TEHAMA

THE LEADING SAAS PLATFORM FOR SECURE IT SERVICE DELIVERY

—

Complete SaaS-based work environments built for securing a global workforce

—

What if there were a more secure, more efficient way to remotely connect your global employees and IT consultants to your corporate networks, without providing privileged credentials? What if it were possible to create secure development and innovation sandboxes with complete control over individual, team, and network access? What if you could remove the risks of remote employees' and consultants' endpoint devices being compromised or stolen, and eliminate the risks of malware and corporate data loss completely?

Tehama is a secure, SOC 2 Type II, SaaS solution that provides all the IT infrastructure enterprises need to securely leverage and grow global teams. Tehama provides secure perimeters for cloud workspaces that securely connect employees and third-party consultants to the mission-critical and data-sensitive applications within the enterprise or on cloud, with deep forensic auditing and compliance. Launch "ready-to-work" complete, secure, and productive IT work environments — in minutes not months.

To learn more visit tehama.io or contact us at sales@tehama.io

Tehama integrates security with agility

Leveraging a global workforce is riddled with security risks: from abuse of privileged credentials and data theft to legacy hardware and infrastructure constraints. Virtual desktop infrastructure (VDI) and Desktop-as-a-Service (DaaS) do not provide sufficient protection and also do not ensure the regulatory compliance that is required.

You need to establish a secure perimeter around your cloud workspaces and corporate data.

Protect against intellectual property & data theft - securely contain all IP and work assets in secured collaborative environments, eliminating the risk of data theft. The workspaces within these secured perimeters allow for global remote access to corporate networks and assets, with zero trust network segmentation, and a holistic security and trust framework.

No more employee laptop management - use secured and isolated end-user compute environments conforming to corporate image policies, without incurring delays to start dates associated with shipping and receiving custom, dedicated managed hardware.

Zero-trust network and application isolation - apply a zero-trust access model for all employees and third-party contractors - globally, applying MFA (Multi-Factor Authentication) and network access policies resulting in access control and precision necessary for securely connecting remote employees and third-party contractors to secured internal networked assets, with full access control and visibility.

Dynamic on-demand and secure developer environments - deploy secured and isolated end-user compute environments conforming to corporate image policies for globally dispersed access, without incurring the time and costs associated with infrastructure purchase, configuration, and complicated vendor tool configurations.

Compliance & Audit Enforcement - deliver all development and IT Services using secured, isolated, and fully functional IT development environments which meet SOC 2 Type II compliance regulations. Tehama offers the ability to create, control, and maintain highly regulated work environments compliant to SOC 2, GDPR, OSFI, FIPS, and NIST.

Tehama saves costs and increases security with a virtual and ***secured perimeter*** that extends a zero trust network to global employees and third-party IT services providers. With Tehama there is no longer a risk of data being lost on employee laptops or malware intrusion into corporate networks. Tehama streamlines the onboarding, management, scalability, security, and auditing of remote employees and third-party IT service providers -- at the speed of SaaS.

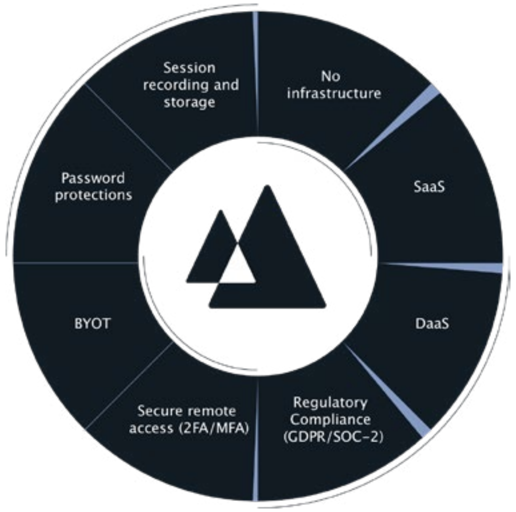
To learn more visit tehama.io

Tehama secures access to corporate data for global employees and contractors

Reduce costs by avoiding IT infrastructure with a complete and on-demand SaaS solution.
At the core of the Tehama platform is a wickedly smart architecture that creates virtual secure perimeters around cloud workspaces. Unlike naked VDI or DaaS solutions, and VPN, Tehama provides additional levels of controls and capabilities required to quickly onboard, manage, scale, secure, and audit a global workforce or third-party IT service vendor.

