

An Enterprise Guide to your new office The Virtual Office as a Service (OaaS)

By Jaymes Davis
Director of Product Strategy, Tehama

 partner
network

Advanced
Technology
Partner

End User Computing



Going mobile: Around 70 per cent of large enterprises believe most employees won't have a traditional, physical office space by 2021, according to a recent Everest Group report.

1 The office... evolved

The office as we know it is changing rapidly.

This has been true for years, of course, ever since the first digital computers shook up the modern workplace. But as new technologies, processes, and ways of thinking about work have evolved, this digital transformation of the modern office has only accelerated. Indeed, the next phase may not even involve what we typically think of as “offices” at all – a recent [Everest Group report](#)¹ indicates that close to 70 per cent of large enterprises believe most employees won't have a traditional, physical office space by 2021.

That's a lot of employees to manage who don't have a well-defined, company-supplied office space. Complicating matters is that most of these workers require the very same level of secured privileged access to corporate networks and information systems as their in-office counterparts.

Why a cloud-based workforce is so compelling

These societal and workplace changes are big reasons why enterprises are increasingly transitioning to a cloud-based workforce. By using a secure and compliant cloud VDI (virtual desktop infrastructure) to facilitate a global workforce they're able to save money, enhance agility, and reduce risk when deploying and managing secure workspaces for both remote and in-office employees (as well as partners and third-party contractors). That means a secure service delivery platform through software-controlled, [secure workspaces](#)² with firewalls, storage, end-user compute infrastructure, and security and access policies all managed from a single platform.



Secure and compliant cloud VDI has in a relatively short time already proven itself superior to other secure networking and desktop infrastructure options, including:

On-premise VDI or cloud desktop as a service (DaaS):

While these technologies can be effective, they're not even close to that right out of the box. Neither include critical features like multi-factor authentication (MFA), anti-virus tools, or secure channels to connect to information systems. They also don't include compliance mechanisms and are missing important security features like firewalls and automated patches and updates.

Virtual private networks

(VPN): At one time VPN was considered state-of-the-art, but that was a long time ago. These days VPN is relatively costly, hard to patch and propagate fixes across multiple devices, and not very secure: once an end point is connected to your system via VPN, any malicious files hanging around on that computer have a clear path to the goal (in this case, your systems).

Shipping laptops:

Some organizations still rely on the old-fashioned method of physically couriering laptops to remote workers, but at this point, the drawbacks here are pretty well-documented: shipped laptops can get damaged en route, or (even worse) go missing – a situation ripe for data theft. They're also hard to fully manage and keep secure if contractors engage in risky online behaviour. Equally challenging is recovering laptops from employees and contractors at the end of an assignment.

