

Trust that is implicit is becoming dangerous in IT. Creating a large corporate perimeter and trusting everything inside has proven to be a flawed design and needs reconsideration.

Zero Trust is a holistic approach to security that addresses these changes and how organizations work and respond to threats. It's the model and the philosophy corporates need with borderless networks. Whether inside or outside of the corporate network – nothing should be trusted automatically. With Zero Trust, this trust is established but is constantly re-evaluated. Hence temporary.

Zero Trust enables to control entire network, from inside the office premise to the cloud platforms. No more lack of control outside the corporate perimeter, or struggles with remote users. And helps create Zero Trust network.

InstaSafe's Zero Trust Access (ZTA) is a secure remote access business enablement solution. With cloud and application-agnostic design, we make sure that only the required application is just a one-click away across any cloud.

With Privacy first as the motto, InstaSafe makes sure that the user data – at rest or in motion, is always secured.

InstaSafe's Zero Trust Application Access provides security technologies and controls that help accelerate and simplify your journey to Zero Trust. It allows you to control access to your apps and data based on User Identity and Device Health. Our cloud-based user-friendly, zero-trust security platform for all users, all devices and all applications. helps you orchestrate and monitor your Zero Trust network - create segments around users, devices, apps, networks, and more; monitor all user activity across the network and identify potentially compromised user credentials; device health check for every device so that, in the event one is compromised, the device can be automatically isolated and blocked from connecting with other devices or network, provides insight and visibility.

