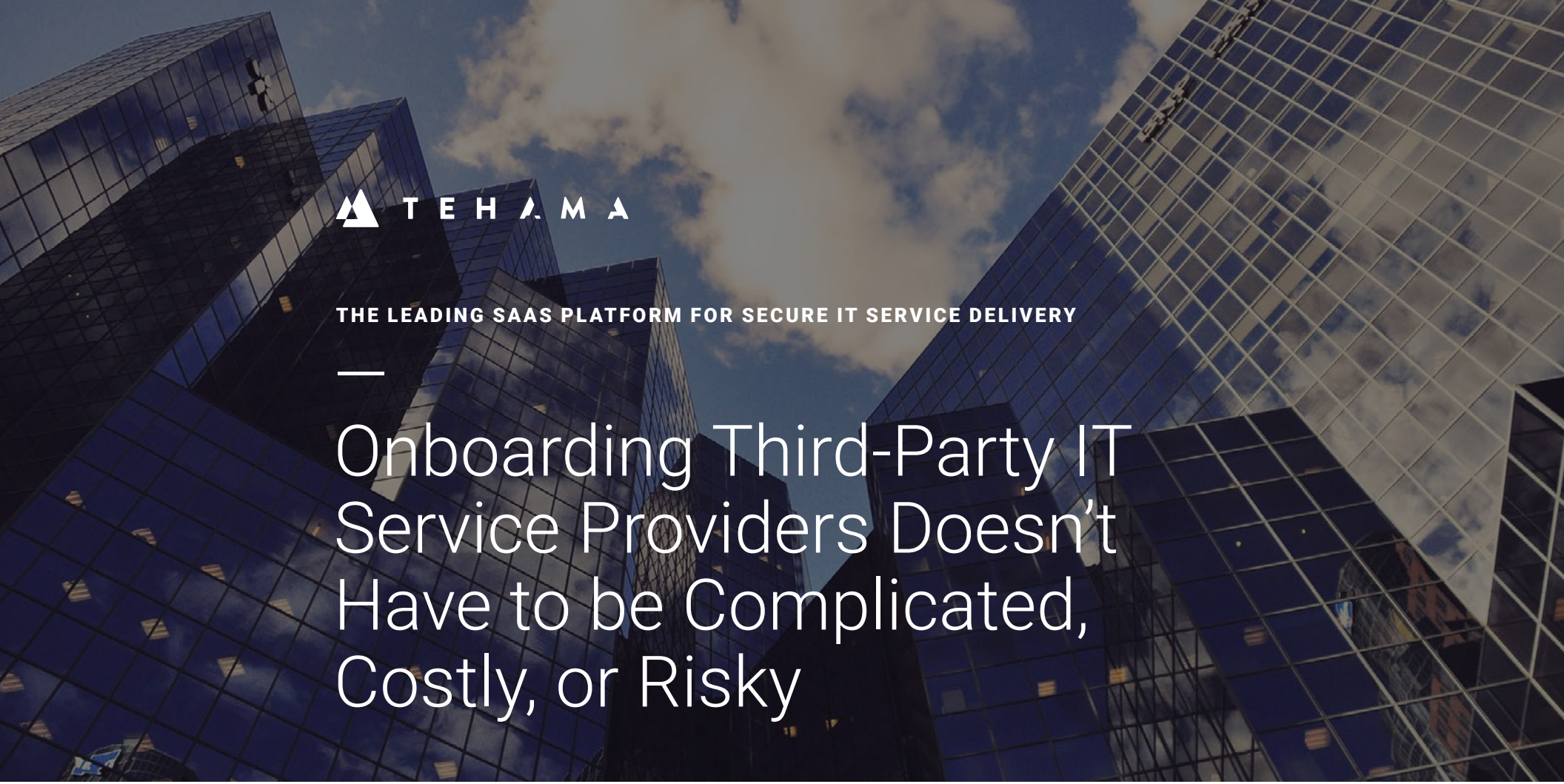


TEHAMA

THE LEADING SAAS PLATFORM FOR SECURE IT SERVICE DELIVERY

Onboarding Third-Party IT Service Providers Doesn't Have to be Complicated, Costly, or Risky

