GO-Global

Windows applications, anywhere.

GO-GLOBAL VERSUS MICROSOFT RDS

Unlike products that wrap features around Microsoft® Remote Desktop Services (RDS), GO-Global provides full replacements for Microsoft's multi-session functionality and its Remote Desktop clients, display driver, protocol, internet gateway, and management tools, which can save at least 40% over other multi-user remote access solutions.

The chart below provides examples of the GO-Global technology and Microsoft functionality it replaces.

MICROSOFT	RDS ADD-ON VENDORS	GO-GLOBAL
Multi-Session functionality in Windows® kernel (aka WinStations).	Use Microsoft's multi-session kernel.	GO-Global's System Extensions Driver provides a session-private sandbox for drivers and processes.
Microsoft's Remote Desktop Client for Web provides remote access to Windows desktops and applications.	Web clients mostly use Microsoft's Remote Desktop Protocol (RDP).	GO-Global Web App provides zero-install, browser-based access to remote Windows applications using 100% GraphOn technology.
Remote Desktop (RD) clients for endpoint devices provide remote access to Windows desktops and applications. Some are open source or 3rd party.	Extend or wrap Microsoft or 3rd party clients for Microsoft's Remote Desktop Protocol.	GO-Global App for Windows, Mac, Linux, iOS, and Android enables remote applications to run as if they were running locally on the client device, using 100% GraphOn technology.
Remote Desktop Protocol display driver converts Windows graphics commands to Microsoft's Remote Desktop Protocol.	Use Microsoft's display driver and protocol.	GO-Global Virtual Display Driver converts Windows graphics commands to GraphOn's RapidX Protocol (RXP).
RD Connection Broker provides load balancing of connections across Microsoft hosts.	Replace the RD Connection Broker with their own load balancing functionality.	GO-Global has built-in load balancing between hosts or can use a 3rd party network load balancer for connections.
RD Gateway provides secure internet connectivity for RD Clients by tunneling RDP through SSL/TLS.	Replace RD Gateway with their own security wrapper for the RDP protocol and RD Clients.	GO-Global uses OpenSSL to secure communication between clients and hosts.

Continued on next page

Secure Access to Corporate Systems

Two-Factor Authentication

The pandemic-driven surge in employees using RDP to connect from home to their work computers was accompanied by a surge in brute force attacks on RDP to gain entry to corporate systems. While some employees are returning to the office, many organizations are adopting flexible work policies that allow end user to work more from home, extending the risk for continued attacks. Unlike RDS/RDP, GO-Global protects against brute force attacks with Two-Factor Authentication (2FA) for end user logons.

Single Sign-On

Many organizations are adopting Single Sign On (SSO) to make it easier for employees to access the applications they need to do their job, while ensuring compliance with corporate security policies. Unfortunately, SSO has historically only been able to authenticate users to web applications, not Windows applications. Windows does not support logons without a password and as such does not support strong authentication through SSO to the logon module.

GO-Global enables IT and CISO organizations to allow end users to connect to Windows applications through SSO by providing support for OpenID Connect (a simple identity layer on top of the OAuth 2.0 protocol) to enable single sign on to Windows applications published by GO-Global, allowing users to sign in once to their identity provider using the authentication policies and credentials defined by that provider, and then access those Windows applications with just one click.

GRAPHON

GRAPHON CORPORATION

189 North Main Street, Suite 102 • Concord, NH 03301 USA • **sales@graphon.com**