TEHAMA

The #1 SAAS Platform to Securely Manage Your Global Workforce

—

Secure Cloud Workspaces for Law Enforcement Agencies

Law enforcement agencies require the highest level of security for communication and collaboration. That's true now more than ever as police departments and emergency services are increasingly targeted by cyberattacks. Any lost data can have serious operational and privacy implications.

Protecting and accessing private records and confidential assets requires a strong chain of custody backed by strict and auditable compliance controls. But strong security can't slow down an investigation or prevent information from being shared among joint task force partners across multiple departments, agencies or municipalities.

> Tehama provides a cloud-based software-as-a-service (SaaS) platform with secure, collaborative workspaces that connect internal and external teams without the risk of intrusion or data theft, and the ability to execute dark web investigations without provenance back to the police agencies.

Key Features

- Secure, cloud-based, collaborative workspaces
- Zero-trust access controls
- Role-based access
- Dynamic firewall rules
- Policy controls and audits

Key Benefits

- Securely manage all access to confidential data and records
- Ensure regulatory compliance
- BYOD and quickly connect anywhere, anytime
- Eliminate the need for risky, complex and costly VPN connections or virtual desktop hardware

What law enforcement agencies can do with Tehama

Tehama's on-demand SaaS platform makes it possible to:

Collaborate securely with other agencies or departments
Investigations are conducted in a secure, isolated, cloud-based environment with a zero-trust approach to data access and management, eliminating the risk of compromising chain of custody or other cases.

Start investigations and other projects faster
Collaborative workspaces can be built quickly and scaled up/down as needed, with fast, easy and secure onboarding of key stakeholders, internal teams, external agencies and remote workers or collaborators.

Investigate the dark web with confidence
Investigators can search the dark web via Tehama's secure virtual room with no traceability back to their agency's IP address or domain — and all evidence is collected in perfectly witnessed session recordings.
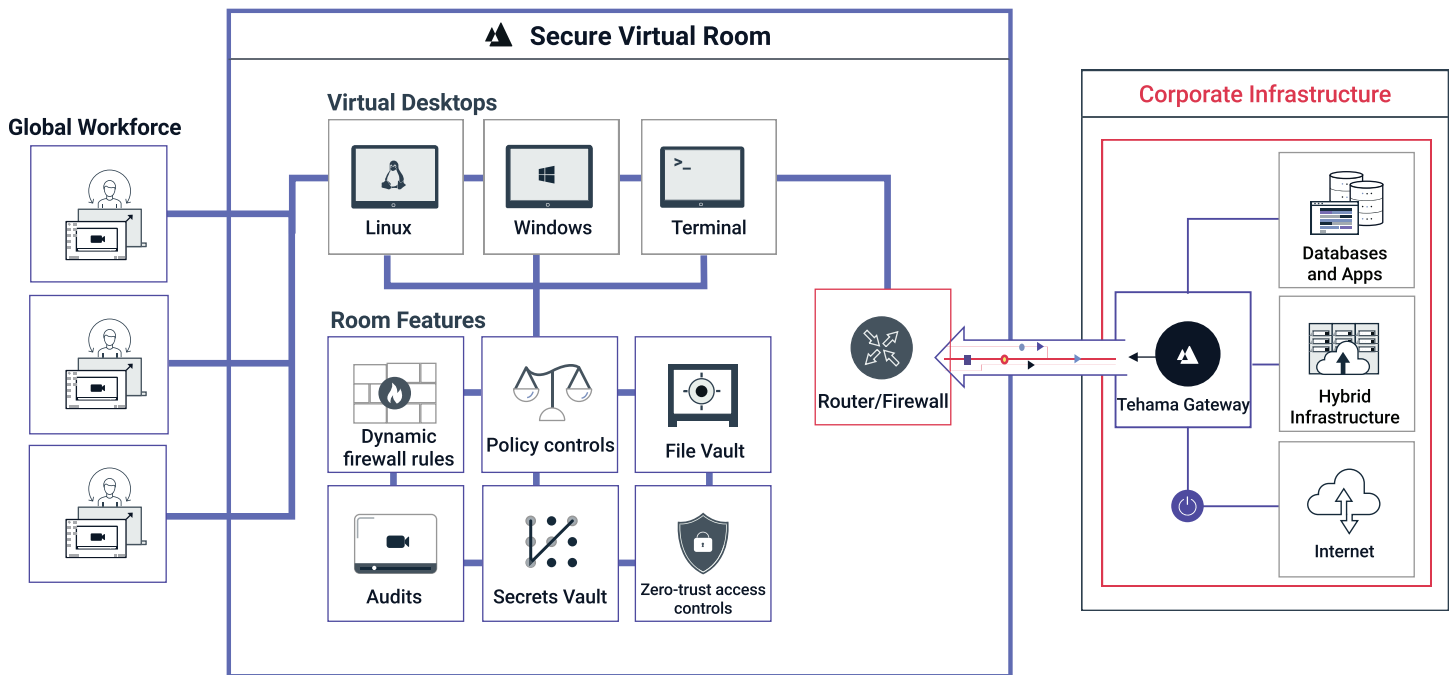
Meet the compliance requirements of governing bodies
Tehama is fully compliant with GDPR and SOC 2 Type II. It also provides access policy controls to ensure work being done on the platform conforms to the requirements of each specific project.

Secure high-risk environments
The Tehama platform can be used with mobile digital communications, including computers and other devices installed in police vehicles.

TEHAMA

A single platform for secure, cloud-based collaborative workspaces

Tehama provides all the components for secure cloud-based collaboration, including dedicated encrypted network channels, firewalls, storage and end-user compute infrastructure — without the complexity of integrating and managing your own virtual desktop infrastructure (VDI), desktop-as-a-service (DaaS) or standalone access/security management tools.

Platform architecture

Each secure virtual room is connected directly to your agency's network via the Tehama gateway, which permits traffic flow to your network only to eliminate the risk of third-party attack. Virtual desktops are accessible via the Tehama Web UI and AWS client tool only — both of which require strong authentication.

Session recordings show all user activity performed in a room, right down to the keystroke, for exceptionally accurate auditing as well as forensic analysis and live viewing for training and monitoring purposes.

The File Vault is an encrypted storage volume that enables secure information-sharing, fully isolated from any other rooms to ensure zero data leakage. The Secrets Vault provides secure storage of credentials and firewall rules for privileged-access assets — with masking to prevent any possibility of copying credentials outside the Tehama platform.

About Tehama

Tehama is the leading SaaS platform for secure IT service delivery, enabling law enforcement agencies and global enterprises to onboard, manage, scale, secure and audit employees and third-party IT service providers — without the costs and project delays associated with IT infrastructure procurement and deployment.

For more information on Tehama, visit tehama.io or contact tehama@tehama.io

How Tehama is different from VDI, DaaS and VPN

Our platform provides additional levels of controls to ensure fully secure information-sharing and digital collaboration. We enforce higher levels of authentication and provide zero-trust access controls that let network admins specify which systems and applications individuals can access—down to the IP address and port.

The result: more security, more control and more isolation.

How Tehama approaches security and compliance

Tehama allows you to set strict policies for data and application access with robust user identity management and "just-in-time" user provisioning through SCIM and SAML. Access to credentials and other assets is available only after successful two-factor authentication and single-use passwords prevent access after a session has ended. Tehama is *SOC 2 Type II certified by Deloitte*, proof of our mature processes and strict adherence to compliance regulations. Deep logging and continuous auditing capabilities make it easy to see when personal information has been used or obtained by any third party or partner for full compliance with GDPR and other privacy legislation.