Preventative Security in Healthcare: The IGEL Approach to Endpoint Security

Fortifying Endpoint Security for Compliance and Patient Data Protection

Contents

Introduction

Clinicians and physicians need instant access to key applications and patient electronic health records (EHRs) with high performance and availability. Tap-and-go access to key apps, rapid badge-in and badge-out practices, high resolution imaging, video 4kHD video, and high-quality unified communications like Teams, Zoom, and Webex for both internal staff and external telehealth are all essential tools to support clinicians in providing the best possible care. The steady growth of cyber-attacks and looming ransomware threatens healthcare organizations' end-users and IT infrastructure, affecting patient care. To achieve the balance of security, compliance, and quality patient care, IT and cybersecurity managers strive to safeguard sensitive protected healthcare information (PHI) without slowing down access to data and apps by the doctors, nurses, and administrative staff.

A Secure Endpoint Strategy for Now & Next

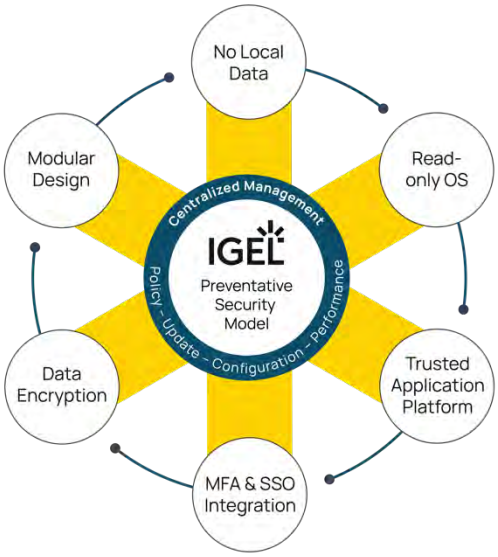
Many healthcare organizations are already experiencing the security benefits of moving application workloads away from the endpoint to secure browsers, VDI, DaaS and SaaS environments. IGEL secure endpoint OS **reduces the endpoint attack surface by 95%** by removing the need for endpoint security and management agents including EDR, AV, DLP, backup and recovery etc., organizations dramatically reduce the time and labor IT spends on managing endpoint security while saving significant capital and operational expenses, reducing endpoint **total cost of ownership by up to 75%**

With the upcoming Windows 10 end of support and migration to Windows 11, IT admins are evaluating migrating their desktops to the cloud with Microsoft Azure Virtual Desktop and Windows 365 and Cloud PC. Alternatives include Windows desktops and applications running in the cloud and on-prem with Azure Local, healthcare organizations can improve their endpoint strategy by deploying secure IGEL OS on existing hardware, designed for both on-prem and the new cloud-first architectures. Read the Enterprise Strategy Group Report.

In this paper we discuss the components of the IGEL Preventative Security Model™ and patient data protection standards like HIPAA, GDPR, and NHS DSPT. IGEL integrates with leading authentication and SASE solutions, minimizes the attack surface through a modular and read-only OS, prevents local data storage to mitigate data breaches. This integrated approach aligns with zero trust principles for healthcare and IT security.

IGEL Preventative Security Model in Healthcare

IGEL OS is designed around the Preventative Security Model™ which removes the common attack vectors exploited by bad actors for ransomware and other cyber-attacks.



IGEL Preventative Security Model™

Core tenets of the IGEL Preventative Security Model™

No Local Data Storage

- No customer, patient or financial data is stored at the endpoint eliminating data breaches from lost or stolen endpoints.

Read-only OS

- Users cannot unwittingly, or maliciously, install malware to the endpoint. Organizations reduce the risk of ransomware and other cyber-attacks.

Trusted Application Platform

- A secure boot chain of trust ensures that IGEL OS has not been tampered with.

Multifactor Authentication and single sign-on solutions

- IGEL integrates with leading authentication and single sign-on solutions to ensure fast, trusted, and secure access to desktops and applications.

Disk Encryption

- The disk partition containing settings, passwords and browser profiles is encrypted with AES-256 encryption in XTS-plain64 mode with 512 bits of key material. The key can be secured with TPM 2.0.

Modular Design

- The IGEL App Portal enables IT to install partner applications as required. This keeps the endpoint as "lean" as possible to minimize the attack surface of the device.

