IGEL Security Whitepaper

Contents

Introduction

As enterprise workloads increasingly shift away from being run at the endpoint to either hosted environments such as virtual desktop infrastructure (VDI), desktop as a service (DaaS), or pure cloud software as a service (SaaS) applications, organizations have a once in a generation opportunity to re-think their endpoint strategy, and in particular, a better approach to endpoint security. While today's endpoint security strategies largely consist of layers of defenses built to protect inherent vulnerabilities, IGEL takes a different approach, utilizing a secure Linux operating system that removes these vulnerabilities through a Preventative Security Model™. In this paper we will discuss the components of the Preventative Security Model, standards that IGEL can support adherence to, and security partners that IGEL partners with to deliver a complete security solution that supports best practice security approaches such as Zero Trust.

Preventative Security Model

IGEL OS is designed around the Preventative Security Model which removes the attack vectors exploited by bad actors for ransomware and other cyber-attacks. Through the Preventative Security Model, IGEL can be a key element in the delivery of Zero Trust approaches to IT security.

Key tenets of the IGEL Preventative Security Model

Read-only OS

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

No Local Data Storage

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

Trusted Application Platform

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

Modular Design

- By delivering only what is needed at the endpoint, the attack surface is kept to a minimum. The IGEL App Portal enables partner applications to be installed as needed.

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.

Support for leading authentication and single sign-on solutions.

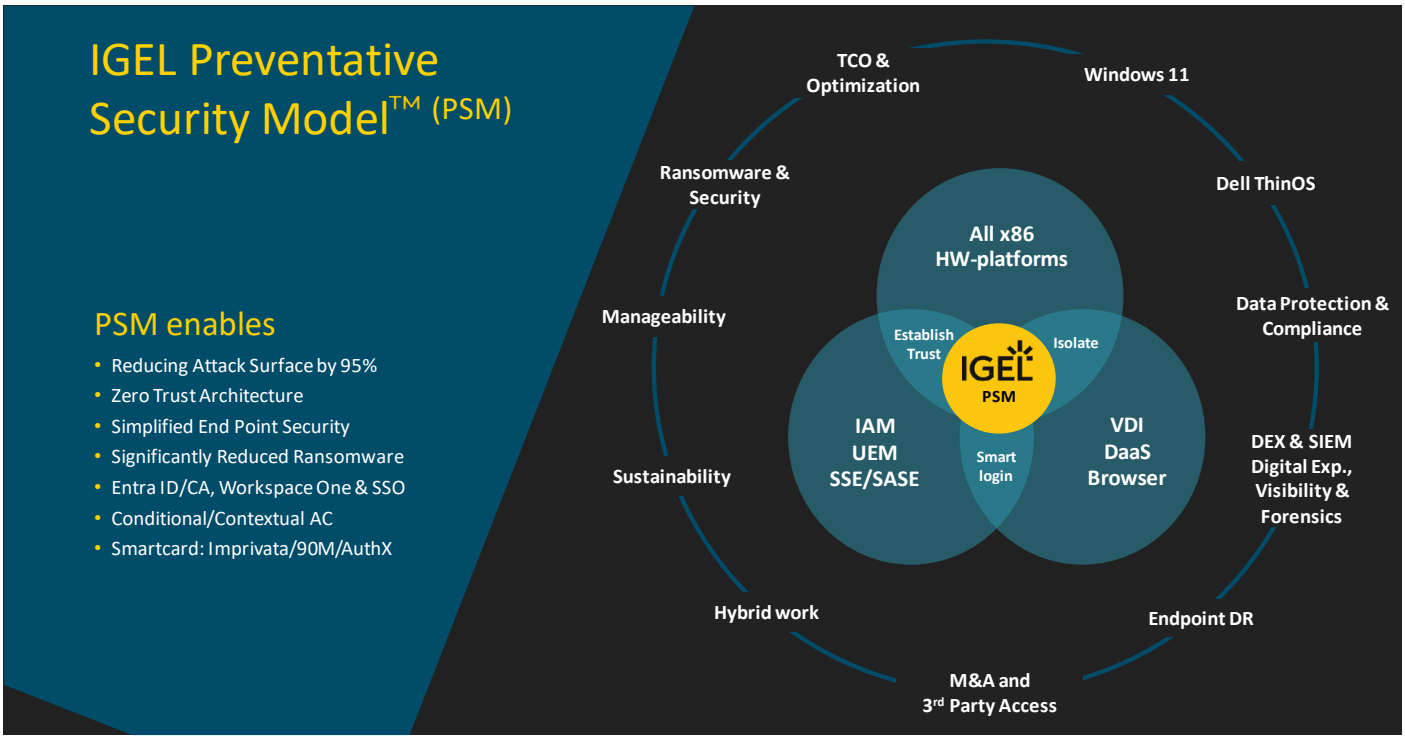
- IGEL integrates with leading authentication and single sign-on solutions to ensure fast, secure access to desktops and applications including:
  - 90meter
  - Imprivata
  - Microsoft EntraID, EntraID-CA
  - Okta
  - OpenID Connect
  - Ping Identity Ping One
  - VMware Workspace One Access