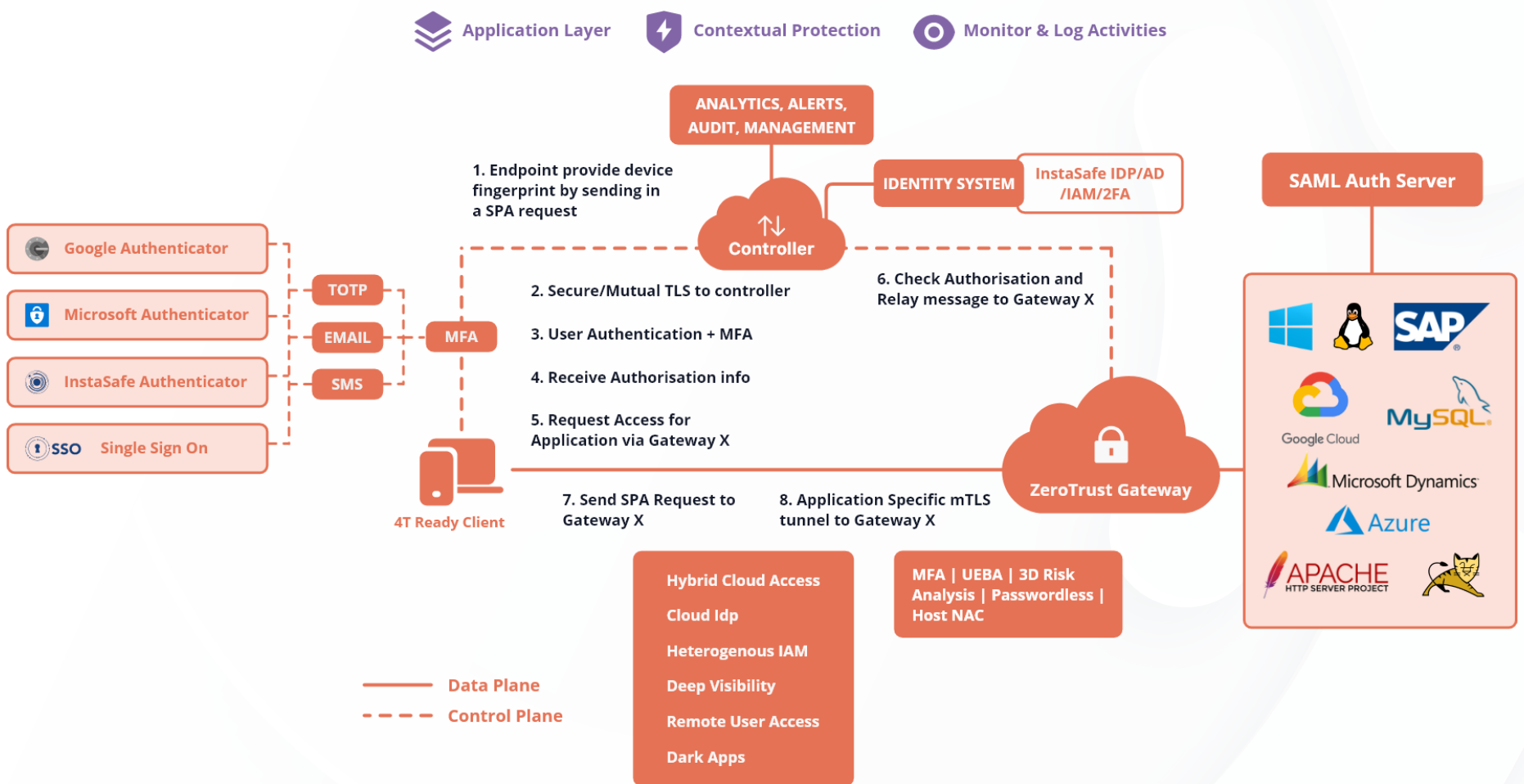


Figure 1 - How ZTA works

Zero Trust Security

- Access policies - User, group, devices, applications
- "Least Privileged" access
- **Inbuilt MFA and SSO**
- **Single Message Authorization (SMA)**
- Simplified DDoS protection
- No visibility to Gateway before authentication
- Default Drop-all firewall
- **Mutual TLS 1.3, AES 256 Encryption**

- **Hybrid Deployment (SaaS and On-Premise)**
- **Device Binding and Device Posture Check with Geo-location binding**
- **Separate path for data and control traffic**
- **Secure VPN Alternative**
- **Controlled and Contained direct tunnel access for application**
- **Always On. Azure AD Join**
- **Agent and Agentless Access**

Identity & Access Management (IDAM)

- Identity/Device posture based authentication
- **Single Sign On (SSO) Authentication for SAML supported Apps**
- **Support of Directory Sync with On Prem AD, Azure AD, LDAP**
- **MFA via OTP, T-OTP, MPIN, Push Notification, Facial and Fingerprint**
- Dynamic Authorisation based on Geo-risk and Temporal (Time based) Risk Assessment
- **ML based Behaviour Authentication**
- Integration with third-party SIEM solutions - QRadar, ArcSight, Splunk

- Unified login and reuse of Auth
- **Authentication supported included TACACS, RADIUS, FIDO, OAuth**
- **Hardware Token (Yubikey) based Authentication**
- **Secure access to Multi-cloud and Hybrid workloads**
- **Auth Server Failover at DR site**
- **Supports SMS Gateway integration**
- **Automated onboarding of users from third-party IDP**

Remote Access & Application Access

- Application Access Control - Granular, per-session access based on a verified user and device identity
- Direct data tunnel from user to App server
- **Role Based Access Control (RBAC)**
- User access to Thick Client, Web, RDP and SSH Access
- Layer 3 and Layer 4 protocols and related apps access

- **Context Based Access with LAN, WAN and Geo-Location**
- Global Access policy enforcement
- **Frictionless and secure Remote access with zero latency**
- Provide application alone access
- **Contextual Access based on Certificate installed, OS license validity, OS Patch, device context, time based access**

Data Security & Leak Prevention

- Clipboard protection - copy/paste prevention
- Screen copy security - Prevent Screen capture, recording
- **Whitelisting / Blacklisting of IPs**
- File download prevention
- Secure workspace on chromium container

- **Single Device login**
- **Watermark Protection**
- **Blocking Apps like Anydesk, Teamviewer**

Simplified Management

- Centralised Management
- Agent-based, Agentless access for users
- Agents for Windows, Linux, MacOS, iOS, and Android
- Ease of Client administration
- Integration with 3rd party business process tools
- 4-step Application Onboarding process

- **Endpoint control features on Boot up**
- **Easy to schedule backups**
- **Single click access to applications**

Central Logging & Reporting

- Continuous health and log monitoring
- Historical and Compliance reports
- Audit logs for access, login, login failure
- **Custom alerts for non approved devices**

- **Network Access logs**
- Single-pane management dashboard for monitoring traffic, access and health
- **Visibility and audit trail for user and network activity**

Scale

- Horizontally scalable Gateway
- Unified access to Applications across Clouds and DCs
- Scalable across infrastructure assets and users

- **Hyper-scalable solutions - deployed across hybrid environments**
- **Deploy across multiple cloud environments within days**
- **Fast and Easy deployment**
- **Save time and resources**

