Deloitte.

White paper: Zero Trust Access for Virtual Desktop Infrastructure Evolution

Contents

Reduce Virtual Desktop costs, enhance user experience, improve data protection and infrastructure security with Zero Trust Access

Zero Trust by Deloitte offers a broad range of services to help organizations align to leading cyber practices and secure the ubiquitous nature of their modern enterprises. Zero Trust Access (ZTA) is a managed service that can accelerate this journey by securely connecting what matters most: users to applications.

Enterprises have historically leveraged Virtual Desktop Infrastructure (VDI) to protect valuable data and infrastructure for both local and remote access use cases. These solutions typically cost $500-1,000/year/user when combining VDI and operating system licenses with infrastructure or cloud hosting costs (e.g., server, compute, storage). Enterprises moving to consumption-based Desktop-as-a-Service (DaaS) solutions face similar costs, with $40-80/month/user charges depending on central processing unit (CPU) and storage requirements. The complexity of these systems also requires highly skilled and costly information technology (IT) personnel for ongoing application management. Further, additional security controls typically need to be integrated into VDI and DaaS environments to protect enterprise data and applications from lateral movement and data exfiltration threats.

Deloitte’s Zero Trust Access (ZTA) can remove the need for Virtual Desktops and provides a turnkey solution designed to enhance user experience, protect enterprise data and applications, decrease operational burden, and drive measurable cost efficiencies.

The enterprise data protection challenge

IT security teams process customer data that is regulated (banking information, health records) or valuable in the wrong hands (identities, credit cards, digital certificates). To help prevent data loss, security teams have used VDI to control access to applications processing valuable data served from enterprise resource planning (ERP) platforms, or from in-house application servers. Employees in hospitals, call centers, law firms, banks, and distribution centers are familiar with VDI where either a browser or a local application is used to perform their tasks. VDI solutions have also been leveraged as a remote access alternative to traditional virtual private network (VPN) technology, especially for organizations that need to secure remote connectivity from unmanaged devices (e.g., third parties, personal devices).

Connecting users directly to the applications they are entitled to vs. the networks on which those applications communicate helps enforce the core tenet of Zero Trust – least privilege.

Virtual Desktops, whether run in a data center, in the cloud, or consumed as a service (e.g., DaaS) can be costly, ranging from $40-80/month/user2 plus personnel costs to manage these services. The complexity of application packaging + publishing, compatibility testing and connectivity to enterprise applications remains a burden to IT teams.

The majority of Virtual Desktops are used for app-access control and data protection in industries such as Health Care, Banking, Financial Services, Insurance, call-centers, manufacturing, legal, logistics etc., where the loss of data can have significant legal or financial consequences. With the proliferation of Software-as-a-Service (SaaS), VDI is used to prevent data exfiltration. Remote software development is another use case where organizations need to establish safeguards against source-code theft and secure the ubiquitous nature of the extended ecosystem.

With limitations of VPN exposing enterprises to breaches, Zero Trust Network Access (ZTNA) solutions have emerged to help protect data centers and cloud-based private applications. ZTNA solutions can be thought of as a replacement of VPNs to help reduce the risk of enterprise infrastructure breaches. These help protect the enterprise data center or cloud application instances by:

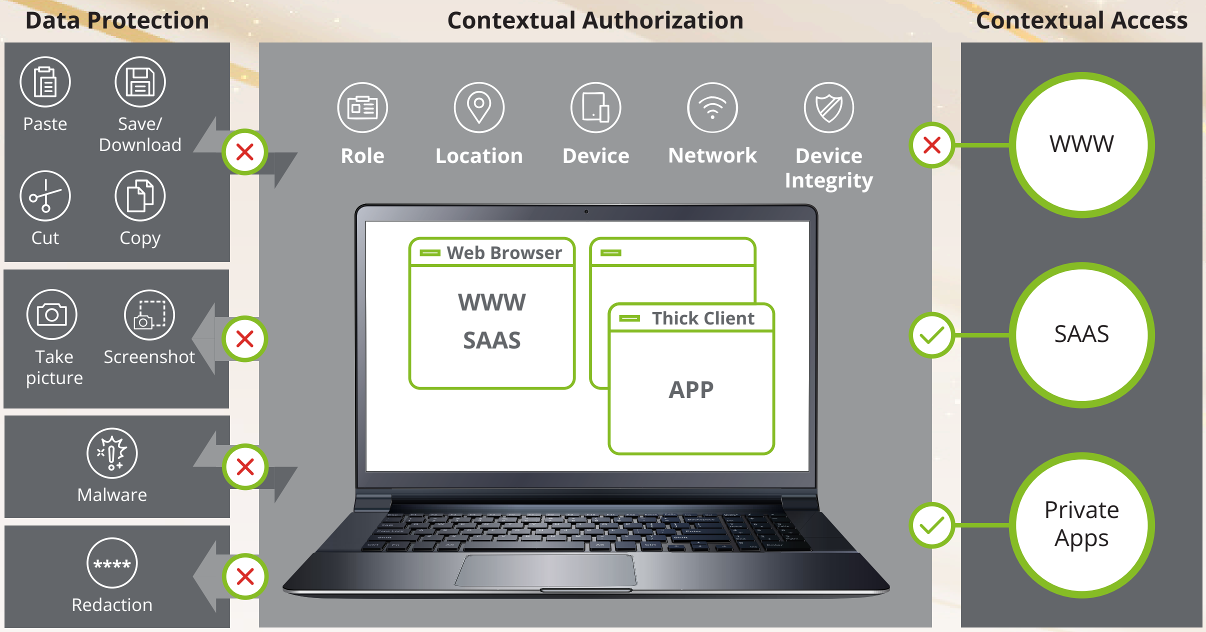
- Limiting users to access only those applications for which they are assigned through identity-based controls
- Preventing lateral movement inside the data center or private cloud by limiting the reach of client devices to configured and permissible applications only.