Gene Villeneuve
Senior Vice President of Tehama

This white paper discusses the risks and challenges when hiring third-party IT service providers or providing remote employees network access. This white paper also proposes a solution to secure and simplify the onboarding, management, scaling, securing, and auditing of third-party IT service delivery teams. There are limitations with current VDI, DaaS, and VPN technologies or shipping laptops and this white paper explains the principles of secure perimeters for cloud workspaces, and introduces a solution that allows enterprises to place a high degree of trust in the remote IT service delivery team (vendor) and their endpoint devices.

January 2019

According to the Gartner Research Group, the single biggest challenge Chief Procurement Officers (CPOs) face today is the prolonged time it takes to securely onboard outside organizations and vendors into their information systems and business applications. Onboarding a new vendor can take anywhere from six to nine months. These wait times are inconvenient, create delays in project milestones, undermine the company's innovation trajectory, and are concerning to the CEO as it damages the brand.

Leveraging a global workforce is challenged with complexity and riddled with security risks: from abuse of privileged credentials and data theft to legacy hardware and infrastructure costs and constraints. Virtual Desktop Infrastructure (VDI) and Desktop-as-a-Service (DaaS), jumpboxes, and Virtual Private Networks (VPN) do not provide sufficient protection and do not ensure regulatory compliance is adhered to. Moreover, VPN technology is outdated, costly, hard to manage and still presents endpoint device risks and network risks. Enterprises need to secure, accelerate, and simplify how they onboard external third-party IT service delivery teams and provide access to mission critical and data sensitive systems while mitigating and stopping the cybersecurity risks.

Business Pain

- **Many ad-hoc environments needed**
- **Onboarding new customers takes weeks, months**
- **Unable to meet customers' compliance requirements**

Solution

- **Tehama creates a "clean room" with virtual workspaces, creating a lock between corporate networks and the workspaces, and a secure network communication channel with compliance.**

Business Value

- **Customer onboarding reduced to 3-4 days from weeks**
- **Security and auditing greatly increases customers' satisfaction and is leading to higher value projects**

The single biggest challenge Chief Procurement Officers (CPOs) face today is the prolonged time it takes to securely onboard outside organizations and vendors into their information systems and business applications. Onboarding a new vendor can take anywhere between six to nine months. These wait times are unacceptable, create delays in project milestones, undermine the company's innovation trajectory, and are concerning to the CEO as it damages the brand.

Gartner Research Group states that 50% of IT services will be outsourced by 2020. Global enterprises must grow their labor reach beyond their brick-and-mortar walls to be competitive and agile. Leveraging and growing a global outsourcing team that includes third-party vendors — systems integrators, managed service providers, partners, contractors, Gig economy workers and freelancers - is key to agility and growth, however our connected world of digital business and the security risks have never been greater.

As per recent **Norton** research, the cost of an average data breach to a U.S. company is $7.91 million USD. Verizon reported that 81% of hacking-related breaches leveraged stolen or weak passwords. And in a 2018 **survey on cybersecurity**, 44 percent of respondents found end users to be their company's weakest security link, where 80% of breaches are related to privileged credential abuse.

Engaging a third-party vendor creates additional threat surfaces and challenges such as the following:

- Time to onboard or offboard vendors
- The need for regulatory compliance
- Abuse of privileged credentials
- Legacy hardware and infrastructure management and administration (duty of care)
- Risk of lost or stolen hardware like laptops
- Malware intrusion from untrusted devices
- Intellectual property and data theft, breach, or loss
- Reputational damage

How are the threats to corporate IP and data, businesses, and reputations being protected in your organizations when engaging third-party and contingent workers?

Why Traditional Solutions like VDI, DaaS, VPN and Shipping Laptops are Failing Vendor Onboarding

Virtual Desktop Infrastructure (VDI) hosted on-premises or in a data center is used for remote employee and contractor access by many organizations. Others use Desktop-as-a-Service (DaaS) cloud workspaces: all the major cloud providers offer these. Some organizations develop a hybrid system. Many organizations are still shipping managed laptops to their contractors. And some are using naked VPN software and credentials to grant access to third-party vendors.

