Tehama Frequently Asked Questions

Q: What does Tehama do?
A: Tehama is the fastest, easiest, most secure way to deploy a virtual workforce. With our next-generation DaaS platform, enterprises can create cloud-based virtual offices, rooms, and desktops anywhere in the world. No other solution on the market today connects remote workers with mission-critical and data-sensitive systems, with the speed, agility, unparalleled security, and comprehensive audit trail via built-in SOC 2 controls, real-time activity feeds and session recordings that Tehama offers.

Q: What makes Tehama different from other virtual desktop deployment solutions?
A: Tehama takes a different approach by prioritizing security in order to arm organizations with the tools they need to enable their employees to work from home safely, quickly, and easily. In addition, The cloud-based platform is the fastest, easiest, and most secure way to deploy a virtual workforce.

Q: What is Tehama's total funding?
A: Total funding to date is $10 million.

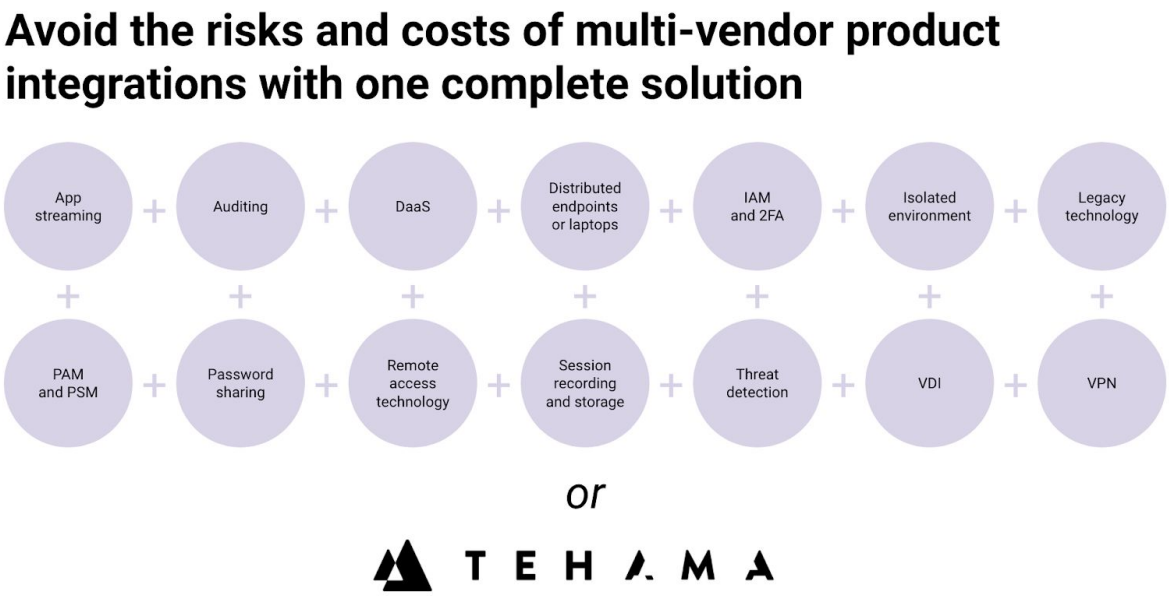
Q: How many employees does Tehama currently have? Are you hiring?
A: Yes, we are currently hiring to help fill our growing team.

Q: If I already have AWS for my infrastructure, how does Tehama work with my platform?
A: Tehama's secure Room and Desktops can connect to infrastructure deployed anywhere in the world. Tehama can connect to applications deployed on AWS cloud infrastructure or applications deployed on Azure, OCI, IBM Cloud, GCP or other data centres, on-premises or on the cloud. Many customers use Tehama to complement their AWS deployments by provisioning desktops from Tehama to people (admins or end-users) who need to work on the applications deployed on AWS. The benefits of Tehama desktops are fast time to provisioning of Windows or Linux Desktops, security of data from the endpoint to the application, data encryption, deep audit logs… and no need to buy laptops or desktops, VPN licenses or hardware, endpoint security tools, additional firewalls, or session recording and audit tools.

