SOLUTION BRIEF

Secure Clinical Access to Azure Virtual Desktops and Windows 365 Cloud PCs

No Click Access™ to Microsoft Azure Virtual Desktops

Desktop and application virtualization have been critical technologies in healthcare for almost two decades. The natural progression for many organizations is to maximize the benefits of this approach by moving to on-prem or cloud-hosted VDI or DaaS, such as Microsoft Azure Virtual Desktop (AVD), Azure Local, Windows 365 Cloud PC, and Windows 365 Frontline. A critical challenge though has been how to ensure healthcare providers retain the fast badge tap access that can save minutes and hours every day. In an industry-first collaboration, IGEL and Imprivata have integrated IGEL OS and Imprivata Enterprise Access Management to enable fast, no-click access to Microsoft AVD and Windows 365 Cloud PCs.

Imprivata Enterprise Access Management (EAM) improves efficiency and productivity while ensuring compliance with security and regulatory requirements. Care providers can access IGEL OS endpoints and Microsoft virtual desktops using proximity card authentication with a single badge tap. Organizations looking to utilize leading electronic health record (EHR) solutions, including Epic in a Microsoft-hosted environment, now can support the secure clinical workflows required to save clinicians time and protect patient information. The integration also facilitates a smooth transition from on-premises VDI to AVD, enabling the essential clinical workflows including desktop roaming for ambulatory and in-patient facilities, tap-in and tap-over functionality, kiosk mode workflows, and a single endpoint strategy for the entire organization.

Reducing clinical workstation costs, improving security

IGEL's endpoint operating system allows lightweight and efficient laptops, thin clients, and zero clients to be used by care providers, IT, and back-office staff to access patient information quickly. Read-only and with a small footprint, IGEL OS dramatically reduces endpoint management time and effort by eliminating the need for multiple security, management, and backup and recovery agents. The IGEL Universal Management Suite (UMS) delivers easy yet powerful SaaS-based management of endpoints. IGEL has been a leading provider of endpoint solutions to healthcare organizations for over a decade, with an extensive healthcare partner ecosystem and integrations with key peripheral devices, including dictation and signature capture devices.

Key Features

- Integrates IGEL, Imprivata Enterprise Access Management (EAM), AVD, Windows 365 Cloud PC, and Windows 365 Frontline
- Support for local peripherals with IGEL Advanced Device Redirection
- Supports roaming Microsoft desktops or apps, virtual kiosk, and Imprivata Fast User Switching workflows
- Secure read-only OS
- SaaS-based management of endpoints
- Supports native applications for Teams, Zoom, and others
- Native apps for Microsoft Intune and Microsoft Edge available on the IGEL App Portal
- The leading solution for tap-and-go clinical access for Microsoft AVD and Windows 365 Cloud PC

Key Benefits

- The only secure endpoint solution for tap-and-go clinical access for Microsoft AVD and Windows 365 Cloud PC
- Streamlines and quickens clinical access with minimal login times for clinicians
- Modernizes and secures access to critical data and resources
- Dramatically reduces endpoint management time and effort by eliminating the need for multiple security, management, and backup and recovery agents
- Supports compliance requirements for HIPAA, DSPT, GDPR

Supporting Telehealth and Collaboration

IGEL supports native applications of popular video conferencing and collaboration tools like Teams and Zoom. With IGEL, users can use native applications or offload the workloads from the virtual environment for a seamless experience. This ensures healthcare providers can conduct patient consultations smoothly, resulting in a high-quality user experience and patient satisfaction score.

Improving Compliance and Sustainability

Imprivata and IGEL support organizations in working towards compliance with Health Insurance Portability and Accountability Act (HIPAA) and the UK's National Health Service Digital Security Protection Toolkit (DSPT) requirements. By minimizing the endpoint's attack surface, IGEL reduces the impact of endpoint-related common vulnerabilities and exposures (CVEs) and the need for NHS Cyber Alert triage and remediation.

Modernizing and Securing Access to Critical Data and Resources for a Leading Healthcare Organization

Secure back offices are crucial for organizations with shared workstations to protect employees' data. Efficient workflow systems for distributed hybrid and remote workers can boost productivity and collaboration. For example, a healthcare provider with 4,000 clinical workers encountered several obstacles, including slow booting and login processes, high latency, poor virtual machine (VM) performance, slow login times, and costly VDI resource management when accessing necessary applications and resources throughout the day.

The healthcare organization opted to use IGEL and Imprivata Enterprise Access Management (EAM) with tap-and-go badge verification to address these obstacles, streamline clinical access, and minimize login durations. Additionally, they chose to migrate from conventional on-site VDI to Azure Virtual Desktop (AVD) to simplify virtual desktop administration and assistance and stabilize licensing expenses.

Now, clinicians can tap their badge to an IGEL OS endpoint and automatically launch and log in to their AVD environment in seconds without manually entering a username or password. This solution has enhanced productivity — which improves overall patient outcomes — by minimizing login times and enabling Fast-User-Switching for multiple workers to quickly tap in and tap out from the same endpoint.

Test Drive the IGEL Agent for Imprivata with Microsoft Azure Virtual Desktop and Microsoft 365 Cloud PC

Learn more on IGEL Secure Endpoint OS in Healthcare