Centralized Management

- IGEL Universal Management Suite (UMS) provides a single point of management for tens of thousands of IGEL's endpoints both on, and off, the corporate network. UMS 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 SIEM platforms for compliance with existing policies.

Through the **IGEL Preventative Security Model** organizations can save significant resources on the acquisition, testing, management and troubleshooting of security and management tools including antivirus, endpoint detection and response, data loss prevention, backup and recovery, and more.



A Secure Endpoint Strategy for Now & Next

Many organizations are already experiencing the security benefits of moving application workloads away from the endpoint to VDI, DaaS and SaaS environments. The ability to use a secure by design endpoint OS has been proven to reduce security risks and reduce time to recovery in the event of an attempted attack. By removing the need for endpoint security and management agents including EDR, AV, DLP, backup and recovery etc., organizations can save significant CAPEX and OPEX.

As organizations consider their Windows 11 migration strategy, many are evaluating moving Windows 11 to the cloud with Microsoft Azure Virtual Desktop, Windows 365 and Cloud PC. With the Windows desktops and applications running in the cloud, organizations can rethink their endpoint strategy, deploying a secure OS that is designed for the new cloud first architectures.

IGEL Security Capabilities

IGEL OS Trusted Application Platform

- A secure-boot chain of trust ensures that components of the IGEL OS have not been tampered with.
- A controlled boot sequence is initiated upon switching on the device.
- 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 fail to 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 designated by IGEL or Microsoft keys approved by IGEL can load the operating system. IGEL generates and manages the cryptographic platform exchange keys which are included in the corresponding UEFI versions.
- If tampering is detected, the system will not boot.
- Configuration files are written to a dedicated and encrypted partition ensuring 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.
- With IGEL OS 12, Apps and services are separated from the base OS. Only the required features and functionality are deployed to the endpoint based on the administrator's decisions. This optimizes the endpoint keeping the endpoint as "lean" as possible to minimize the attack surface of the device, thereby minimizing the opportunity for malware including ransomware attacks. Additional functionality and partner integrations can be downloaded from the IGEL Application Store and distributed from the Universal Management Suite by the administrator.
- The IGEL chain of trust runs with IGEL OS on any compatible x86 64-bit device supporting UEFI and secure boot.
- If users connect to a VDI or cloud environment, access software such as Citrix Workspace App or VMware Horizon checks the certificate of the server to which they are connecting.

This chain ensures system integrity as it makes sure that none of the components in your environment have been tampered with – a core capability of the Preventative Security Model

Authentication

IGEL OS supports modern authentication methods including:

- Kerberos-ticket-handling, based on username and password, with two-factor smartcard solutions (smart-card and PIN) through a three-party-constellation.
- Middleware options to support smartcard + pin
- Multi-factor authentication
- IGEL OS-powered endpoint devices
- Active Directory infrastructure
- Kerberos enabled service (Citrix XenApp or XenDesktop)

Authentication can be enhanced with IGEL partners including:

- 90meter
- DeviceTRUST
- Evidian
- Imprivata
- Microsoft Entra ID
- Okta
- Ping Identity Ping One
- VMware Workspace One Access
- Yubikey

IGEL OS Integrated Security

IGEL partners with leading vendors across the application and security space. The IGEL Ready partner program ensures solutions are tested and supported for even the most demanding environments. Security partnerships and integrations include:

Secure enterprise browsers	Secured browser with restricted access to sensitive data enabling enterprise-controlled access to HTML based protocols and websites.
Multiple integrated VPN solutions to tunnel access to protected and on-premises company resources.	OpenVPN Connect Standard and Government NCP-e VPN client Genua GenuCard support for highly secure connections through HW VPN box
Keyboard encryption	Keyboard encryption via the Cherry Secure Board guarantees immediate encryption of keystrokes to lock out keyboard logging and key stroke tampering. Secunet SINA Workstation support 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.
A broad range of supported smartcard solutions addressing the needs of different verticals like healthcare and financial services.	IGEL Smartcard SafeNet Aladdin eToken Thales SafeNet middleware for Gemalto/SafeNet eToken, IDPrime smart cards and token Cryptovision sc/interface middleware for Cryptovision smart cards NXP Cryptas IDProtect middleware for IDProtect smart cards A.E.T. SafeSign middleware for SafeSign smart cards Pointsharp Net iD middleware for Net iD smart cards Coolkey middleware Coolkey OpenSC middleware OpenSC 90meter middleware

