Comparison between OpenVPN and InstaSafe Zero Trust

Why InstaSafe Zero Trust is a better security alternative than OpenVPN

celestix

Features	OpenVPN	InstaSafe
Global visibility for users and application - Single pane of glass shows which users are accessing private, internal apps	Partial	Yes
Secure Private Application access - Access to unlimited private internal applications (whether public/private/hybrid cloud or legacy datacenters) without exposing the network to users or applications to the Internet	No	Yes
Enterprise DarkNet with DDoS protection for applications - Applications are only visible to users that are authorized to connect to them	Yes	Yes
Single console for policy definition and management - All policy for global deployment via a single pane of glass	Partial	Yes
Lightweight application used to provide access to internal Apps	Yes. But Administrator need to provide CA, PKI and TLS keys separately.	Yes, user friendly installation. (<1.4mb)
Granular access control by user or group for up to five specific application definitions, each of which may contain multiple hosts and/or ports.	Partial	Yes
Continuous health monitoring - Application health is continuously monitored to ensure that ports are available and users can connect to the app	Partial	Yes
Basic device posture enforcement - Checks the registry, existence of file system and posture certificate for each device	Partial	Yes
Customer-provided PKI - Customer-provided certificates ensure complete privacy	Yes	Yes
Double encryption - Provides encryption to microtunnel using customer’s PKI	Yes	Yes
Real-time user transaction view - Instantaneous logs for end-user support	Partial	Yes
Log Streaming Service - Automatically streams logs to SIEM provider	Limited Functionality	Yes

Security	OpenVPN	InstaSafe
Inbound Firewall Rules	Yes	Zero. No Inbound firewall rules
Mutual TLS	Yes	Yes. Endpoint & Server verify each other
SSL / TLS version	SSL v3 mostly (some on TLS 1.2)*	TLS 1.2 (approved by NIST and PCI DSS)
Endpoint fingerprinting	No	Yes. User device fingerprint (MAC address + HW ID + etc.) is checked on every login
Host check	Partial	Yes. Support Windows, Linux, MacOS, Android (iOS)
Certificate based authentication	Yes. Company needs to manage PKI setup and integrate (very complex)	Yes. Enforced with managed PKI. Transparent to user & the admin.
2FA Support	Partial. Mostly 3rd party supported	Yes. Built-in OTP support based on Google Authenticator, Email or SMS. 3rd party 2FA supported.
Device Binding to User	No. Attacker can login from any system (even using mobile to bypass host checks)	Yes. User can login from only authorized & registered device. Hence, “stolen password” attacks are blocked
Application Access	No. Access control is limited in many ways resulting in excessive access rs)	Yes. Restrict access only to specific applications (specific ports and protocols)
Authentication & Authorization outside Company setup	No. Authentication & authorization of users is only after they are inside your network	Yes. We authenticate & authorize users & device even before they reach your edge firewall

Network	OpenVPN	InstaSafe
Simultaneously access applications in multiple DCs / Clouds	No. complex ACLs and routing issues.	Yes. Users can access applications located anywhere without traffic backhauling
Extend AD security to remote employees (Domain Joining)	No	Yes. Authenticate remote users to AD (located inside DC), push GPO and other functionality
MPLS failover / replacement	No	Yes. InstaSafe SecureAccess can be deployed to provide failover for MPLS or replace MPLS

Management	OpenVPN	InstaSafe
Single & simple web based management	No	Yes. Single pane of glass management for all users & all DC / Cloud locations / Branches
Simple User Provisioning	Partial	Yes. Bulk upload of users (for local users), Auto sync of AD / LDAP users
Simple & Granular Access Policies	No. Granular access policies need to be configured separately for each location	Yes. Easily configure granular access policies centrally - control access to application located anywhere (DC, DR, Cloud, Branch etc.)
Redundancy & Availability	Partial. Automatic failover requires multiple devices in each location.	Yes. InstaSafe Cloud Network is fully redundant with automatic failover to multiple locations globally.

Benefits	OpenVPN	InstaSafe
No Hardware	Yes	Yes. InstaSafe SecureAccess is a software only solution
OPEX Model	No. Solutions require large CAPEX	Yes. InstaSafe SecureAccess is billed annually as subscription. Zero setup fees.
Scalability / Elasticity	No. Forklift upgrades / refresh is required to handle higher loads (especially for DR situations)	Yes. Companies can start with small department and expand as per need - Zero impact on infrastructure
Lower TCO	No. Complex infrastructure. More highly skilled manpower in multiple locations	Yes. Zero Hardware. Less highly skilled manpower
BYOD	Partial. Many legacy VPN systems have limited functionality for mobile devices	Yes. Securely allow BYOD with full remote access functionality to improve productivity
Multi DC support	No. Need to install different OpenVPN server at Secondary DC and user needs to carry two agents.	Yes. With Single agent user can access multiple application hosted in multiple DCs