Additional Services

- Support options - 24x7, 8x5
- Always-available Email support

- **Technical Support for partner groups**
- **Dedicated Technical Customer Success Managers**

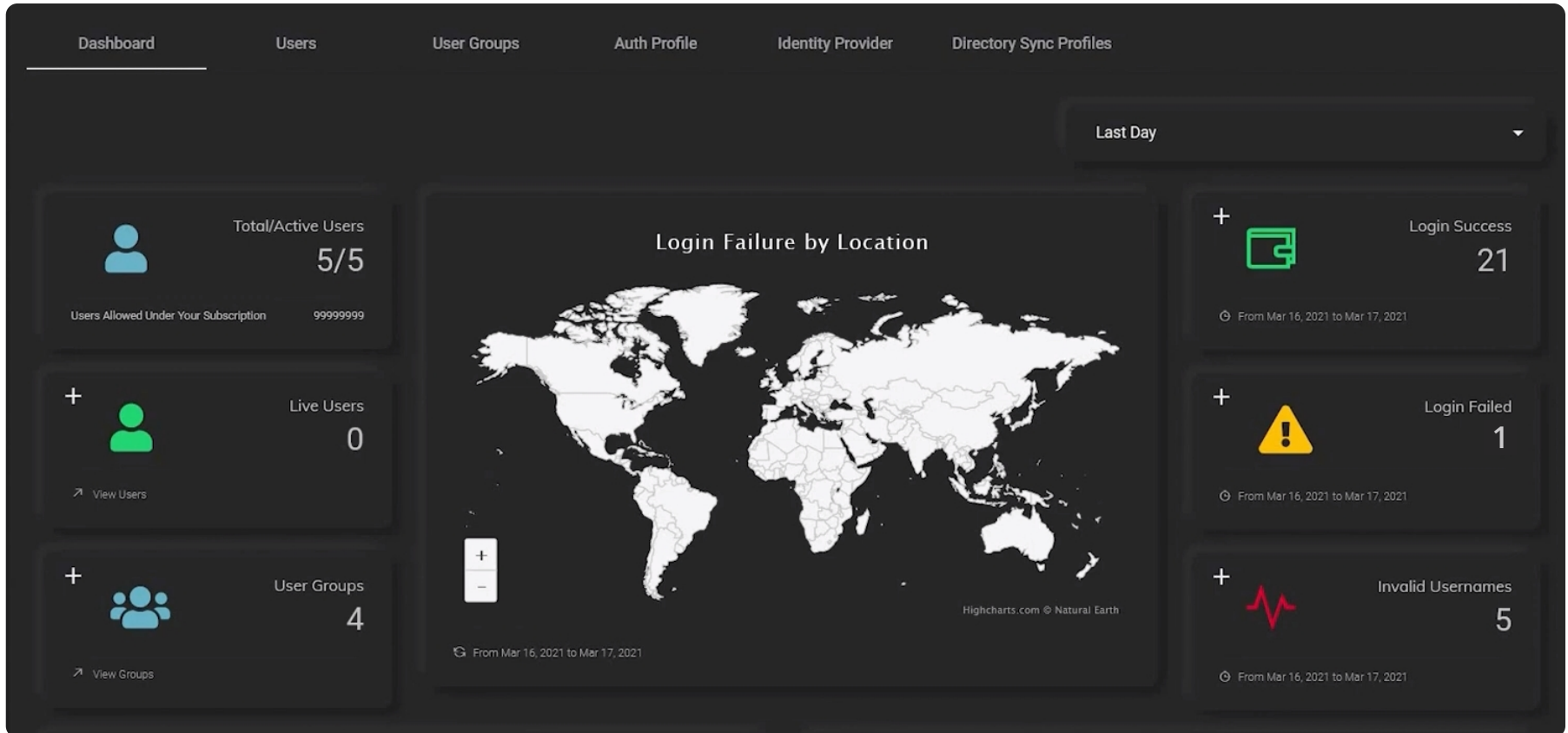


Figure 2 - Dashboard

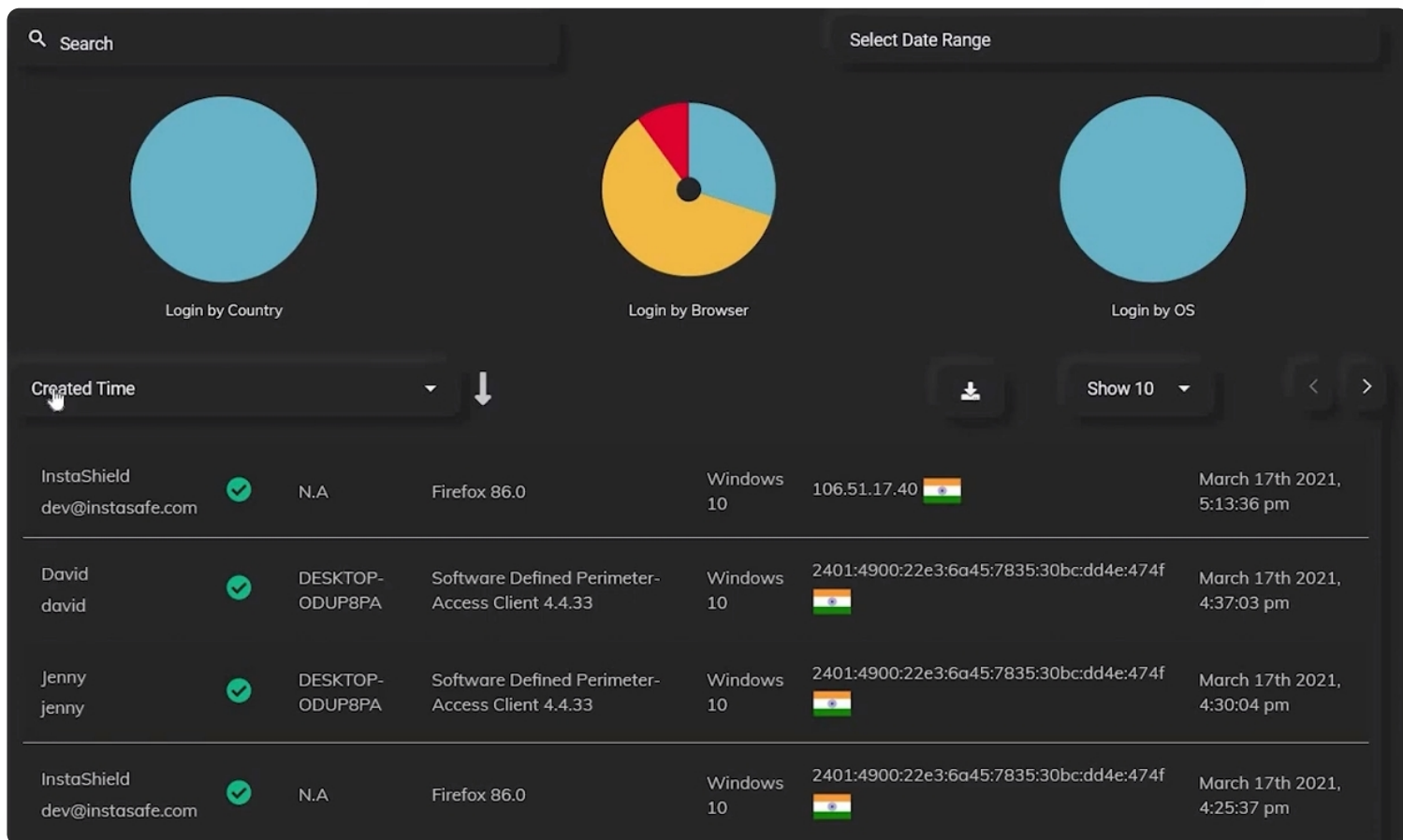


Figure 3 - Audit Log

About InstaSafe

InstaSafe - Trusted cybersecurity provider that offers innovative security solutions and technology backed by crowdsourced vulnerability discovery to protect and keep organizations and businesses safe.

InstaSafe's mission is to secure enterprises from the misuse of excessive trust and privilege access. We empower organizations across to globe in preparing their security infrastructure for digital transformation in a cloud-dominated world. Recognised by Gartner as one of the top representative vendors providing Zero Trust Security, InstaSafe Secure Access and InstaSafe Zero Trust Application Access follow the vision that trust can never be an entitlement, to offer securely enhanced and rapid access of enterprise applications to users situated anywhere across the globe. We secure 500,000 endpoints for more than 150 customers, spread across 5 continents, with our 100% cloud-delivered solutions, ensuring that our offerings are in line with our mission of being Cloud, Secure, and Instant.

Let's talk more about how InstaSafe can empower your remote workforce through transformational and seamless security.

✉ sales@instasafe.com

🌐 www.instasafe.com