Q: I already use VPNs? How is Tehama different?
A: In response to the urgent need for enterprises to rapidly scale a remote workforce, many organizations instinctively turned to virtual private networks (VPNs). This initially made some sense. After all, in many cases VPNs were already in place at many organizations. They had historically done an adequate job, mostly because they were used so infrequently and weren't the primary method of working. But as the global pandemic forced companies to move massive numbers of staff to VPN, cybercriminals immediately began preying on the personal devices and relatively insecure consumer networks being used. This trend is decreasing the time to

productivity. Whenever a company sets up a VPN for remote users, and inevitably important decision is whether to support split tunneling. Split tunneling on a VPN is a real threat to companies having to trust more home networks and deal with bandwidth concerns. This impacts two major elements of an enterprise's work-from-home effort: Security and productivity.
Tehama eliminates the need for VPNs by securing a direct connection to only the applications required for the remote teams. It also prevents any internet traffic from entering the Room and doesn't share split tunnelling that opens up risks for home and public wifi network traffic to be funnel through enterprise firewalls. You can learn more about Tehama and VPNs at this blog.

Q: I already have DaaS and / or VDI. How is Tehama different?
A: DaaS and VDI provide the base Windows or linux Desktops. Once you have the base licenses, organizations still need to provide the infrastructure either via a physical server bought and maintained in a data centre owned by the customer or outsourced. More recently organizations have been deploying their VDI and DaaS licenses on public cloud platforms avoiding the need to buy dedicated servers while simply using cloud infrastructure. The shortcomings of VDI and DaaS for work-from-home use cases are no VPN, end-point security, session recording, deep logging, data loss prevention, IAM, PAM tools are provided. Organizations need to stitch these services together to secure the end to end workflow. Tehama is purpose built to secure the remote workforce use case and to reduce the multiple threat surfaces that pop up with a remote workforce. This image describes the benefits to Tehama compared to managing several tools.



Q: What do you use to ensure compliance with regulatory requirements?
A: Many organizations are struggling to ensure their work-from-home employees are complying with industry standards and regulations. Tehama has deep audit and compliance capabilities that provide full visibility into all activities that happen while using Tehama. From the moment an Tehama organization is created to the moment it is archived every action is captured via a detailed audit log and session recordings. The audit logs can be searched, exported or viewed via reports within Tehama. Sessions can be viewed in real time or replayed via the session recordings. An additional security and compliance later can be added to ensure geofencing, nationality, etc requirements are adhered to. Tehama can also be deployed within the geographic boundaries of the UK, Canada, USA, Germany, Ireland, Australia, Ireland, and Singapore to ensure data residency.

Q: What are you doing to isolate end-point device risks?
A: Many organisations fear employees and third-parties working from home on shared personal or public wifi networks. The remote teams use these networks with their own devices or work issued laptops. These internet access points are not administered with stringent security requirements or tooling and open up additional threat surfaces with potential malware, man-in-the-middle attacks, bots, or internet throttling. Tehama removes the risks of endpoint device malware intrusion by essentially turning the endpoint devices into dumb-terminals that only receive encryption pixel and images from the virtual desktops hosted in the virtual Tehama Rooms on the cloud. This way, no data is on the laptop and no data can infiltrate the virtual desktops. This is achieved by use of a Teradici PCoIP client customized for Tehama. It provides the richest and most secure experience for a virtual desktop.

Q: How do you prevent data from being lost?
A: When employees work from home one of the biggest concerns is confidential data loss. Most employees are not wired to practice stringent data protection measures. Often they share confidential information via email or other sharing devices. Tehama constrains all of the data sharing into the Tehama Room. Tehama does have a facility to upload and download data to a Room where all activity is logged, so that the Room administrators know who uploaded or downloaded data. This feature can also be turned off so that no data ever enters or leaves the Room from end-user desktops, other than via the approved applications. Tehama Rooms can also be configured to only work with the applications necessary for the tasks, meaning, Rooms can turn off public internet access and / or white list only the sites required to do the work.