COMPARISON SHEET

PARAMETER	INSTASAFE [ZTAA] *Zero Trust Application Access*	VPNs and Legacy Solutions
SECURITY		
Inbound Firewall Rules	Zero. No Inbound firewall rules	NO
Mutual TLS	Yes. Endpoint & Server Verify Each other	N/A
SSL / TLS version	TLS 1.2 (based on the guidelines & Principles lead by NIST and PCI DSS)	N/A
Endpoint fingerprinting	Yes. User device fingerprint (MAC address + HW ID + etc.) is checked on every login	YES
Host check	Yes. Multiplatform Support Windows, Linux, MacOS, Android, iOS	Windows
Certificate based authentication	Yes. Enforced with managed PKI. Transparent to user & the admin	NO
Multi Factor Support	Yes. Behaviour Based Authentication, Built-in OTP support based on Google Authenticator, Email or SMS. 3rd party 2FA supported.	Partial, Third-party solution need to buy Add-on
Device Binding to User	"Yes. User can login from only authorized & registered device. Hence, “stolen password” attacks are blocked"	YES
Application Access. Not Network	Yes. Restrict access only to specific applications (specific ports and protocols)	N/A
Access	Layer 7 Application level Access	Network level layer 3
Geo location and Geo Fencing [Location & Radius Based]	"Yes. User can login from only authorized & registered device. Hence, “stolen password” attacks are blocked"	Limited only Geo location
FQDN	Yes	Limited
Behaviour based Authentication	Yes	Limited
Authentication & Authorization outside Company setup	Yes. We authenticate & authorize users & device even before they reach your edge firewall	N/A

COMPARISON SHEET

PARAMETER	INSTASAFE [ZTAA] *Zero Trust Application Access*	VPNs and Legacy Solutions
MANAGEMENT		
Single & simple web based management	Yes. Single pane of glass management for all users & all DC / Cloud locations / Branches	PARTIAL
Simple User Provisioning	Yes. Bulk upload of users (for local users),Auto sync of AD / LDAP users	Yes
Simple & Granular Access Policies	YES	Limited Functionality
Redundancy & Availability	Yes. InstaSafe Cloud Network is fully redundant with automatic failover to multiple locations globally.	N/A
Global visibility for users and applications - Single pane view providing information related to users connected and the applications being accessed	Yes.	PARTIAL
Secure Private Application access — Access to unlimited private internal applications (whether public/private/hybrid cloud or legacy datacentres) without exposing the network to users or applications to the Internet	Yes.	YES
Enterprise Dark Net with DDoS protection for applications — Applications are only visible to users that are authorized to connect to them	Yes.	PARTIAL
Single console for policy definition and management — All policy for global deployment via a single pane of glass.	Yes.	PARTIAL
Lightweight application used to provide access to internal Apps.	Yes.	N/A
Granular access control by user or group for up to five specific application definitions, each of which may contain multiple hosts and/or ports.	Yes	PARTIAL
"Continuous health monitoring - Application health is continuously monitored to ensure that ports are available and users can connect to the app."	Yes	NO
Microsegmentation	Yes	YES

COMPARISON SHEET

PARAMETER	INSTASAFE [ZTAA] *Zero Trust Application Access*	VPNs and Legacy Solutions
MANAGEMENT		
Basic device posture enforcement — Checks the registry, existence of file system and posture certificate for each device.	Yes	YES
Customer-provided PKI — Customer-provided certificates ensure complete privacy.	Yes	NO
Double encryption — Provides encryption to micro tunnel using customer's PKI.	Yes	LIMITED
Real-time user transaction view — Instantaneous logs for end-user support.	Yes	LIMITED
"Ability to respond to network brown out situations that impact performance (Latency / packetloss etc"	YES; without impacting User Experience	YES
Log Streaming Service — Automatically streams logs to SIEM provider	Yes.	PARTIAL
BENEFITS		
No Hardware	Yes. InstaSafe Secure Access is a software only solution	YES
OPEX Model	Yes. InstaSafe Secure Access is a software only solution	YES
Scalability / Elasticity/ Maximum User per Cluster	Yes. Companies can start with small department and expand as per need – Zero impact on infrastructure	LIMITED
Lower TCO	Yes. Zero Hardware. Less highly skilled manpower	NO
BYOD	Yes. Securely allow BYOD with full remote access functionality to improve productivity	YES
Network access across branch/HQ- to-branch	Yes	Limited Functionality
Network access inbound from users to HQ/branch	Yes	Limited Functionality
Elastic scaling (adapt to user movement)	Yes	LIMITED