VDI is just a point solution

VDI and DaaS are both well established—but they aren't enough. These technologies are little more than unmanaged operating systems (OS) hosted in the cloud, lacking the controls and framework that the IT team places on managed laptops. Cloud-based OSes don't provide multi-factor authentication (MFA) for controlled access, they lack anti-virus tools, and lack a secure communication channel connecting the OSes and end-user compute environments to the enterprise IT assets and infrastructure. Moreover, they lack a mechanism to control and manage privileged credentials.

In addition, VDI and DaaS sourced desktops are lacking the necessary mechanisms to meet any level of regulatory compliance—a very big problem for organizations with stringent compliance requirements, such as those found in Banking, Insurance, Utilities, Transportation, Healthcare, and Government.

VDI and DaaS also lack the core IT infrastructure typical of every enterprise: firewalls, routers, patch and update mechanisms, OS image management, and a host of compliance management and enforcement mechanisms. All of these are needed to perform enterprise development or IT service delivery at a global scale; these are all necessary to offer and support a controlled and maintained end-user compute environment.

VPN risks

VPN technology is outdated, costly and hard to manage. Worse yet, it poses significant threats to corporate networks. Remote programmatic attacks on open network firewall ports are common, hard to patch—and it's even harder to propagate the fix across equipment updates. Once a user's computer is connected by VPN to the corporate network, any malware that may be on the user's system has a direct path for propagation.

Shipping delays for managed desktops

Shipping laptops to consultants and contractors presents additional threats. If a laptop is lost or stolen even modern disk encryption software can't prevent a determined hacker to access sensitive data. Laptops in the hands of contractors still can't be fully managed if the contractor decides to connect to a public WiFi network in a café or hotel or wherever. If the contractor engages in risky end user behavior they risk compromising the customer's laptop with malware, keystroke loggers or other malicious software that could infiltrate the corporate systems.

However, providing third-parties and remote employees with access to internal corporate networks, cloud applications, or hybrid solutions is still a necessary requirement.

> "You just signed a contract with an IT off-shore outsourcer for 50 consultants. Is your intellectual property safe?"
>
> **Álvaro Hernández Tortosa**
> FOUNDER, ONGRES

What's the Solution to These Limitations?

Organizations need a solution that secures and simplifies onboarding, managing, scaling, and auditing third-party vendors. The traditional methods available on the market today are failing to support organizations' requirements for fast delivery of projects, access to global and diverse skills, while maintaining security and compliance. The following section proposes a new solution to secure and simplify IT service delivery.

Introducing Tehama to Secure and Simplify IT Service Delivery

In today's fast paced world with pressing business requirements and a growing global talent pool, organizations are adopting strategic IT outsourcing, tactical outsourcing, and freelancer strategies to increase their project delivery velocity and flexibility. However, onboarding systems and processes remains complicated and delays time to productivity. Figure 1 outlines the lengthy steps and processed required in many organizations today before project work can begin. ***See figure 1.***

Tehama was created with the explicit purpose to help organizations quickly, and securely, onboard third-party and contingent vendors at the speed of SaaS, with strong security and compliance capabilities, at a fraction of the costs of today's systems. Tehama is a comprehensive Software-as-a-Service (SaaS) platform that provides the capabilities needed for securely connecting contingent employees and contractors to corporate networks. In a single, holistic SaaS platform, Tehama offers a solution to onboard, manage, scale, secure, and audit third-party vendors while maintaining compliance with SOC 2 Type II, MFA-controlled access to cloud VDI and DaaS end-user compute environments which meet the regulatory requirements typical of the strictest of industries: SOC 2 Type II, GDPR, FIPS. Figure 2 outlines the core benefit of Tehama to accelerating and securing all third-party IT service vendor work. ***See Figure 2.***