IGEL OS Trusted Application Platform

- Secure boot-controlled chain of trust sequence initiates upon switching on the device to ensure the IGEL OS is intact. The IGEL chain of trust runs with IGEL OS on any compatible x86 64-bit device supporting UEFI and secure boot.
- Signature checks on both update and boot processes for both system and user partitions detect tampering and prevent loading of modified code. If the signatures do not validate, the system will not boot. If any other partition is impacted, the system will boot with impacted modules deactivated. Flash media cannot be mounted on any other device.
- IGEL uses its own partitioning system with compressed partitions that obfuscate data. Checksums of IGEL partitions avoid loading of modified code.
- IGEL OS bootloader signed by Microsoft (on behalf of UEFI Forum) on IGEL boots on systems with UEFI Secure Boot enabled. Only boot loaders signed with keys appointed by IGEL or Microsoft keys approved by IGEL can load the operating system. IGEL generates and manages the cryptographic platform exchange keys, included in the corresponding UEFI versions.
- If tampering is detected, the system will not boot.
- Configuration files written to a dedicated encrypted partition ensure the security of configuration information.
- System updates always finish completely while the device stays bootable. Critical updates are always processed in two phases to ensure success.
- If users connect to a VDI or cloud environment, access software such as Citrix Workspace App or Omnissa Horizon checks the certificate of the server to which they are connecting.

IGEL Central Management Console

While the Preventative Security Model serves as the foundation for the powerful security capabilities of IGEL OS, **the IGEL Universal Management Suite (UMS)** is centralized management console for tens of thousands of IGEL's endpoints both on, and off, the corporate network. IGEL Universal Management Suite can manage all aspects of IGEL OS including:

- Policy – Set pre-defined policies by device or group.
- Update – Deploy OS and application updates to IGEL's endpoints.
- Configuration – Apply configurations including language, firmware, interface, and USB settings.
- Performance – Collect endpoint performance and logging information. Logs can be exported to security information and event management (SIEM) platforms for compliance with existing policies.

IGEL Universal Management Suite Security includes:

Encrypted Transport Layer Security (TLS) tunnels

- TLS tunnels ensure connections and file transfers from the UMS management console to the endpoint device are secure.

Centralized and cryptographic updates

- Updates from the UMS are validated by IGEL OS before installing on the target endpoints. IT admins can easily and quickly roll out security updates from one console to tens of thousands of endpoints in a network-friendly manner.

Secure shadowing

- IGEL enables the IT admin to securely shadow a remote endpoint device for troubleshooting purposes. For example, a helpdesk engineer can take over the endpoint device's keyboard and mouse. The UMS console, or alternatively, an external VNC viewer, establishes a secure connection to the UMS server, which establishes a TLS tunnel to the device, verified by a one-time-password issued by the UMS and sent to IGEL OS on the target device to grant permission. In addition, every secure shadowing session is logged by the UMS.

Streamlined security patches

- Due to the modular design of IGEL OS, updates and patches are small when compared to traditional endpoint updates. A high availability extension ensures simultaneous update of endpoints in large environments from the UMS console.

Policy based access to peripherals attached to IGEL OS end point

- An IT administrator can manage USB ports and device types like USB HID or USB storage devices on an IGEL OS powered endpoint via the management console.

High Availability

- The high availability extension enhances the deployment of new settings across tens of thousands of devices simultaneously. This is eased by a distributed Universal Management Suite (UMS) architecture, which optimizes the distribution process to guarantee that every device can update its settings at any moment, maintaining network capacity efficiency.
  Additional information is available in the Knowledge Base.

Auto log-off

- By combining a session type with an automatic log-off command, the device can log the user out of the last session. Username and password are needed to log in again.