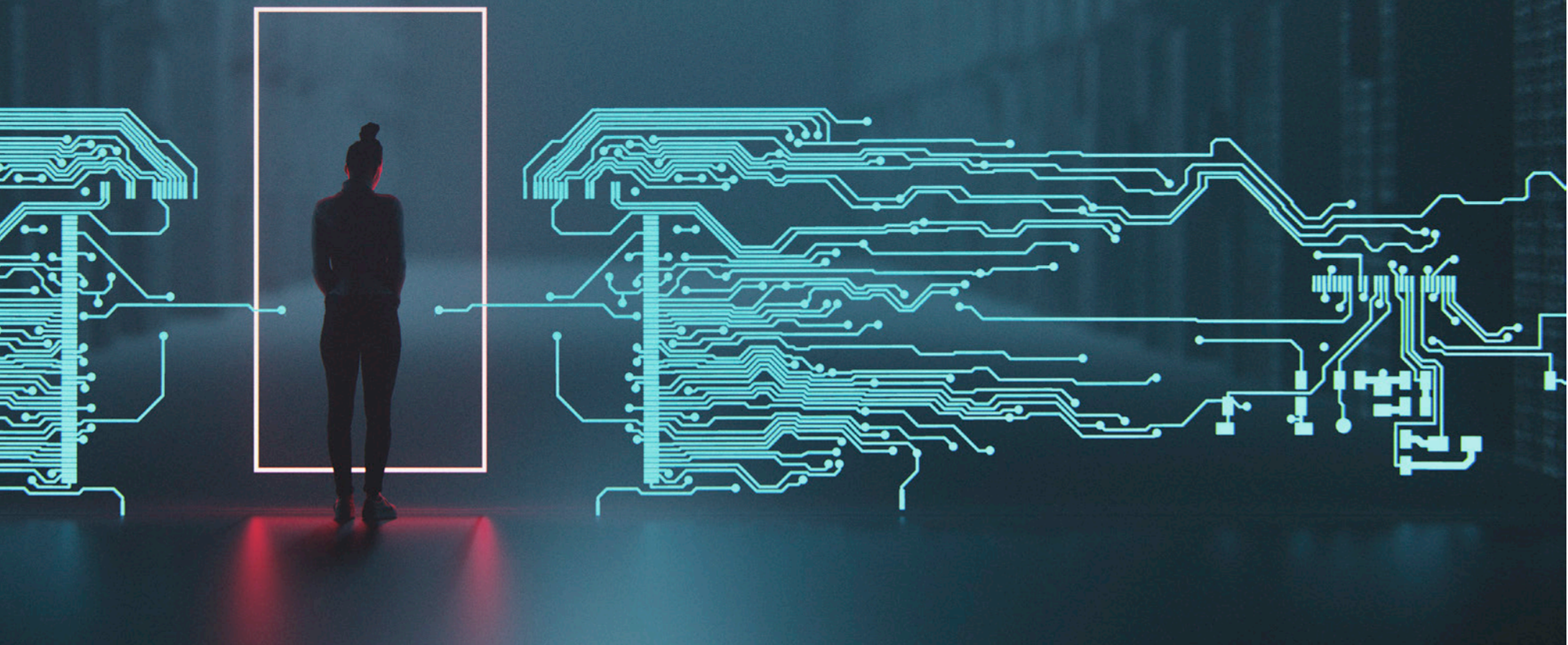
The above alternatives all have another big drawback: their speed of deployment (or lack thereof). Anyone who has provisioned secure access to company information systems and business applications for third parties knows how time consuming it can be: in many cases onboarding a new vendor, employee, or contract worker can take more than half a year, leading to frustrated staff, delayed projects and damage to the company's brand.

With this in mind, it probably goes without saying that enterprises must find ways to accelerate and simplify the onboarding of external organizations and partners, while also providing secure access to mission critical and data sensitive systems.

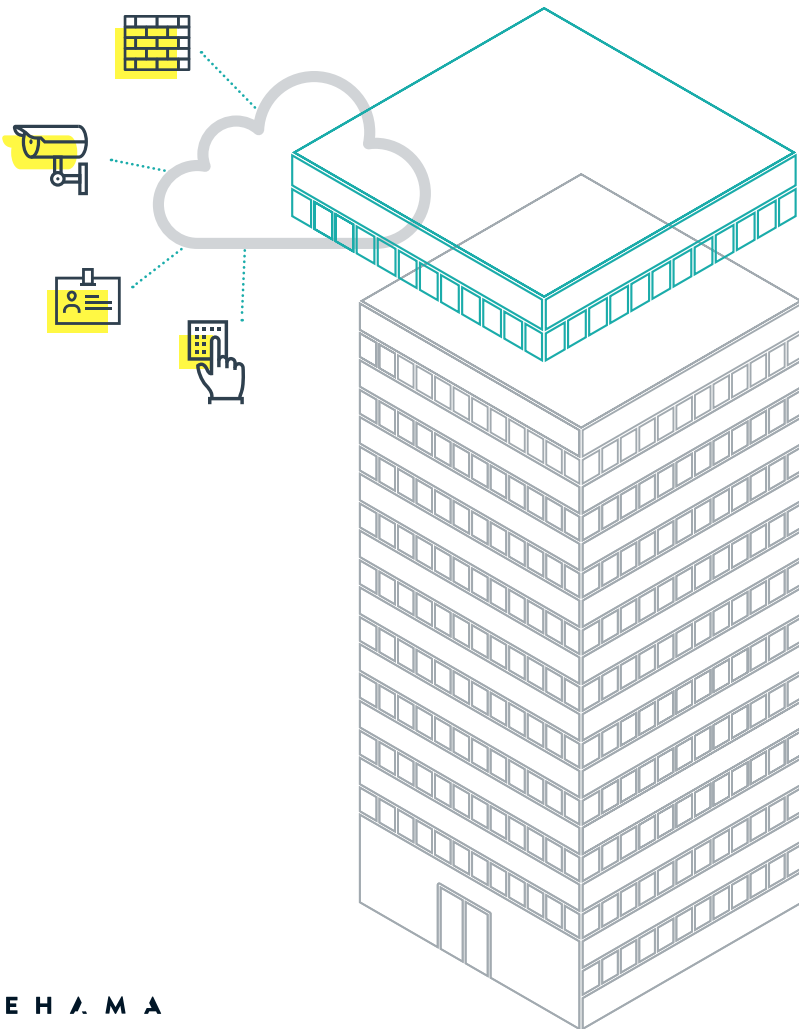
In many cases onboarding a new vendor can take more than half a year, leading to frustrated staff, delayed projects, and damage to the company's brand.

