



citrix®



Beyond virtual desktops: rethinking secure application access

Discover how organisations are
modernising secure application access
by evolving existing VDI estates

The next phase of workplace access

Workplace IT is under growing pressure from multiple directions. Security threats continue to evolve, compliance requirements are becoming more demanding, cloud costs remain under scrutiny, and increasingly complex environments are driving up operational overheads.

Yet organisations must respond in a way that strengthens governance, maintains control and improves cost efficiency, without compromising the seamless access to applications and data that employees expect, wherever and however they work.

Against this backdrop, many organisations are reassessing how secure access is delivered. While virtual desktop infrastructure (VDI) has provided a reliable foundation for secure workplace delivery for three decades. Many organisations still rely on VPNs (virtual private networks) to extend network access to remote users. However, VPNs typically grant broad network-level access rather than application-specific access, increasing the attack surface, while making VPN credentials a common target for attackers.

The rise of hybrid working, cloud adoption and zero-trust security principles is driving interest in more identity-led, application-centric approaches.

For many, the opportunity lies not in replacing existing platforms, but in extracting greater value from them.



Rather than replacing existing environments, organisations should focus on modernising in a way that is both pragmatic and cost-effective,”

Cliff Mann, Workplace VDI Practice Lead at Computacenter.

By combining strategic guidance with a clear understanding of existing environments, organisations can identify practical steps to modernise secure access, reduce complexity and improve operational efficiency. This approach will enable them to establish a workplace strategy that better aligns security, user experience and commercial objectives, while maximising the value of existing investments.



Converging pressures reshaping secure access

The relationship between security, operational efficiency and commercial sustainability has shifted.

While these were once treated as separate concerns and dealt with independently, today they are recognised as interconnected security decisions directly affect operational efficiency, business resilience and the risk of financial penalties when controls fall short. Gartner's CIO Leadership Perspective Survey 2026¹ shows that security and risk management is the top priority within the CIO function, for the third year running, with increasing operational efficiencies and productivity as the CIOs enterprise priority.

At a time when budgets are restricted, IT departments are also subject to growing scrutiny around cloud and operational spend, increasing the focus on ensuring that every investment delivers measurable value and predictable costs. Compounding this challenge, organisations are facing heightened complexity.



Many organisations are running a mix of cloud and on-premises infrastructure that wasn't designed to work together, with access policies, identity controls and management tools that have evolved over time. This has left IT departments with greater security risks and operational inefficiencies, with more surfaces to protect, more tools to maintain, and more teams required to keep it all running."

Nicolas Sharp, Head of Workplace Sales at Computacenter.

Reducing friction without losing control

In parallel, expectations around secure access have grown, with users showing less tolerance for friction. Employees working across locations, devices and applications expect fast, consistent access without the delays and workarounds associated with earlier remote access models. When access is cumbersome, users often look for alternative solutions, increasing the risk of shadow IT. To minimise this risk, organisations must strike the right balance between control and usability.

For IT and security teams, balancing these competing priorities remains a significant challenge: strengthening governance without increasing management overhead; improving visibility without adding to tool sprawl; and reducing costs without compromising resilience.

¹ 2026 CIO Leadership Perspectives, Gartner, March 2026.



Moving beyond traditional VDI to secure application access

The organisations navigating these challenges most effectively are those moving away from perimeter-based, device-centric models toward approaches built around identity and application access.

This enables them to provide users with seamless access while continuously verifying identity and permissions in line with zero-trust principles and maintaining a leaner underlying infrastructure.

“For organisations that have built their workplace strategy around VDI, the question is not whether to replace it. VDI has delivered real value: centralised control, simplified compliance and consistent access across managed devices,” comments Sharp. “What organisations now need to do is build on those strengths and modernise their approach to meet today’s requirements.”

The rise of application-centric access

Organisations are increasingly prioritising secure application access, simplified workplace delivery and more adaptable workforce access models, without adding to operational complexity. This means that application and data delivery that once needed to be device-centric now needs to be delivered through more flexible, identity-led models. Browser-based access is maturing rapidly, reducing endpoint dependency without sacrificing security or governance. And as workforces have become more distributed, the operational overhead of maintaining traditional VDI environments at scale is prompting organisations to look for ways to simplify.