The combination of ZTNA with web protection technologies, such as Secure Web Gateways (SWG) and Content Access Security Brokers (CASB), is the trending means of protecting the enterprise from external threats today. However, this group of technologies requires that the enterprise control/ manage these devices. Further, SWG and CASB services do not provide data protection once the data is delivered to a user's endpoint device. Due to these limitations, VDI is often positioned as a remote access solution for employees or third parties connecting from unmanaged devices.

Ultimately, traditional workforce and remote access solutions such as VPN, DaaS, and VDI can lack the elastic scalability and inherent resilience needed to drive business agility. They can also be costly, complex, operationally burdensome, and ineffective at enforcing modern Zero Trust principles.

Enterprises using Virtual Desktops still should deploy a form of ZTNA to protect their infrastructure. Conversely, ZTNA solutions do not obviate the need for VDI as ZTNA does not protect data once it is delivered to the user's endpoint device.

Zero Trust Access



Grounded upon Zero Trust principles, Deloitte's ZTA helps accelerate adoption by enforcing "least-privilege" policies for applications and users across Software-as-a-Service (SaaS) and private applications in public or private clouds. ZTA can replace legacy VDI, DaaS, and VPN technologies with a modern cloud service that can significantly reduce total cost of ownership (TCO) and enforce broad data protection via innovative micro-container technology.

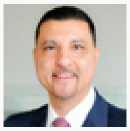
ZTA is trending as a Virtual Desktop replacement because of its ability to provide rapid risk reduction and cost efficiencies. Instead of deploying costly and separate Virtual Desktops and ZTNA solutions, ZTA delivers a single cloud-delivered solution that provides broad access security for the enterprise for both unmanaged and managed devices. Dynamic and continuous authorization, application segmentation and data leakage protection are natively built into the platform and do not require the integration of additional controls.

Additionally, ephemeral connectivity brokers secure peer-to-peer (P2P) communication between end users and target applications, alleviating the need to back-haul traffic through corporate data centers or route through third-party points of presence (POPs). The result is a rapid and frictionless user experience that does not rely on real-time streaming of the virtual environment and limits the risk of man-in-the-middle and session hijacking threats.

Feature Comparison: ZTA vs. ZTNA vs. Virtual Desktop

Core Capability	Notes	ZTA	Virtual Desktop	ZTNA
Client-side data security	Protection of data, code, and imagery via cut/paste, print controls, file upload/download, no screen- scraping and watermarking	✓	✓	×
Client-side application security	Segmentation and protection of applications that are hosted on a user's local device, along with the data processed within	✓	×	×
Client-side file security	Downloaded, or locally generated data are stored separately and encrypted. Can be wiped easily and protected from user and malware	✓	×	×
Device Support	Support for un-managed and corporate managed devices	✓	✓	×
SaaS Data Protection	Protection of data served from SaaS by preventing copy, cut, paste, print, file upload, screen scraping and watermarking	✓	✓	×
Granular and conditional access	Virtual Desktop provides granular access controls to distinguish which apps a user can access. ZTA provides a superset of such controls, including dynamic checks to detect security condition changes such as device, location, app version, and debugging	✓	Requires integration of additional controls	✓
Data Center/ App Protection	Virtual Desktop does not control where apps access in a network. Separate ZTNA software should be installed in a Virtual Desktop instance to control where client apps can access. This is an integral part of Deloitte's ZTA Service	✓	Requires integration of additional controls	✓

Contact Us To Learn More



Andrew Rafla
Principal
Deloitte & Touche LLP
Tel/Direct: +1 201 499 0580
arafla@deloitte.com

Egemen Tas
Managing Director
Deloitte & Touche LLP
Tel/Direct: +1 201 499 0547
egtas@deloitte.com

Chalan Aras
Managing Director
Deloitte & Touche LLP
Tel/Direct: +1 408 704 4897
chaaras@deloitte.com

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

[1] https://www.appsanywhere.com/resource-centre/vdi/how-much-does-it-cost-to-implement-vdi.

[2] https://www.computerworld.com/article/3628190/microsoft-reveals-windows-365-virtual-desktop-prices-20-to-162-a-month.html.

[3] https://www.networkworld.com/article/3652568/sse-is-sase-minus-the-sd-wan.html

Deloitte.

About this publication

This publication contains general information only and Deloitte and Palo Alto Networks are not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte and Palo Alto Networks shall not be responsible for any loss sustained by any person who relies on this publication.

Product names mentioned in this publication are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte & Touche LLP is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this publication.

About Deloitte

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.