does not gain access to the company and its applications and data.

6 Physical security

Physical security is still a critical factor. People with direct physical access to hardware can be a serious potential security risk. However, if data and applications are in a cloud environment, disgruntled employees—and others working on site who have the ability to cause accidental harm—no longer have close access to these assets. It is much harder for them to locate the data in a cloud environment.

In addition, hyperscalers have the resources to prevent physical theft of data, including security guards, locked cages for servers, and other state-of-the-art physical security controls that most organizations do not have.




Read more

Read “[Empowering developers through cloud services](#)” for more insight into how Red Hat® Cloud Services can help you navigate your journey to cloud-native applications.



About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with [award-winning](#) support, training, and consulting services.

 facebook.com/redhatinc
 @RedHat
 linkedin.com/company/red-hat

North America
 1 888 REDHAT1
 www.redhat.com

**Europe, Middle East,
and Africa**
 00800 7334 2835
 europe@redhat.com

Asia Pacific
 +65 6490 4200
 apac@redhat.com

Latin America
 +54 11 4329 7300
 info-latam@redhat.com