With models that are more application-centric, users get secure, consistent access to what they need regardless of device or location, and IT teams can retain the visibility and control they require without managing unnecessary complexity. This also ties into moving from traditional security of trusting a managed network perimeter to a zero-trust approach that involves continuous, policy-driven verification that travels with the user.

“Organisations can modernise incrementally by building on existing investments, addressing capability gaps and improving the user experience where friction is greatest,” suggests Mann. “The result is a workplace strategy that delivers greater agility and cost predictability while bringing security, operations and workforce experience into closer alignment.”



Unlocking greater value from existing investments

Effective optimisation begins with visibility.

Yet gaining a clear understanding of workplace, access and endpoint environments is not always straightforward. Visibility across workplaces, access and endpoint environments is often fragmented, making it difficult to identify where inefficiencies are compounding costs, where security posture has drifted, or where users are experiencing friction that could be reduced.

Without clarity, modernisation efforts risk addressing symptoms rather than root causes, and investment decisions get made without the evidence to support them. "A structured approach to estate assessment reveals what's already working, what's underperforming and where the greatest opportunities lie," explains Mann. "By building a clear picture of how environments are configured, how applications are accessed and how users actually work, organisations can identify the highest-value opportunities for optimisation."

Realising the full potential of Citrix

For organisations running Citrix environments, an assessment-led approach can uncover significant opportunities to improve performance, security and cost efficiency. Citrix offers more than just a point solution for virtual desktops, but a complete platform for workplace technology. Many Citrix estates have capabilities that are either underused or not fully aligned with current business requirements, creating a gap between the value the platform can deliver, and the value organisations currently realise. Closing that gap does not necessarily require new technology investments; it requires the expertise to identify, prioritise and activate existing capabilities.

User profiling and persona analysis can reveal where users are over-provisioned and where access policies no longer reflect actual working patterns.

Access policy reviews often identify opportunities to simplify administration and reduce complexity, while security posture assessments help address control gaps and strengthen resilience. Estate assessments can also highlight opportunities to extend device lifecycles and optimise infrastructure utilisation.

Through ongoing optimisation, renewal planning and long-term workplace strategy, organisations can make more informed investment decisions and direct resources towards the areas that deliver the greatest business impact. This helps establish a workplace environment that is more secure, efficient and cost-predictable, while remaining aligned to evolving business priorities, workforce expectations and security requirements.



Achieving cost predictability without compromising flexibility

As workspace environments have become more complex, so too have the commercial models that support them.



Licensing arrangements that made sense when infrastructure was mainly on-premises have become harder to manage as more workloads reside in the cloud, consumption patterns change and the relationship between infrastructure, platforms and access services becomes more interdependent,”

Nicolas Sharp, Head of Workplace Sales at Computacenter.

For many organisations, the pace of change in workplace technology has made costs harder to forecast and control. Yet IT leaders are increasingly expected to provide clear visibility of technology spend over the next three to five years.

When costs are unpredictable, budget planning becomes more difficult, investment decisions are delayed and the ability to deliver strategic initiatives can be hindered.

As a result, organisations are placing greater emphasis on licensing and consumption models that improve visibility, simplify management and provide the flexibility to adapt as business requirements change. They need to create a more predictable and sustainable foundation for secure access and digital workspace delivery.

Services-led support can play an important role in achieving this. By combining licensing expertise with ongoing assessment, optimisation and strategic guidance, organisations can ensure that commercial models remain aligned with operational requirements and future growth plans. The right partner can also help simplify implementation and management, maximise the value of existing investments and support continuous improvement, enabling organisations to balance cost control, operational efficiency and user experience over the long term.



Citrix Platform Flex

Citrix Platform Flex introduces a flexible, consumption-based model that supports a range of application delivery scenarios, rather than being limited to traditional VDI workloads. The platform enables organisations to align access, security, and performance to distinct user requirements through a persona-based approach, replacing rigid, one-size-fits-all models.

By aligning costs to actual usage, Platform Flex provides greater financial control while reducing over provisioning and underutilisation. This approach supports consistent user experience, operational efficiency, and scalability across on-premises, cloud, and hybrid environments.



The future of secure access and workplace delivery

The future workplace model is lighter, more integrated and built around application-centric access, requiring fewer resources while embedding security more seamlessly into the user experience.