COMPARISON SHEET

PARAMETER	INSTASAFE [ZTAA] *Zero Trust Application Access*	VPNs and Legacy Solutions
BENEFITS		
File control	Yes, by application	PARTIAL
Threat updates	Updates every 10 mins	PARTIAL
Licensing model/ Deployment mode	Per user & Gateway Bandwidth Costs are Nil, Flexi Hybrid Deployments	Costs applicable on per user basis, and bandwidth and data costs are additional & Deployed on -premise only
RESTFUL API automation	Full platform configuration	N/A
Integration with SIEM, MFA (AZURE) Asset Management	Available for all the Popular SIEM's	N/A
RDP & SSH ACCESS	Yes	Yes but back haul of traffic
Screen recording , Cut, Copy, Paste Disable Screen capture & Time Based check features	Yes [Supports all Web and Cloud based Apps]	LIMITED
Integrated SSO	Yes Inbuilt	N/A
User Provision by Syncing with Corporate AD	Yes with certs based Functionality	NO
Domain Join of the Systems WFH or the Outside of Office Network	Yes with always on Secure tunnel to corporate network	NO
Pushing GPO & Other Policies	Yes , policies can be pushed to remote machines with SCCM tools or other policy engine mechanism	NO
Software Defined Perimeter [Control, Data , Access Plane different as True SDP]	Built on Cloud Security Alliance Architecture & true SDP based on CSA Architecture	NO
Existence in the Market	7+ Years	5+ years as Traditional VPN
Local Support	Yes. Team is based out of Bengaluru, Mumbai, Delhi ,USA	N/A
Number of Endpoints Protected & POP's	42 Active Pops Across Globe with 10 Mill Endpoints	Not widely Deployed
Gartner Market Guide for Zero Trust Network Access (ZTNA)- 2020	Featured in Report for 2 consecutive times	NO
DSCI Report on Work from Home Solutions	Featured in Report	NO

COMPARISON SHEET

Features	Accops	Microsoft/Legacy Solutions	InstaSafe ZTNA /ZTAA
Mutual TLS (Server and Client)	Server Only	N/A	Both Client and Server Side
Support for latest TLS protocol: TLS 1.2	N/A	Limited	N/A
Support for latest ciphers	N/A	Limited	N/A
Hardware accelerated encryption	N/A	Limited	N/A
In Premise appliance /gateway scalability	2000	< 500	Unlimited [Based on the G/w Sizing]
Maximum users per cluster	20000	< 2000	Unlimited
Web based management	N/A	N/A	N/A
Integrated access portal for web apps, hosted apps, SAAS Apps	N/A	N/A	N/A
SSO for web apps, SaaS Apps	[Limited]	N/A	N/A
User based policies Device entry control Endpoint Internet control Endpoint host scan: AV/FW/AS Check for Windows updates Always On-VPN Two factor authentication User Experience SMS, Email OTP integration Third Party Authenticator – QR Code Self service portal for users for OTP/Password management	N/A	N/A	N/A
Support for all desktops OS	N/A	Limited	N/A
Support for iOS, Android	N/A	Limited	N/A
Supports multiple organizations /domain as single site	N/A	N/A	N/A
Screen recording , Disable Screen capture & Time Based check features	[Limited]	N/A	N/A

COMPARISON SHEET

Features	Accops	Microsoft/Legacy Solutions	InstaSafe ZTNA /ZTAA
Application Restrictions	N/A	N/A	N/A
Support for Cloud deployment	N/A	Limited	N/A
Software Defined Perimeter [Split Plane Architecture]	N/A	N/A	N/A
No Need for VPN	Need VPN	N/A	Works on Zero Trust Principles Secure Access to applications without a need of VPN's
Geo location and Geo Fencing [Location & Radius Based]	Only Geo	Limited	Both Location as well as Geo Fencing
Supports Internal & Cloud Web applications	Only Private & internal web apps	No	Supports all web and cloud based Apps
Integration with SIEMS's	Limited	Limited	Supports all popular SIEM's
Screen recording & Cut copy paste	Only for internal Private apps	No	Supports internal as well as cloud apps
RDP & SSH ACCESS	Yes , Backhaul of the traffic	N/A	Supported
Integrated SSO	No	No	Yes