InstaSafe Zero Trust Secure Access is a unified security platform that empowers security teams to allow seamless security and management of remote access capabilities across multi-cloud and on-premise environments, while eliminating the need for VPNs and other obsolete security tools. InstaSafe's award winning Zero Trust methodologies allow IT teams to employ a model of continuous authentication and authorisation, and implement a least privilege access model on scale, while ensuring visibility over user activity. What differentiates InstaSafe's solutions is its ability to deploy both agent based or agentless models as per customer needs, and support multiple use cases within the organisation, ranging from secure cloud adoption, to remote access to on premise as well as cloud applications.

InstaSafe
Cloud. Secure. Instant.

Zero Trust

InstaSafe Zero Trust Key Capabilities

Work from Anywhere:
With InstaSafe, IT teams can manage access to all applications from a single vantage console. At the same time, employees can work securely from anywhere without worrying about compromising their networks

Replace your VPN:
InstaSafe enables secure access to applications of any kind, to workforces situated anywhere. Compared to legacy solutions like VPNs, InstaSafe minimises attack surface and prevents malicious actors from gaining insider access to sensitive resources

Manage Vendor Access:
With advanced monitoring and authentication features, and all round visibility over all user activity, privileged access of resources to third party contractors using unmanaged devices becomes simple and easy

Secure On-Premise and Cloud Applications:
Instead of relying on multiple tools to access on-premise and cloud workloads, simplify access and prevent the risk of lateral movement with InstaSafe

Never Trust, Always Verify
No resource is trusted by default. Users and devices are able to access only a limited number of resources based on permissions set by security teams.

360 degree Visibility and Control
Stringent control over who accesses what resource, based on the continuous assessment of user attributes and device state. Options to restrict or monitor user activity based on risk assessment.

Identity Based Verification
Access is based on continuous authentication of user identity and assessment of device posture.

Benefits

- **Simplify your IT infrastructure:** Simplify deployment and maintenance with a hyperscalable SaaS solution that doesn't need complex firewalls
- **Minimise your attack surface:** Enable a least privilege access model that grants access based on continuous verification of identity of users and devices
- **Prevent cyberattacks:** By minimising attack surface and using a continuous risk assessment system, prevent common cyberattacks and insider threats
- **Reduce cost of IT:** Reduce total cost of operations by as much as 40% by deploying hardware free solutions
- **Monitor all Access:** Monitor and manage all user activity and access to on premise and cloud applications from one dashboard

To know more about InstaSafe's Zero Trust Solutions, go to **www.instasafe.com**