Role Based Access

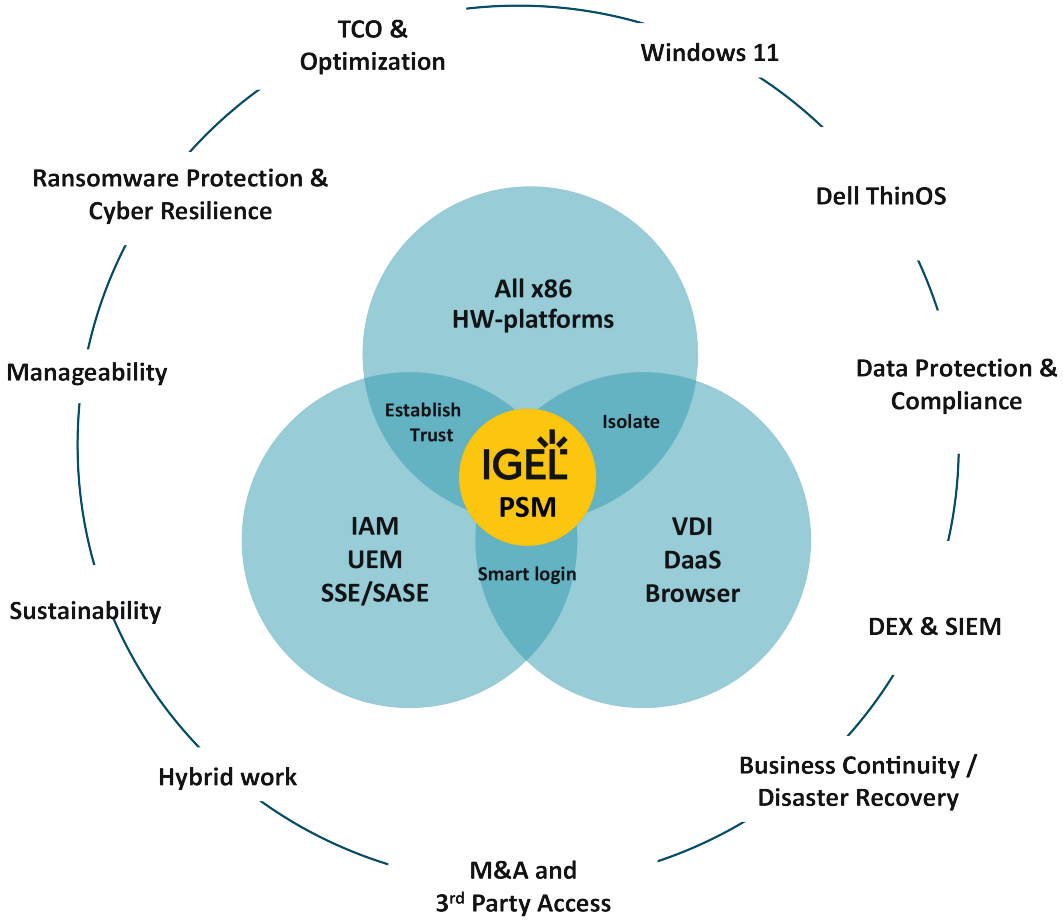
- Highly tunable role-based access and transaction logs ensure a high level of security and compliance for all types of workers throughout the healthcare organization.

Multiple integrated VPN solutions

- Multiple integrated VPN solutions to tunnel access to protected and on-premises company resources. OpenVPN Connect Standard and Government NCP-e VPN client GenuCard support for highly secure connections through HW VPN box.

IGEL Preventative Security Model and Partner Ecosystem

At the intersection of hardware, applications, and security, the Preventative Security Model™ establishes **trust, isolates, and enables smart login** through integration with leading solutions. IGEL optimizes healthcare environments while helping assure excellent digital experiences for clinicians, physicians, administrators, and operational staff. The IGEL Ready partner program ensures solutions are tested and supported.



The following table illustrates how IGEL collaborates and integrates with multiple key technologies to deliver powerful, comprehensive solutions and services within healthcare:

Endpoint Hardware	Endpoints—including desktops, laptops, tablets, and thin clients—enable healthcare professionals to access electronic health records (EHRs). IGEL OS runs on any compatible x86-64 device. Partners **HP, Lenovo, and LG** Business Solutions pre-install IGEL OS. In addition, IGEL OS runs on a wide range of industry specific devices as listed on the IGEL Knowledge Base.
Peripheral Hardware	IGEL OS supports popular unified communications peripherals like **EPOS, Jabra, and Poly** mics and headsets, dictation devices, and software for clinical communications such as Vocera and many more. Keyboard encryption via the **Cherry** Secure Board guarantees immediate encryption of keystrokes to lock out keyboard logging and key stroke tampering. IGEL OS supports SINA workstations from **Secunet** that are approved for processing classified information up to and including SECRET, NATO SECRET and SECRET UE/EU SECRET. Advanced Device Redirection ensures seamless user experience by providing full functionality of local peripherals within virtual desktop environments.