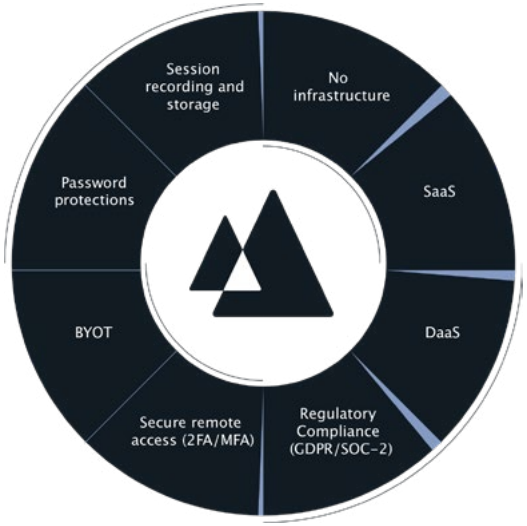
Quickly Onboard / Offboard and Manage Third-Party Vendors

Once an organization selects a vendor, they need to follow a formal IT onboarding process. This requires credentials to be created, access to systems defined, approvals within the buying organizations' management and compliance hierarchy made, and often managed laptops provisioned. VPN credentials and VDI or DaaS systems also need to be created. Often these steps take weeks to months and the project managers become frustrated and fall under mounting pressure from management and internal customer scrutiny.

Figure 1: Current Solutions to onboard third-party vendors are lengthy and delay time to *productivity.*

Figure 2: Tehama accelerates time to productivity.

Tehama's Comprehensive SaaS Platform



Complete control over user access to secure perimeters

With Tehama, the buying organization establishes an edge computing environment with application access only to systems required as defined in the project contract. This step involves creating a Tehama Room or a secured virtual perimeter on the cloud and defining the network and application isolation rules to grant access only to the systems defined in the contract. The Room can be defined within minutes and is managed exclusively by the buying organization. Access policies such as Secret Clearance, FIPS, OSFI, SOC 2 Type II, GDPR can be defined within the context of the Room, thus ensuring compliance is adhered to while delivering the project.

Once the Tehama Room is defined, the project manager at the buying organization works with the third-party vendor customer manager to define who will be assigned to the project. The Room owner (buying organization) and the third-party vendor follow a simple workflow to approve and grant each contractor access to the Tehama Room. Once access is granted the project manager assigns virtual desktops (DaaS) to the contractors with the right CPU, memory, and hard-disk requirements (Microsoft Windows or Linux). Each virtual desktop can be provisioned in 5-10 minutes and done in parallel, meaning, if 50 contractors each require a desktop, all 50 can be provisioned within 10 minutes.

At any given time within the project the Room owner can remove a contractor to quickly offboard them, or once the contract is complete the Room owner can simply turn off Room access and prevent all future access to the corporate network or Room.

Scale Third-Party Vendor Teams

As third-party projects get defined, grow, evolve often the scope changes or more contractors need to be assigned. Tehama was designed to help scale contractors and contingent workforces by quickly adding sub-contractors and provisioning desktops customized for the project work. Tehama's elastic scaling gives Room owners the ability to ramp up and down resources as needed.

Adding sub-contractors and additional Room members can be managed directly by the Room owner. If the Room owner (buying organization) needs to hire additional contractors, or add a second or third IT service provider, they can be quickly added and granted access to the Room following the simple and accelerated process to onboard new members. Once new organizations and members are added to the Room the teams can collaborate and share work to continue delivering the project.

Customizable end-user compute desktops

The Room owner can also create custom desktop images (Windows/Linux) complete with the tooling required to be productive on the contract such as IDE tools, collaboration tools like Slack, HipChat, productivity tools, and endpoint device management tools like detection intrusion desktop agents. By defining custom desktop images organizations can quickly add new members and have them be productive within minutes of receiving access to the newly provisioning custom desktop images. This way organizations can save the weeks typically spent buying, configuring, managing and shipping laptops to contractors. More importantly, by eliminating the costs of managed laptops organizations dramatically reduce the overall costs of the project and avoid any risks of laptops being stolen, lost, or abused.

