InstaSafe
Cloud. Secure. Instant.

6 CLOUD SECURITY BASICS THAT EVERY CIO AND CTO SHOULD KNOW

Swipe

InstaSafe
Cloud. Secure. Instant.

01. MERE BASICS ARE NO LONGER ENOUGH

With market competition getting fiercer with every passing day, and enterprise technologies making their foray into the modern business scene at a breakneck pace, the game is no longer about the basics!

You must have an in-depth understanding of the various service offerings from your vendor, how their products work, what are the limitations and sharing constraints, and how much control you have over the resource and data accessing.

Swipe >

InstaSafe
Cloud. Secure. Instant.

02. MANAGE THE INTERFACES WELL

The interface of the cloud and your enterprise is the most vulnerable site for cyberattacks, as proved by the Kaseya ransomware attack. It is not possible to read the minds of attackers while configuring the security of your enterprise. However, ensuring a definite understanding of what you can control and how you allow access to data and resources in a cloud environment certainly is.

Swipe >

InstaSafe
Cloud. Secure. Instant.

03. MISCONFIGURATIONS ARE AS BAD AS POOR SECURITY

Misconfigurations and vulnerabilities are related on many levels. In fact, they invite the attackers, just like the security weaknesses. With the emerging vulnerability tracking and technological innovation, it has become easier to identify, locate and predict the vulnerabilities in cloud security.

Hence, as a CTO or CIO, you must gain visibility into the cloud environment and configurations to gain an in-depth understanding of your cloud security posture.

Swipe >

InstaSafe
Cloud. Secure. Instant.

04. RELYING ON VENDOR FOR SECURITY

Be it cloud security or security against cyber attacks, you should never rely on the vendor or any cloud service provider. You have to view every access to your enterprise's data or information or resources as a threat and validate it with stringent checks.

Swipe >

InstaSafe
Cloud. Secure. Instant.

05. CLOUD IS NOT INHERENTLY SECURE

The Cloud might offer you a plethora of features, benefits, and functionalities, but the cloud environments are not inherently secure. And, this has been proved by many security tragedies. This is why most companies with strict data and information regulations tend to place and monitor their confidential resources and assets in their in-house data centers. They use the cloud for less critical data and workloads.

Swipe >

InstaSafe
Cloud. Secure. Instant.

06. DUE DILIGENCE AND CYBERSECURITY INSURANCE

Due diligence is vital for ensuring security at all times, be it the vendor, cloud service, security solutions, or the incoming connections. As a CTO or CIO, you are solely responsible for doing your homework regarding the worth and reputation of the vendor and tools you are using for cloud services.

Swipe >

InstaSafe
Cloud. Secure. Instant.

WE ARE INSTASAFE

InstaSafe empowers organizations in their digital transformation journey, by enabling secure access of enterprise applications to users, with enhanced security, seamless experience, and minimal risk.

As an industry pioneer in Zero Trust, human-centric solutions, we, at InstaSafe have backed the belief that at the center of security for businesses, lies the ability to enable workforces to unleash their potential, irrespective of where they are. Which is why we help organizations in fulfilling their goal of productivity on scale, by simplifying the challenge of ACCESS.

With our hyperscalable and modular solutions, we aim to make the cloud and remote journey for businesses and workforces, much simpler, and much more secure.