Secure Browser, DaaS, SaaS, and VDI	IGEL partners with industry leaders across DaaS, SaaS, or VDI. Secure browser: **Island**. The Island secure browser enables restricted access to sensitive data for enterprise-controlled access to HTML based protocols and websites. DaaS: **Microsoft Azure Virtual Desktop (AVD), Windows 365 Cloud PC** SaaS: Broad range of partners incl. **Crowdstrike, Palo Alto, Fortinet** VDI: **Microsoft, Omnissa, Citrix, Parallels, Workspot**
Identity and Access Management (IAM)	The IGEL Agent for Imprivata integrates IGEL OS and **Imprivata Enterprise Access Management** to enable fast, no-click access to Microsoft AVD, Windows 365 Cloud PCs, and Microsoft Frontline. IGEL OS supports modern authentication methods including: • Kerberos-ticket-handling, based on username and password, with two-factor smartcard solutions (smartcard and PIN) through a three-party-constellation. • Middleware options to support smartcard + pin • Multi-factor authentication • IGEL OS endpoint device • Active Directory infrastructure • Kerberos enabled service (Citrix XenApp or XenDesktop) • Biometric solutions Enhance Authentication with IGEL partners including: • **Imprivata Enterprise Access Management** • **Microsoft Entra ID, EntraID-CA** • **Microsoft Intune** • **Okta** • **OpenID Connect** • **Ping Identity Ping One** • **DeviceTRUST** • **YubiKey** • **HID Global fingerprint.** Contextualized access to services and applications. Context of a device is key in a mobile world to provide secure access to enterprise infrastructure in real-time.

Unified Endpoint Management (UEM)	The **Microsoft Intune Agent** for IGEL OS provides visibility of IGEL OS devices within the Intune console giving admins a single place to asset track and apply security checks and policies. **Omnissa Workspace ONE** and IGEL provide a seamless and powerful user experience with WS1 and Horizon 8. Benefits include improved endpoint security, rapid and secure onboarding, simplified management, and reduced costs.
Secure Access Service Edge (SASE)	SASE, or Secure Access Service Edge, is a modern networking and security framework that integrates network and security functions into a cloud-based service. In healthcare, SASE eases secure access to electronic health records and patient information across clinical locations over wide geographic areas. IGEL and partners **Microsoft, NetScaler, Netskope, and Zscaler**, Palo Alto, supports SASE in: • Remote Access • Branch/Satellite Facility Connectivity • Enhanced Security • User Experience • Scalability • Cost Savings & Operational Efficiencies
Digital Experience (DEX)	Digital Experience (DEX) supports widely distributed workforces where work-from-home and hybrid work models dominate. IGEL partners with DEX industry leaders **ControlUp, Liquidware, eG Innovatations,** and **Lakeside.**
Security Information and Event Management (SIEM)	IGEL OS communicates with various SIEM platforms via the REST API on the Universal Management Suite. User, login, account, and configuration event logs and can be used by SIEM platforms, the Rsyslog interface or filebeats for further analysis and event correlation. Example systems include Splunk or Graylog

How IGEL Supports Zero Trust

IGEL helps organizations significantly reduce the risk of ransomware or malware at the endpoint supporting organizations that are implementing a Zero Trust approach to security. Thanks to integrations with leading security partners, the support of Zero Trust can reach beyond just the device and can include:

User/Identity

IGEL partners with leading authentication vendors to deliver identity and access management, multi-factor authentication and conditional and contextual access.

No user credential information is stored on the endpoint ensuring no session information could be retrievable.

IGEL integrates with leading Secure Access Service Edge (SASE) and Secure Service Edge (SSE) vendors to further support security and Zero Trust initiatives.

Device

IGEL's Preventative Security Model eliminates common endpoint device vulnerabilities in the target of cyber-attacks. The inherent read-only OS, no local data storage, and a modular design, IGEL meets Zero Trust Device Pillar capabilities including:

- Device inventory
- Device detection and compliance
- Device authorization
- Remote access
- Patch management
- Endpoint management.

Applications and workloads

With IGEL OS, users have no ability to install unvetted applications to the endpoint device which prohibits rogue, corrupt, or malicious applications on the endpoint. This further reduces the operational overhead of detecting and auditing application instances and licensing at the endpoint enabling a focus on virtualized or SaaS application instances.

Only the IT Admin can start software deployment, authorize upgrades and patches available from IGEL or IGEL Ready certified apps available through the IGEL App Portal.

