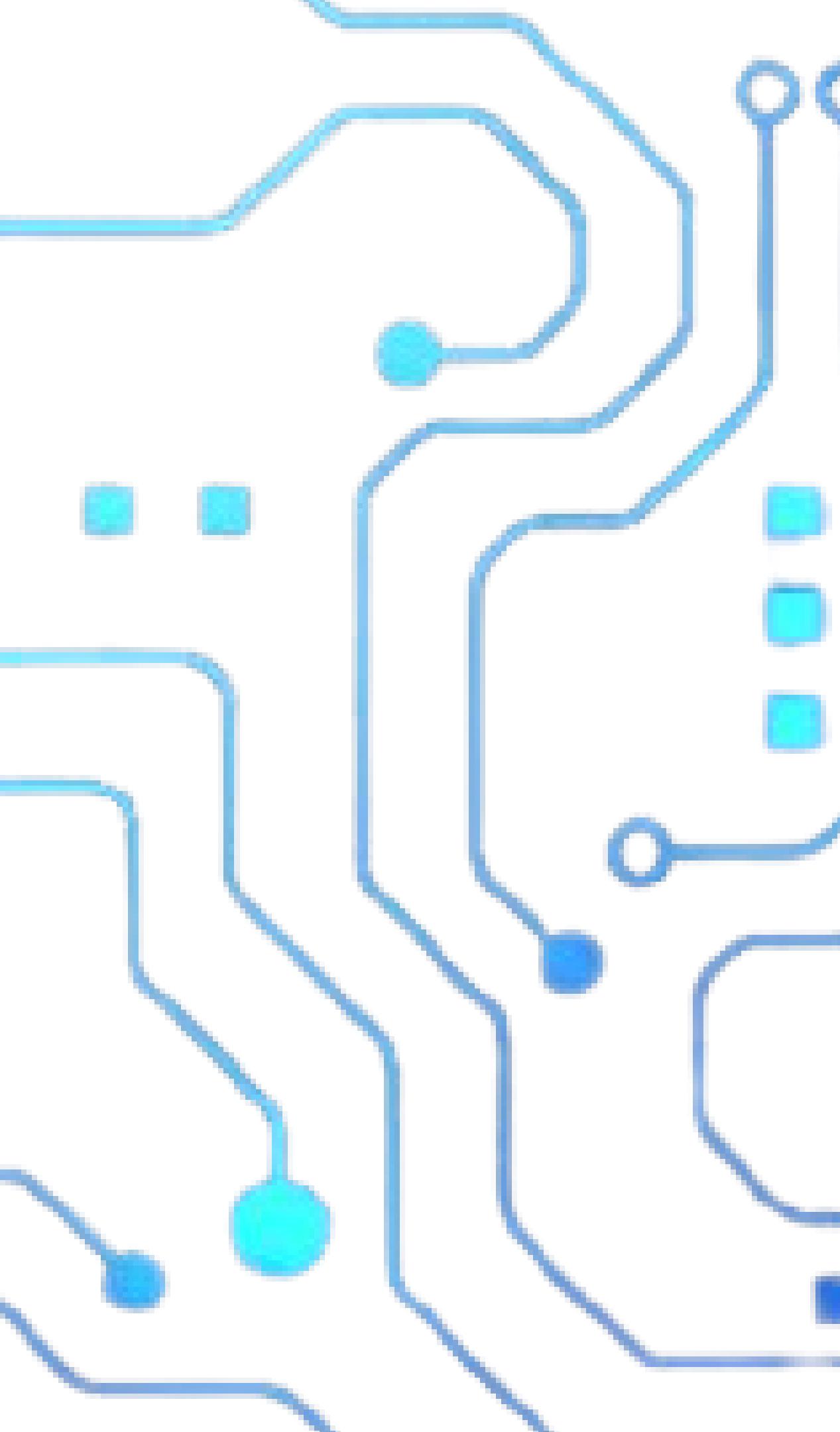


Cloud Security

CYBERTUTORIAL WEB.APP

WHAT IS CLOUD SECURITY?

Cloud security is a collection of procedures and technology designed to address external and internal threats to business security. Organizations need cloud security as they move toward their digital transformation strategy and incorporate cloud-based tools and services as part of their infrastructure.



Why Cloud Security Importing?

- It guards against security breaches.
- It helps manage remote work.
- It helps ensure disaster recovery.
- It also helps comply with regulations.
- It eliminates weak links and builds access levels.

Ensure that you have a window into the workload, both in real-time and historically.

Gain Visibility

01



CLOUD SECURITY

3 Key Practices



Use policy-based behavioral monitoring and investigate with cloud context.

