Transient

Using Zero Trust Access to Replace VDI

Still paying the VDI tax? Use TransientX for complete security at 70% lower cost.

Summary

Enterprises have been relying on Virtual Desktop Infrastructure (VDI) for nearly 30 years to protect their data and applications. Running VDI infrastructure or using its new cloud variant, Desktop-as-a-Service (DaaS) can range between $500 to more than $1000/year per user when VDI licenses, MSFT licenses, network, server and storage infrastructure or cloud costs are included. Further, the complexity of these systems requires support by highly skilled individuals at significant annual operational costs.

Zero Trust Access from TransientX eliminates the need for VDI. TransientX provides a complete zero trust network access (ZTNA) solution for protecting the data center at a total cost that can be up to 70% lower than VDI, with a fraction of IT personnel time and skills required to support. To stop paying the Citrix, VMWare, Nutanix or Windows Virtual Desktop tax, read below to learn how TransientX can deliver immediate savings and greater enterprise security.

The Enterprise Security Challenge

Many enterprises process customer data that is regulated (for example banking information, health records) or worth significant sums in the wrong hands (identities, credit cards, digital certificates). To prevent data loss, security and application teams have relied on VDI from companies like Citrix and VMWare to control access to applications holding this valuable data. Employees in hospitals, call centers, law-firms, banks, and distribution centers are familiar with the virtualized Windows desktop where either a browser, or more often, a local application is used to perform their tasks.

The primary value of these solutions is twofold:

- **Protect application servers:** Don't let bad-actors access the data center or cloud where the apps and data reside
- **Protect enterprise data:** Don't allow end-users to mis-use enterprise-held data

Traditionally a combination of VPN and VDI has been used to accomplish these goals with each delivering these key features:

VPN and Security Infrastructure: Protect app servers	VDI: Protect data
▪ Single Sign On (SSO) ▪ Conditional Access Controls ▪ Network Segmentation	▪ SSO ▪ Conditional Access ▪ Copy-paste/download ▪ Keyboard logging prevention ▪ Browser isolation ▪ Screen recording

VDI, whether it is run in a private data center or in the cloud (e.g. Windows Virtual Desktops or Citrix Workspace), is complex to manage. It is also costly, with software and infrastructure costs of $50-70 per month before discounts, plus the fully loaded employee costs to manage these services. Even with cloud-hosted services, the complexity of application publishing, compatibility testing and managing connectivity to the application remain as work items.

VDI is predominantly used for app-access control in verticals where the loss of data has significant legal or financial consequences. These include healthcare (the top vertical for VDI), banking, financials and insurance, call centers, manufacturing, legal, logistics and other customer-facing groups. An orthogonal use case is contract software development by US-based companies, with contract developers based typically in India. In all of these cases, either a browser or a set of thick-client apps are run in a VDI context. This represents 70-80% of the 300-500 million seat VDI market today.

Zero Trust Access solutions have emerged to protect data centers and cloud-based private applications. These solutions protect the enterprise data center or cloud application instances by:

- Limiting users to access only applications for which they are assigned
- Limiting client devices to only reach configured applications, while hiding all other servers.
- Continuously assessing the user and device to ensure that their activities adhere to risk policies of the enterprise, including reviewing location, software and OS versions, and end-point protection levels
- Using VPN-less access where an agent/connector is deployed in the data center and connects to a cloud-based gateway, eliminating the need for opening firewall ports

Customers using VDI still need to deploy additional security services. While this may be counter-intuitive at first glance, use of applications in VDI does not prevent breaches in data centers. A rogue application deployed in a VDI instance can still wreak havoc in a data center if it has unfettered access!

TransientAccess from TransientX

TransientX has modernized enterprise security for protecting data and application servers. TransientX unifies the solution into a single, cohesive cloud service that delivers true zero-trust security for the enterprise. This eliminates the requirement of VDI such as Citrix Workspace and separate ZTNA solutions while still facing the limitations on requiring cloud-hosted desktops for thick-client applications. With TransientX:

- VDI software or services are no longer required
- Enterprises enjoy the security benefits of a complete ZTNA solution
- Risk of breaches, data loss or ransomware are steeply reduced with a no-gateway technology and an out-bound meet me solution that minimizes attack surfaces.