2 Secure and compliant cloud VDI: Your Virtual Office-as-a-Service (OaaS)

The number of companies running on-premise server rooms are dwindling rapidly in favour of those with their data in the cloud. And for good reason: migrating to a managed cloud service can help lower costs while increasing flexibility, scalability, and security. The same can be said for a cloud-based workforce using secure and compliant cloud VDI.



Secure and compliant cloud VDI is like a virtual 11th floor of your office's 10-storey building – a virtual office as-a-service. Because onboarding and scaling global teams takes minutes instead of months, bringing your latest contractor online doesn't take much more time than riding the elevator to the next floor. And thanks to its robust security services and features, secure and compliant cloud VDI virtually mimics the physical security posture of your company's brick-and-mortar office, including:



i) Secure perimeters

Secure perimeters, automated encryption, continuous malware protection, and network segregation act very much like the solid walls of a physical office.

ii) Session recordings and activity streams

Down-to-the-keystroke, perfectly witnessed recordings of work sessions within secure online **rooms** (along with the ability to play back and **view** all activities that have gone on) are like the CCTV cameras that populate most modern office buildings.

iii) Fast onboarding

We alluded to this above, but onboarding remote employees takes about the same amount of time and effort as does the physical onboarding of an in-office employee by HR (minus all the awkward greetings and handshakes).

iv) Credentials management

Strict access requirements for system or application access, including MFA and least privilege permissions, act like key fob or badge systems at your office door to ensure employee access only. Anything else is akin to handing out office keys to a complete stranger.

Strict access requirements for system or application access, including MFA and least privilege permissions, act like key fob or badge systems at your office door to ensure employee access only.

3 Why a cloud-based workforce? Some use cases to consider

A cloud-based workforce through secure and compliant cloud VDI is helping enterprises in every vertical who require a cost-effective solution for issues like global workforce enablement, supply chain security, personally identifiable information (PII) & intellectual property (IP) protection, high-risk region operations, and business continuity on-demand and within minutes.

Supply Chain Security

A recent Ponemon Institute survey **indicated**³ that while security and risk professionals share confidential and sensitive information with an average of 583 third parties each, only around one-third of them keep a full inventory of these connections (for Nth connections, or third parties of third parties, that number shrinks to 15 per cent). Perhaps the most powerful benefit of a secure and compliant cloud VDI solution is the security it can provide your **services supply chain**⁴ thanks to features like built-in automated compliance tools and the credentials vault, lowering the risk posed to corporate supply chains by small vendors (and all-too-common employee “workarounds” to strict processes).

According to Gartner Inc.,⁵ the most significant challenge faced by most Chief Procurement Officers (CPOs) is the time and complexity involved in onboarding third-party partners and vendors. Added to these challenges are the inherent security risks involved: credential abuse, data theft, legacy hardware or software vulnerabilities, and cost constraints are all conspiring to poke holes in your security perimeter. Secure and compliant cloud VDI enables enterprises to securely onboard third-party vendors and consultants in just minutes, allowing you to quickly spin up virtual private rooms where teams can collaborate on virtual desktops.