Secure Third-Party Vendor Work

The number one cause of data breaches or data loss is due to privileged credential abuse and lost or stolen hardware. According to **Breach Level Index**, 80% of data breaches are due to credential abuse and every 53 seconds a laptop is lost or stolen. Engaging with third-party IT service providers requires extra care and caution when granting access to mission critical and data sensitive information.

Policy-based Access Control

With Tehama, all users (Room members) are vetted by both the Room owner (Buying organization) and third-party vendor through a defined approval and security policy process. Elements such as nationality, clearance levels, policies, and physical location can be defined to restrict and secure access only to those that adhere to those requirements. For instance, a Tehama Room can define policies that will reject individuals from a specific geographic region or without having a defined citizenship. Additional layers of login security can be applied with Tehama's deep partnerships with authentication tools that further restrict end user access based on physical location such as a policy that states only users within 50 miles of a given location can log into a Tehama Room.

Integrate with IAM Tools

Equally important is using multi-factor authentication as a way to further enforce security. Every user must use a multi-factor authentication process to log into a Tehama Room. Buying organizations can use third-party platforms such as Okta, Ping, Duo, or any SAML, SCIM, or AD protocols to authenticate users via those mechanisms, thus giving the buyer organization additional controls over user access rights and privileges,while integrating with tooling and processes currently in place.

All data contained within the perimeter

The additional advantage of the Tehama platform is that access is endpoint device agnostic. Google Chromebook, Mac OS, Windows, or Linux computers or laptops may all be used for accessing the Tehama platform, allowing third party contractors to launch a virtual desktop. All work performed in the Tehama Room is done in the virtual and secured perimeter on the cloud, thus providing additional assurances that all work performed is secured, encrypted in flight, and at rest. Once the user logs off, all work remains locked and encrypted in the secured perimeter: if the contractor's laptop is stolen or compromised organizations are protected from data breach, loss, or intellectual property theft. Due to this smart design and implementation, any malicious software that may compromise the physical endpoint device cannot penetrate into the virtual Tehama Room desktops. All files uploaded into the Room go through an approval process and malicious software or virus checks.

Zero-trust network segmentation

Equally important is the Room owner's ability to lock down firewall ports and system access to ensure only access to systems granted in the contract are accessible from within the Room, meaning the Room owner can ensure contractors cannot launch Facebook, Hotmail, Gmail, or other social media sites. Room owners can also turn off internet access entirely so as to only grant access to the application being worked on as defined in the contract.

No sharing of privileged credentials

When it comes to securing mission critical and data-sensitive systems, organizations must also protect their privileged administrative credentials. Tehama Rooms are built with a Secrets Vault that only grants access to those required to use the credentials when needed. The Secrets Vault obfuscates all passwords from the Room members; only Room administrators have control of the passwords. The benefit to organizations is that third-party contractors and sub-contractors in the Room cannot see or share the passwords, thus providing additional levels of protection from credential and information abuse.

The Tehama Rooms (secure perimeters) are established around cloud workspaces and secure all work done. With the deep Tehama zero-trust security and infrastructure framework surrounding and supporting these end-user compute environments, they can be trusted as secure virtual extensions of a corporate organization, and accessible, in a trusted manner, by global employees and contractors. Moreover, understanding that all data in the rooms is encrypted with 256 bit encryption at rest and in transit provides additional levels of security for both the buying organization and the third-party service vendor.