Monitor & Investigate

03

02

Trust But Verify

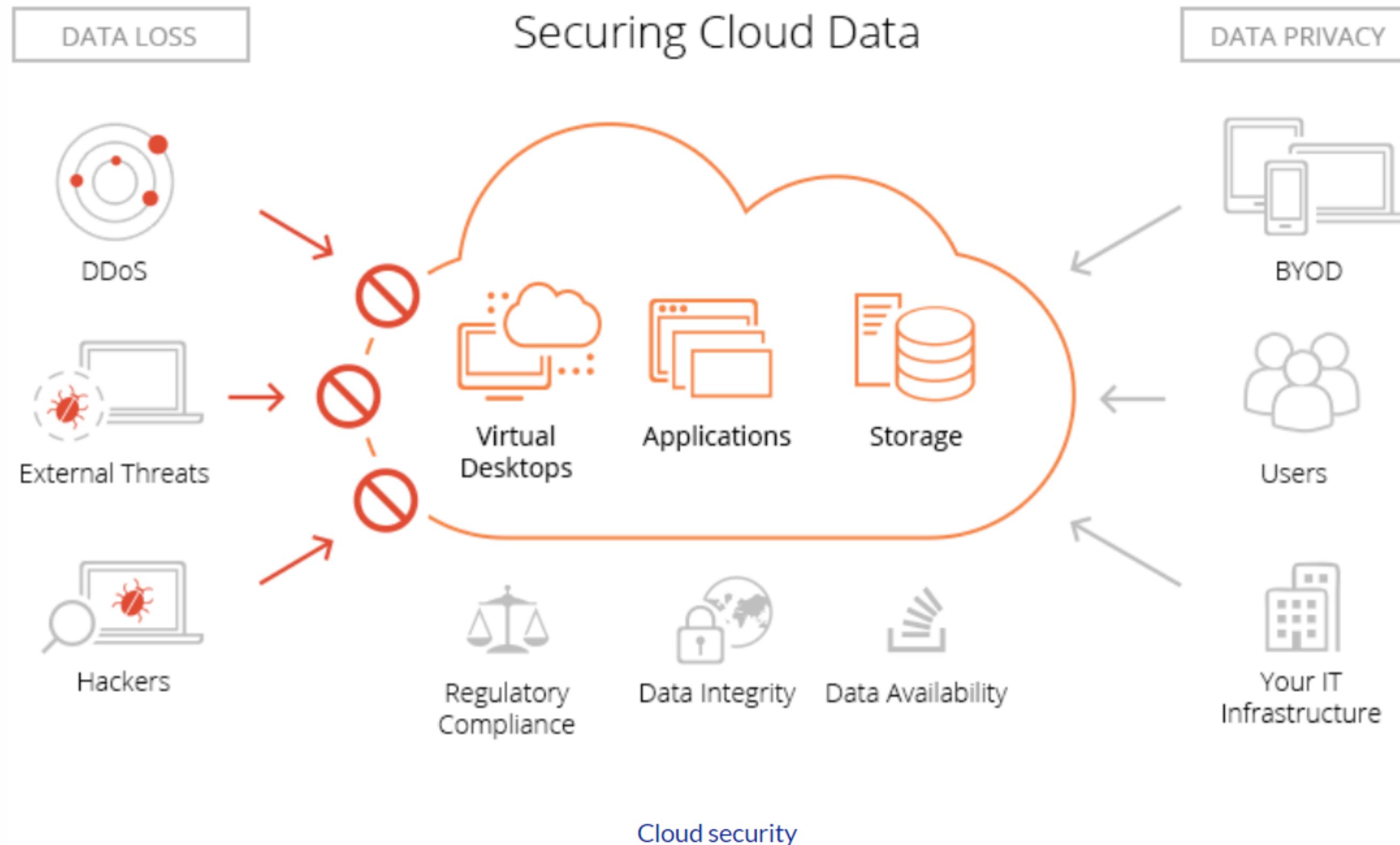
Trust is essential to move and build quickly. But verifying business-critical activity is key to managing risk effectively.



What are the main benefits of cloud security?

- Blocks threats earlier. Stop malware before it spreads to your network.
- Enables more secure cloud use. Improve security without impacting end-user productivity.
- Helps secure users, data, and apps. Protect apps, data, and users in the cloud against compromised accounts, malware, and data breaches. Better support policy compliance.

Challenges of cloud security





What types of cloud security solutions are available?

- Identity and access management (IAM).
- Data loss prevention (DLP).
- Security information and event management (SIEM).
- Business continuity and disaster recovery.