Solution Brief

Healthcare and Life Sciences
Telehealth
Connected Client

Intel, IGEL, and Lenovo Support Manageable Connected Clients for Mobile Telehealth

To handle a sudden onrush of telehealth and at-home visits during the COVID-19 pandemic, one healthcare provider improved security, manageability, and cost-effectiveness with a mobile connected client solution featuring Intel® Core™ processor-based Lenovo ThinkPad laptops running a centrally managed operating system from IGEL.

A large mental healthcare provider in the northeastern US delivers community-based behavioral health services to vulnerable populations. The patients, whose lives are often complicated by intellectual disabilities, addiction, abuse, or other forms of trauma, are not always able to visit a clinic, so the practitioners spend much of their time in the field.

The clinic provides each practitioner with a remotely managed laptop that is configured for maximum availability, uptime, and data security, often under difficult conditions. A seven-person team manages health information technology (IT) operations for more than 1,200 staff members at 70 sites, including 600 employees with connected client laptops.

Challenge: Rapid transition to telehealth service delivery

In early 2020, the healthcare provider's IT team faced a new challenge. Because of the COVID-19 pandemic, on-site patient visits were discontinued abruptly and replaced with telehealth services. Prior to the pandemic, and before **emergency federal legislation** enacted in March 2020, these videoconference visits were not allowed to be used for behavioral health services in the organization's home state. With the rule change, many health services providers in the state struggled to ramp up their capabilities while complying with new regulations and ensuring security and privacy protections for patient interactions and sensitive data.

Meanwhile, the pandemic also prevented employees from bringing devices to the home office for regular maintenance or updates. To help employees make the transition to telehealth, the IT team needed a fully remote device management solution that would deliver a satisfactory user experience while maintaining data security and patient privacy.

Solution: IGEL OS on centrally managed connected clients

The organization had already begun converting its on-premises devices to a connected-client model in 2018. Not long before the pandemic began, the IT team made the transition to IGEL Technology's endpoint operating system for support of virtual desktops used by most of the on-premises devices in its 70 locations. By the time the pandemic began, the IT team was well positioned to complete the transition.

The IGEL Cloud Gateway was enabled on all the remaining mobile endpoints so that the IT team would have remote access to all devices in the fleet. The IGEL Cloud Gateway substitutes for a VPN for any IGEL OS–powered device, enabling the user to access the corporate virtual desktop and applications from any location with internet access. The Cloud Gateway also gives IT the access needed to shadow a remote user's device whenever the user needs support at home, in the field, or at a coffee shop.

Before the pandemic, mobile users received laptops with a large software stack that included all necessary applications and a full operating system (OS) installed on the hard drive. There were downsides to that approach, however. Every time a healthcare practitioner needed to access the laptop, it required a double log-in: first on the device's Windows desktop and again on the organization's virtual desktop. The laptops took a long time to boot up, and batteries did not always last for an entire workday in the field.

For the IT team, the full installation made remote endpoints difficult to manage. Some updates and maintenance required users to connect to the local network in the office. And when the OS had a major update, it did not always run successfully on the older laptops, limiting the useful life of those devices. Further, if a laptop were stolen or simply left unattended in a nonsecure environment—on a site visit or in an employee's home, for example—there was a risk of exposing applications and sensitive data to unauthorized users and malware.

Post-transition, Intel® Core™ processor-based Lenovo devices ran the IGEL OS to provide access to virtual desktops and connect to server-based applications via the IGEL Cloud Gateway. With the centralized management setup, the IT team provides all employees—many of whom continue to work remotely—with more secure access to the same applications and data that are available in their offices and clinics. In addition, the IT team installed the same IGEL OS on older laptops, effectively turning a heterogeneous fleet into a homogeneous set of easy-to-manage remote endpoint devices.

The pandemic coincided with the introduction of a first responder's cellular network service in the region, and the organization was able to provide employees in the field with much-needed mobile connectivity. The IGEL OS and IGEL Cloud Gateway installed on the endpoint clients provided full support for cellular, Wi-Fi, and LAN connectivity to applications and data through the IGEL Universal Management System (UMS) on the organization's servers. As a result, each employee's virtual desktop was readily available, and full local software installations were no longer needed. From an IT perspective, IGEL kept users happy and productive while enabling manageability through a more secure, encrypted network connection.

How it works: IGEL OS and IGEL Gateway

When the organization's facilities were closed during the pandemic, the IT team enabled the IGEL Cloud Gateway on all employee devices. All subsequent updates, patches, configuration changes, and maintenance could be administered via a connection to the IGEL UMS.

IGEL OS Benefits

More secure access to telehealth. Applications and patient data are available over cellular networks for employees working from home or in the field.

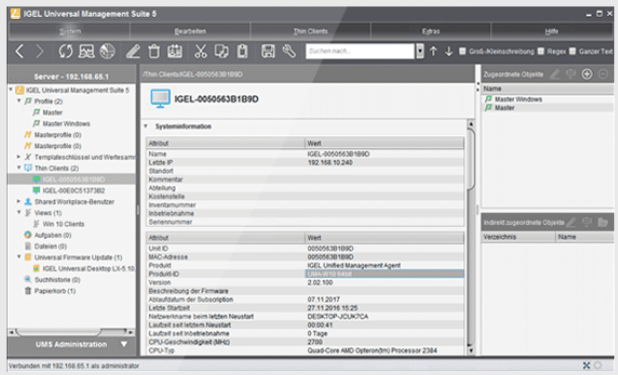
IGEL OS is read only. Users can't store sensitive data or applications on the vulnerable endpoints. If a laptop is stolen or hacked, for example, the data is less likely to be compromised. Plus, the IT team can wipe the device's hard drive remotely.