Third-Party Audit and Compliance Simplified

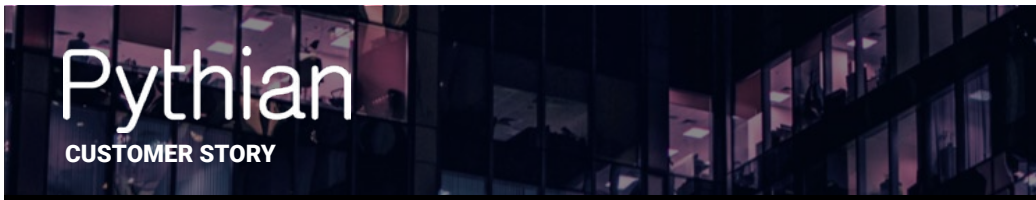
Many third-party IT service providers have SOC 2 Type I and II certifications but does this mean how they implement and manage the delivery of the contract work adheres to the compliance controls? Every year vendor management teams need to audit their third-party IT service providers to ensure the project is and was delivered according to the compliance regimen outlined in the contract. Often these audit costs are steep and require teams of auditors to travel for onsite audits. Moreover, new regulations like GDPR and 23 NYCRR 500 section 11 are forcing additional controls and reporting requirements on organizations to show they have met compliance obligations when dealing with third-party service providers.

All activity is logged

With Tehama, every action performed from the moment a Room is created to the moment a Room is decommissioned or archived is logged. Moreover, every Room member's action is perfectly witnessed in real-time and recorded just like closed circuit television cameras in banks. By perfectly witnessing all work performed, the Room owner can reconstruct any breach scene or observe in real-time what the contractors are doing. From a single location, a Room owner can observe in real-time any work being delivered inside a Tehama Room from any contractor anywhere in the world. This feature not only improves worker productivity and focus but also allows for collaboration between the Room owners and the contractors. The recordings can also be used by auditors to replay any events over the duration of a contract. They also help protect the both the customer and the third-party in cases of contract disputes or breaches.

The deep auditing also counts hours of work delivered by whom and when, what resources they accessed, what credentials they used, what files they shared and any other activity performed while in the Room. With Tehama's deep audit and compliance features, the Room owners can ensure the contract is delivered with compliance and all logs and session recordings can be handed over to auditors for quick and continuous auditing. Equally important is the ability to externalize the audit logs to popular enterprise audit and SIEM tools like Splunk and QRadar.

With Tehama, organizations increase their confidence in third-party vendor audit and compliance with a unique and industry first trust platform. By providing trust through transparency, organizations can adhere to regulatory compliance reporting obligations when engaging contingent workers.



Pythian

CUSTOMER STORY

Business Pain

- **Global team of over 300 consultants in over 150 cities**
- **Needed to deliver services with a 24X7 365 day secure platform without forcing customers to ship laptops to them**

Solution

- **Compliance and precise access controls allow for a high degree of trust between Pythian and Pythian global clients**

Business Value

- **Ability to quickly onboard a global IT Services team to deliver work for over 200 customers.**
- **Deep compliance and audit visibility for Pythian customers.**

Acronyms

CAPEX	Capital Expenditure
DaaS	Desktop-as-a-Service
IAM	Integrated Access Management
MFA	Multi-Factor Authentication
OS	Operating System
PAM	Privileged Access Management
PSM	Privileged Service Management
SaaS	Software-as-a-Service
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network
AD	Active Directory
SIEM	Security information and event management
SCIM	System for Cross-domain Identity Management
SAML	Security Assertion Markup Language

Conclusion

Leveraging a global workforce is imperative to the success of organizations yet they are currently challenged with time delays when onboarding third-party vendors. Moreover, hiring contingent workers and executing an IT outsourcing strategy is riddled with security risks: from abuse of privileged credentials, malware intrusion, and data and intellectual property loss risks, to legacy hardware and infrastructure constraints. VDI and DaaS, and VPN don't provide sufficient protection and also don't ensure the regulatory compliance that is required. Shipping laptops to contractors adds additional costs to the contracts, delays start times, and increases security risks with endpoint device malware intrusion or lost or stolen devices. A solution to accelerate onboarding, managing, scaling, securing, and auditing third-party IT services vendors work is imperative to the success of organizations.

Tehama, a secure, SOC 2 Type II, SaaS Solution that provides the (secure perimeters around cloud workspaces) necessary capabilities with application isolation and forensic auditing needed to avoid the security risks and to give businesses the agility they need to quickly hire, onboard, manage, scale, secure, and audit a global workforce of third-party contractors or remote employees.