Browser-based access models play an important role in this evolution. As the browser matures as a secure delivery mechanism, it reduces reliance on heavily managed devices without sacrificing the governance and visibility that IT and security teams require. For organisations looking to extend device lifecycles, reduce refresh costs or support a more diverse device estate, this can deliver both commercial and sustainability benefits.

"Identity sits at the centre of the evolution towards application-centric, zero-trust workplace access, as perimeter-based security models give way to continuous, policy-driven verification," comments Mann. "Embedding identity and access controls into the user experience, rather than layering them on afterwards, distinguishes modern secure access from earlier remote access approaches.

This can reduce friction for users while strengthening the security posture of the organisation."

In practice, this approach establishes a secure access model that is simpler to manage, with fewer endpoint dependencies, more streamlined access policies and a stronger long-term security posture. It can also increase operational agility, enabling organisations to respond more quickly to changing business requirements, workforce expectations and security challenges.

The organisations best positioned for this future are those that begin simplifying today through incremental, strategic improvements. By reducing complexity, strengthening security and optimising existing investments, they can build a workplace environment that is more resilient, adaptable and sustainable for the long term.



Citrix Secure Access with Chrome Enterprise

Citrix Zero Trust Network Access (ZTNA) and Chrome Enterprise browser offers a customer enhanced capability for accessing workloads with minimal client installation and integrated management and data loss prevention, enhancing both a customer's security posture and total cost of ownership.



A partnership to turn platform capabilities into practical outcomes

To successfully modernise to secure application access, organisations need more than just the right platform, but the ability to turn platform capabilities into practical outcomes.

Working with a partner that has an in-depth understanding of workplace technology can close the gap between the current and target state.

Together, Computacenter and Citrix provide the services expertise and the platform. While Citrix offers a mature, proven platform for secure application access and workplace delivery that meets the evolving demands of hybrid, distributed and cloud-aligned environments, Computacenter delivers the services expertise to make it work in practice. Computacenter supports organisations at every stage of their modernisation journey, from initial assessment and strategic advisory through to implementation, optimisation and ongoing operational management.

For those reassessing existing Citrix environments, exploring more flexible secure access models and looking to improve

operational efficiency without unnecessary disruption, working with Computacenter can help achieve these goals faster.

“Computacenter’s experience means we can move organisations toward application-centric, identity-led approaches at a pace that suits their business, without disrupting the environments users depend on,” comments Naomi Harrison, Partner Manager at Computacenter. “Computacenter offers the strategic guidance to shape the right approach and the technical depth to deliver it.”

Computacenter’s experience across complex estate management, security transformation and end-to-end lifecycle support means it can proactively identify where full Citrix capabilities aren’t being harnessed, and ensure organisations make the most of them to align with their broader workplace strategy.

citrix. | fusion
preferred
services
partner

Computacenter is a Citrix Preferred Services Partner, with the skills and experience to help organisations assess, optimise and evolve their secure application access environments.





A more sustainable approach to secure access

The move from traditional VDI to secure application access represents a significant opportunity for organisations managing complex workplace environments.

With an identity-led, application-centric approach, organisations can reduce complexity and management overhead, while strengthening their security posture and improving user experiences.

Achieving these goals requires more than just the right platform, however. Organisations need a partner with the operational experience to assess their existing platforms and the practical expertise to help achieve the right outcomes, without disrupting the business in the process. Working with the right partner can make workplace modernisation more manageable, more predictable and more aligned to business goals.

Computacenter and Citrix help organisations achieve this. Together they help improve security posture, simplify operations, reduce cost and ensure workspace investments continue to generate value as requirements evolve.



Get in touch

To find out more about how Computacenter can help your organisation optimise existing Citrix investments and reduce operational complexity, please contact your Computacenter Account Manager, email enquiries@computacenter.com, or call **01707 631000**.



Computacenter is a leading independent technology and services provider, trusted by large corporate and public sector organisations. We are a responsible business that believes in sustainable long-term value creation. We help our customers to source, transform and manage their technology infrastructure to deliver digital transformation, enabling people and their business. Computacenter plc is a public company quoted on the London Stock Exchange (CCC.L) and a member of the FTSE 100. Computacenter employs over 21,000 people worldwide.

www.computacenter.com