Characteristics of a Secure Perimeter

- Cloud-based workspaces lack the control and infrastructure required for enterprise-grade development and IT service delivery. A secure perimeter is needed which has the following characteristics:
- Controlled authentication, identity and access controls using multi-factor authentication (MFA): Integrated access management (IAM) tools ensure that the individuals accessing the resources have the proper roles and privilege.
- Hybrid network access controls: Managed by the enterprise IT Team–whether the network is cloud-only, on-premises, or a hybrid.
- Controlled and audited access to shared files: Securely share files in an enterprise-controlled manner, not by Dropbox, Google Docs, or e-mail.
- Audit trails and access logs: Administrators monitor and apply forensic analysis into exactly who has done what within the environment to greatly support regulation and compliance requirements
- Intellectual Property containment of cloud services within the enterprise boundary: There's a very real possibility that intellectual property work contained and hosted by cloud platforms such as Jira and Bitbucket can be accessed, downloaded, or can otherwise escape the network perimeter of the enterprise. Securing the perimeters around the workspaces in which this work is being done removes the risk completely.


Session recording and storage
No infrastructure
SaaS
DaaS
Regulatory Compliance (GDPR/SOC-2)
Secure remote access (2FA/MFA)
BYOT
Password protections

Comprehensive SaaS Platform

> "Tehama is a game changer. In seconds, we can enable a highly compliant and secure environment for our managed services customers, without the delays and overhead of physical compute hardware."
>
> Chris Opat, CLOUDREACH
> HEAD OF CLOUD OPERATIONS

Tehama Benefits for Enterprises

- **Quickly onboard/offboard, manage, scale, secure, and audit your global teams**

Rapidly build, scale up and down, end-user compute environments which are securely connected to corporate networks for performing development and IT service delivery. Manage access to corporate network assets with zero-trust application-level precision.

- **Increase hardware security and reduce hardware cost**

Shipping managed laptops to employees and IT service providers across the globe opens enterprise networks to additional threat surfaces and security risks. Laptops can be stolen, lost during shipping, or compromised either within the shipping period or once in the hands of the end user.

The solution to this is to virtualize the entire endpoint laptop-shipping process.

Eliminate the need for dedicated hardware altogether. Remove the fear of endpoint devices being compromised or stolen. Eliminate the risk of data loss, and at the same time achieve far greater levels of business agility. Using Tehama, scalable end-user compute provides developers with access to a broad range of hardware compute platforms and higher grade virtual desktops which outperform the compute resources of typical laptops.

- **Meet development regulatory requirements - SOC 2 Type II, GDPR, OSFI, FIPS, 23 NYCRR 500, NIST 800, HIPAA**

Gain immediate access to development environments having high regulatory compliance requirements, without building out costly compliant infrastructure and business processes. Leverage a SOC 2 Type II end-user compute environment and achieve and maintain regulatory compliance requirements for banking, financial services, insurance, and government enterprises.

> **“Before Tehama, we were using ad-hoc mechanisms for our teams to access customers’ environments. The main challenge was the onboarding process took weeks and sometimes months for VPNs and other secured accesses to be established and approved by our customers’ Security Departments. And we were not able to offer our customers audit mechanisms for compliance about how we interacted with their systems.**
>
> **Tehama solves these problems.”**
>
> Álvaro Hernández Tortosa
> FOUNDER, ONGRES

About Tehama

When Pythian, a global IT Services provider, needed to improve agility and security when connecting toglobal customers in an expanding global market, the Tehama Service Delivery Platform (SDP) was created to deliver better IT outcomes, faster, and more securely. Eager for the same benefits of agility and security, Pythian’s customers and partners began requesting access to the Tehama SDP, to securely onboard other service providers and apply continuous auditing and compliance across their services supply chain. Tehama operates as a business unit of Pythian. Our goal is to bring the values of “delivering better IT outcomes, faster, and more securely” to the industry, and to revolutionize how services are delivered across the entire IT services ecosystem.

For more information or a demo, visit tehama.io or contact us at sales@tehama.io.