By following the principles outlined in this white paper and using Tehama organizations can quickly onboard and manage third-parties to accelerate project work, protect corporate data and reputations, adhere to important industry audit and compliance regulations, and decrease the overall costs of managing third-party vendors.

To learn more about Tehama, visit www.tehama.io

Challenges with current tools

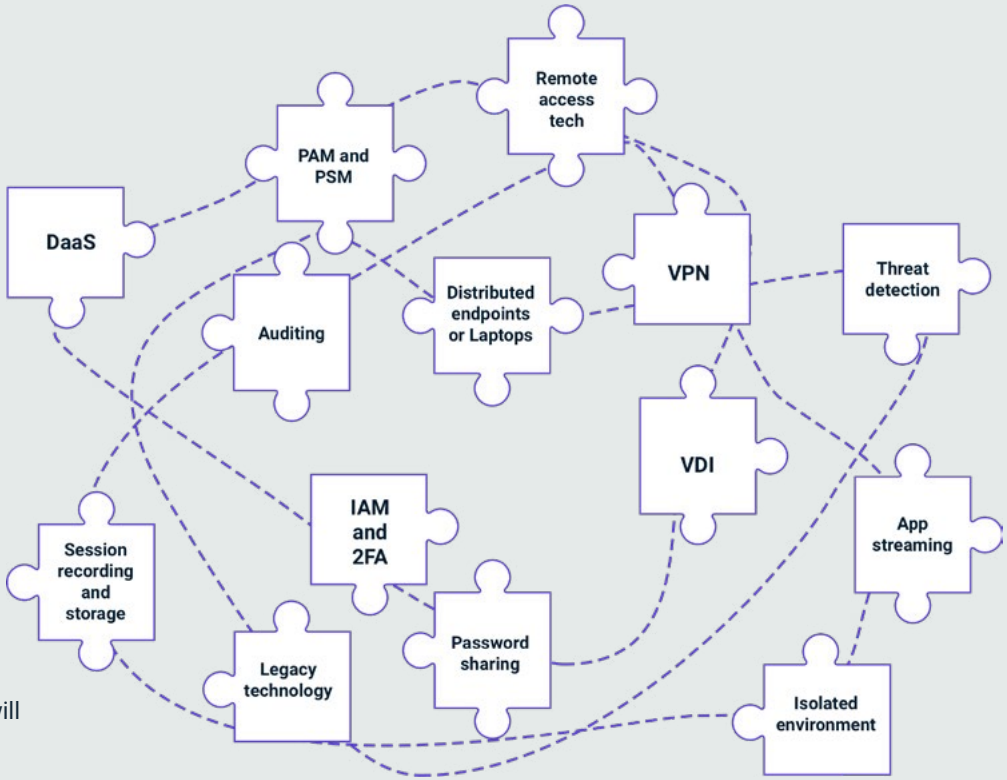
There are many tool vendors available today that offer some of the capabilities noted within this white paper, however assembling all of the tooling to meet this guidance places significant burden on the in-house IT team.

There are numerous tools and capabilities required:

- VDI, DaaS
- IAM
- MFA
- Privileged Access Management (PAM)
- Privileged Service Management (PSM)
- Virtual Private Networks (VPN)

There is no one single vendor that offers all the requirements necessary for securely connecting remote employees and contractors to corporate networks in a single product like Tehama. Assembling all the capabilities into a functional, and manageable suite will be prohibitively expensive, time consuming, and will contain a high level of risk as integration gaps between the subset capabilities will be undocumented and invisible, making them hard to uncover under penetration testing.

In addition, there will be pricing and licensing complexities with the unavoidable multi-vendor approach.



About Tehama

—

Tehama is the fastest, easiest, most secure way to deploy a virtual workforce. With our Virtual Office as a Service 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.

For more information, visit **tehama.io**.

About the Author

—

Gene Villeneuve, SVP Tehama

Gene directs the strategy of the Tehama unit at Pythian. He is a seasoned executive with 25 years of experience at Cognos, SAP, and IBM. Gene is known as a disruptor & innovator with several successful new product launches over his career.