TransientX is a complete VDI replacement for app-access control, representing more than 70% of use cases. TransientX provides all the required functionality to replace VDI in this context, while also protecting the application servers where VDI requires additional solutions.

TransientX vs. VDI

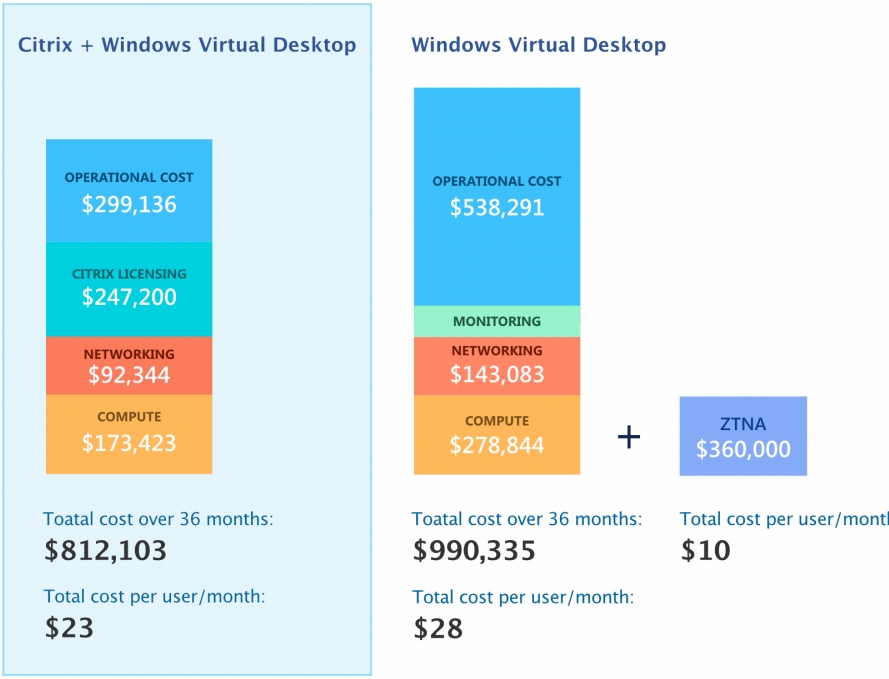
Key capability	Description	TransientX	VDI
Client-side data security	Protection of data, code and imagery via cut/paste, print controls, USB controls for file upload/download, no screen- scraping and water marketing.	✓	✓
Client-side file security	All downloaded, or locally generated data are stored separately and encrypted. They can we wiped out easily and certainly protected from any user and malware.	✓	✓
Granular and conditional access	TransientX provides a powerful continuous authorization capability that is a superset of conditional access, including a variety of dynamic checks to respond to security condition change such as device, location, app version, debugging etc.	✓	Requires separate analytics
Data Center/ App Protection	VDI does not control where the apps access in a network. Therefore, additional ZTNA software must still be installed in a VDI instance to control where those client apps can access. This is already an integral and distinct part of the TransientX solution.	✓	Requires separate ZTNA

TransientAccess from TransientX

Implementing VDI services in the cloud brings significant cost of operations. As shown below, with a 3-year commitment, Cloud-based VDI solutions from Citrix cost at least $23/ month or nearly $300 per year with a 3-year commitment. In addition, a separate full ZTNA solution must be purchased to provide data center security. TransientX provides greater functionality, lower risk of security by virtue of not touching customer data in cloud services, while costing 66% to 75% less for the same solution when all costs are included.

Citrix VDI and Windows Virtual Desktop Costs *

1000 users = $33-$38/month
with 3-year commitment



TransientX Costs **

1000 users = $10/month
with 3-year commitment

Total cost per user/month:
$10

* Source: https://www.citrix.com/products/citrix-virtual-apps-and-desktops/resources/windows-virtual-desktop-calculator.html#/result

** If your organization is struggling with the burden of supporting VDI at scale while protecting against data breaches and staying compliant, contact us to see how moving to ZTNA can make enterprise access secure and easy.

TransientX delivers on the promise of truly secure, easy to use and deploy zero-trust access for an organization's workforce and business partners. We transform fixed and device-centric networks to disposable networks of apps.