Extend usable life of the device. Older devices were reimaged with IGEL OS. The same software stack ran efficiently on older laptops and on a variety of on-premises computers, as well as the new 2-in-1s.

Manage hardware remotely. A heterogeneous fleet of devices can be managed as one homogeneous set with IGEL OS. The IT team can now manage devices remotely to adjust settings and provide a consistent user experience on any device type or model. This was a key feature during the pandemic, when employees could not enter their offices to bring devices to the IT staff for maintenance.

Manage Windows and application updates. The IT team can update, patch, and upgrade Windows and other software in the data center within days of release. Users can log in to their virtual desktops remotely without going through a separate log-in on the local device.

Solution Components



IGEL OS ›
IGEL Universal Management Suite ›

Lenovo Gen 2 ThinkPad L13 ›

Intel® Core™ i5-1135G7 mobile processor ›
Intel® Wi-Fi 6 AX201 networking ›
Intel® Iris® Xᵉ Graphics ›

The IGEL OS enabled a more secure, high-performance access to a virtual desktop installed on-premises in the organization's data center. The system image is delivered via a private cloud, along with the Microsoft Office suite and healthcare-specific applications.

For remote users, the IGEL Cloud Gateway provided full access to all applications and data. Users reported that performance compared favorably to the previous setup, when a full version of Windows and key applications were installed on the device itself. While working at home and in the field, users also felt confident that their data, applications, and devices were protected against unauthorized use.

Connected client setup improves battery life

The IGEL OS on the connected client endpoint offered several advantages. The previous combination of Windows and a full application suite took several minutes to boot up, and users had to log in twice—first on the local Windows desktop and again on the server-based application suite. The locally installed operating system was one factor that caused laptop batteries to drain quickly, sometimes interrupting practitioners' work in the field. Over the years, the OS and applications became more complex, and new peripherals and drivers were added. These older laptops became inadequate, requiring replacement at least every three years.

The older laptops also allowed users to store sensitive data locally, even though the organization's policy forbade it. That local storage capability led to security risks, either when employees neglected to install software updates and patches in a timely way or when an unauthorized user gained access to the laptop.

With IGEL, the IT team manages the IGEL OS–powered endpoints remotely through the IGEL Universal Management Suite and its IGEL Cloud Gateway. IT teams can access laptops and other devices to perform updates, install patches, shadow a user, and monitor performance without having the devices right in front of them.

Better security, remote connectivity on Lenovo 2-in-1 ThinkPad

In 2020, the organization installed the IGEL OS on 275 new Lenovo ThinkPad L13 Yoga 2-in-1s and on an existing fleet of laptops. Even though the older laptops were provided by a different manufacturer, IGEL ran smoothly on all of the Intel® architecture-based devices. While IGEL works on any x86-64-compatible endpoint, the healthcare provider specified Intel Core processor-based models for an extra measure of compatibility and reliability.

The Lenovo ThinkPad L13 Yoga is a lightweight device that functions as both a laptop and a tablet. It runs on the Intel® Core™ i5 processor and Intel® system-on-chip (SoC) platform with integrated Intel® Iris® Xᵉ graphics, a key feature for many health and life sciences institutions and users. The device is also equipped with Intel® Wi-Fi 6 AX201 networking, which was of special concern to the organization because of its extensive field practice and telehealth services as well as COVID-driven telecommuting. For healthcare users, Lenovo offers antimicrobial, water-resistant coatings and sturdy packaging so that the device is not easily damaged by the spills, cleaning solutions, or falls from a desk or cart that are common hazards in clinical settings.

Both IGEL and Lenovo partner with Intel to develop innovative technologies and **solutions for healthcare and life sciences**. Both companies have dedicated health and life sciences teams that develop and recommend products to accommodate the unique needs of healthcare providers. For example, both test an array of headsets, microphones, speakers, and cameras, as well as software for dictation, lossless image processing, and privacy-protection display modes to provide clinicians with a consistent, reliable interface for telehealth and in-person care.

About IGEL

IGEL is a leading international IT software company offering an operating system (OS) and other innovative solutions for accessing VDI, DaaS, and cloud workspaces. The company is known for its endpoint OS solutions and its focus on consistent and continuous customer satisfaction. The IGEL OS helps customers to extend the useful life of hardware devices, reduce operating expenses, and enhance security for fleets of Intel® architecture-compatible devices.

igel.com

About Lenovo

For more than 30 years, Lenovo has helped organizations to revitalize their business through innovative technology solutions. Lenovo offers a full portfolio of PCs and tablets, monitors, accessories, smartphones, collaboration solutions, software, services, and more. Lenovo partners with Intel to deliver architecture that drives performance and helps end customers to excel.

lenovo.com