The **IGEL App Creator Portal** is a powerful tool designed to simplify and streamline the process of building, packaging, and distributing custom applications for IGEL OS devices. It empowers IT administrators, developers, and organizations to create IGEL-compatible applications that meet specific business needs while supporting security and performance standards. The portal also supports **Community** and **Enterprise Certificates**, ensuring trusted and secure app deployments across environments. The IGEL administrator has immense control over the capabilities of each type of end-user based on their job role.

No Local Data

No data is stored on an IGEL OS endpoint. In the event of a device's loss or theft, organizations can ensure that no customer, patient, or restricted information is breached.

Automation and Orchestration

The IGEL Universal Management Suite configures and deploys policies to IGEL OS devices. Administrators have a single view of policy creation and deployment. IGEL logs can integrate into existing security programs by leading SIEM platforms.

Visibility and Analytics

User, login, account, and configuration events logs and can be used by SIEM platforms, the Rsyslog interface or filebeats for further analysis and event correlation. Example systems include Splunk or Graylog

IGEL also partners with visibility and digital experience (DEX) technology providers including ControlUp, Lakeside, and CrowdStrike when partnering with Omnissa, who in turn can consider IGEL-generated data within their overall visibility, monitoring, and remediation capabilities.

IGEL Support for Healthcare Security and Compliance

The IGEL Preventative Security Model brings a fundamental change in approach to endpoint security that supports key security and compliance initiatives in healthcare:

Ransomware Protection

As previously mentioned, a top IT-based concern for healthcare organizations is ransomware, which can hinder or disrupt the delivery of patient care by:

- making critical patient records and other IT systems unavailable
- leading to public disclosure of patient information
- in the most extreme cases, impacting the quality of patient care.

Through the IGEL Preventative Security Model, healthcare organizations globally can significantly reduce the potential for an endpoint-based cyber-attack while also reducing software and hardware costs and the operational hours of planning, implementing, delivering, and troubleshooting the inpatient, outpatient, and primary care clinical endpoints. The Preventative Security Model can improve security of protected health information (PHI) and personally identifiable information (PII) and directly simplify the endpoint security requirements required by:

- Health Insurance Portability and Accountability Act (HIPAA)
- Data Security Protection Toolkit (DSPT) National Health Service, UK
- Cybersecurity and Infrastructure Security Agency (CISA) Framework
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- NIS2 Directive, the European Union's Cybersecurity Framework

Integration with leading authentication and single sign-on solutions including Imprivata, Okta and Microsoft Entra ID coupled with extensive support for healthcare-critical peripheral devices including printers, scanners, signature pads, badge scanners, and speech mics/dictation technologies allows IGEL to be quickly and easily incorporated into a broad range of use cases and workflows.

Business Continuity with a defense-in-depth solution

Hospitals and clinics have a moral responsibility to offer non-stop care for their patients, especially those in emergencies and acute care despite disruptions caused by cyberattacks, IT outages, and natural disasters. IGEL Business Continuity offers multi-level options for rapid endpoint recovery amidst a cyberattack or IT outage.

IGEL Business Continuity includes dual boot and IGEL Business Continuity USB Boot which is set up with an IGEL specialist. The dual boot is installed on the device to enable clean boot to IGEL OS to access apps and data, even on a compromised device. If the hard disk on the device fails preventing dual boot, the IGEL BC USB Boot allows fast access to essential data from any device. The Business Continuity Specialist will guide the IT team in advance to define and test the image, configure and lead endpoint recovery exercises at pre-set appointments throughout the year.

Secure, Protected Digital Signage

IGEL OS is ideal for running digital signage solutions on any compatible x86-64 device by providing a robust security layer and central management to ensure digital signage solutions run safely and efficiently across all functions and locations within a healthcare system for a better employee, patient, and visitor experience.
IGEL offers the IGEL Digital Signage App for easily enabled, secure digital signage.

IGEL OS – Healthcare's Secure Endpoint OS for Now & Next

IGEL is the secure endpoint OS for cloud and digital workspaces. Preventative security, data protection, and business continuity in collaboration with our partners are at the forefront of IGEL OS design and development. This paper represents an ever-evolving set of integrated capabilities designed to reduce the endpoint attack surface and deliver a preventative approach to security for healthcare.

Connect with IGEL to stay informed about the latest developments and features.

Demo IGEL on your own device.

Download trial licenses on **IGEL.com/form-download**

Find more information on **IGEL.com/healthcare**