Global Workforce Enablement

Experts have **been saying**⁶ for a while now that end-user computing (EUC) is on the edge of major disruption, with industry leaders like Cisco **predicting**⁷ the number of embedded networked sensors will reach one trillion by 2022. That’s a ton of extra devices for enterprises to upgrade, secure and manage – especially for companies with large, remote workforces spread across various geographies – which is a big factor why end-user computing is quickly becoming too costly and complex for many organizations. It’s also why many of these same organizations are implementing secure and compliant cloud VDI – it’s less costly, and far easier and faster to implement and manage, for the reasons we’ve mentioned above.

Compliance through PII & IP Protection

Compliance has been a must for companies in heavily regulated industries like banking, financial services, health care, energy and utilities for decades. But thanks to new, strict privacy rules like the General Data Protection Regulation (**GDPR**⁸) and California Consumer Privacy Act (**CCPA**⁹), virtually every company with an online presence now needs to be concerned about compliance – and it's a lot less expensive to get and stay compliant than it is to be found **non-compliant**¹⁰. Your desktop infrastructure solution must be SOC 2 Type II compliant by including built-in compliance tools able to meet the most stringent rules such as those set out by HIPAA, FIPS, PIPEDA, and NERC.

Business Continuity (BC) and Disaster Recovery (DR)

DaaS has been the go-to desktop infrastructure solution for BC and **DR** ever since it replaced unsecure personal devices and residential WiFi networks. But DaaS, too, has a fatal flaw: these systems assume everything inside an organization's network is trustworthy, a blind spot that's being increasingly challenged by sophisticated attacks and insider threats. A secure and compliant cloud VDI secure service delivery platform can perform under pressure when disaster strikes by:

- Providing an on-demand, backup virtual workplace
- Secure, remote access to corporate systems
- Detailed logging and auditing to ensure granular control over the remote work environment

High Risk Region Operations

The same features that make secure and compliant cloud VDI such a solid BC and DR platform are why it's tailor-made for companies with operations in high-risk regions or geographies such as those prone to natural disasters, political instability and even military operations. Today's global talent is scattered across the globe – often in politically distressed areas – yet organizations must leverage that talent to meet their business objectives. Secure and compliant cloud VDI enables organizations to quickly leverage specialized skills from any location on the planet with an internet connection, without fear or malware, spyware, or data breaches thanks to secure and compliant cloud VDI's compliance and security barriers and layers.



Tehama: The world's first and only Virtual OaaS

The reality, however, is that most cloud VDI vendors simply don't or can't offer the security or management options required to be considered a true Virtual OaaS. Tehama's secure and compliant cloud VDI solution provides a secure service delivery platform that's so unique and effective, it's practically created a new technology category by saving users time and money on day one, while eliminating the technical and logistical complexity of shipping laptops or building out VDI infrastructure, enable VPNs, and establishing physical offices.

Tehama eliminates roadblocks by making it efficient and secure to access and engage a global workforce, automating the management of vendors, employees, and contract workers and ensuring all access – and work completed on the platform – is secure, monitored and audited. Tehama provides secure and efficient onboarding of talent while easing the burden of regulatory compliance – getting developers and IT staff back to true productivity.

Contact us for more information on what Tehama can do for your organization, or visit us online for your **30-day free trial.**

Resources

- 1 <https://www.information-age.com/digital-transformation-and-the-workplace-123478275/>
- 2 tehama.io
- 3 <https://info.tehama.io/blog/five-ways-to-keep-a-lid-on-supply-chain-security>
- 4 <https://info.tehama.io/blog/building-a-business-case-for-services-supply-chain-security>
- 5 Gartner Vision 2019 Sourcing Procurement & Vendor Management
- 6 <https://www.forbes.com/sites/forbestechcouncil/2018/05/21/five-reasons-end-user-computing-is-on-the-edge-of-disruption/#50397963441b>
- 7 https://www.huffpost.com/entry/cisco-enterprises-are-leading-the-internet-of-things_b_59a41fcee4b0a62d0987b0c6?guccounter=1
- 8 <https://gdpr-info.eu/>
- 9 https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act
- 10 https://en.wikipedia.org/wiki/GDPR_fines_and_notices

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.