Broad range of supported smartcard readers to address specific vertical needs and compliance criteria.	Elatec TWN4 CCID PC/SC Lite M.U.S.C.L.E. HID OMNIKEY REINER SCT cyberjack
Identity provider support	Imprivata OneSign ProveID Embedded IGEL Agent for Imprivata Evidian AuthMgr Contextualizing VMware Workspace One Access OpenID Connect based Service including Microsoft EntraID, Okta, Ping Identity
Contextualized access to services and applications. Context of a device is key in a mobile world to provide access to enterprise infrastructure in real-time and secure.	DeviceTRUST considers various contextual information (IP, geolocation, network etc.) when controlling access to data and applications enabling granular, compliant conditional access control.
Support for biometric solutions	HID Global fingerprint readers. Fujitsu palm vein scanner.

IGEL also enables secure shadowing of devices to provide instant secure access for helpdesk agents. Role-based access and transaction logs ensure a high level of security and compliance.

IGEL Management

The IGEL Universal Management Suite (UMS) ensures IGEL endpoints are up to date and configured with the correct apps and services to ensure the best possible user experience and highest levels of security. Security features with IGEL UMS include:

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

- Shadowing enables IT personnel 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. The UMS server then establishes a TLS tunnel to the device which is 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 extension
- The High Availability Extension enhances the deployment of new settings across tens of thousands of devices simultaneously. This is facilitated 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. A username and password are required to log in again.

How IGEL Supports Zero Trust

IGEL helps organizations dramatically 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 that are targeted during cyber-attacks. By ensuring the endpoint itself cannot be compromised through a series of secure by design measure including a read-only OS, no local data storage and a modular design, IGEL is able to directly meet many. Device Pillar capabilities including:
    - Device inventory.
    - Device detection and compliance.
    - Device authorization.
    - Remote access.
    - Patch management.
    - Endpoint management.
- Additionally, the need for a complex layer of security and management tools is removed, saving both CAPEX and OPEX budget while delivering greatly improved endpoint security.

Applications and workloads

- With IGEL OS users have no ability to install applications to the endpoint device ensuring rogue, corrupt, or malicious applications cannot be introduced at 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.
- Software deployment can only be initiated by the IGEL administrator. This can be for authorized upgrades and patches available from IGEL or using IGEL Ready certified applications available through the IGEL Application Store.

Data

- No data is stored on an IGEL OS endpoint. In the event of loss or theft of a device organizations can be certain that no customer, patient, or restricted information will have been breached as a result.

Automation and Orchestration

- The IGEL Universal Management Suite is used to configure and deploy policies to IGEL OS devices. Administrators have a single view of policy creation and deployment. Detailed endpoint policies can be created with more than nine thousand options available.
- IGEL logs can be consumed by leading SIEM platforms to integrate into existing security programs.

Visibility and Analytics

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

IGEL Support for Industry Security and Compliance

The IGEL Preventative Security Model brings a fundamental change in approach to endpoint security that can benefit all industries by removing many of the attack vectors in traditional endpoint solutions, immediately decreasing the chances of ransomware and malware, simplifying the operationalization of endpoint security and decreasing the associated costs. Here are some of the ways in which IGEL can support the security and compliance initiatives of five specific industries:

Healthcare

One of the top IT based concerns for healthcare organizations is ransomware, which can disrupt the delivery of patient care by:

- making critical patient records and other IT systems unavailable
- Leading to public disclosure of patient information

Through the IGEL Preventative Security Model, healthcare organizations globally can significantly reduce the potential for an endpoint-based cyber-attack whilst 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:

- HIPAA
- Data Security Protection Toolkit (DSPT – NHS)
- CISA Cybersecurity framework

Integration with leading authentication and single sign-on solutions including Imprivata, Okta and Microsoft Entra ID coupled with extensive support for the critical peripheral devices including printers, scanners, signature pads, badge scanner, speech mics ensure IGEL can be incorporated into a broad range of use cases and workflows.

Financial Services

Financial services organizations are at the forefront of digital transformation, innovation and growth leveraging digital to deliver innovative new services and customer experiences while reducing costs. As with other industries they are also a leading target for cyber-attacks. This innovation, along with stringent compliance regulations, is driving FSI organizations to rethink the desktop computing model centralizing data and resources through cloud services. The IGEL Preventative Security Model plays a critical role in closing the security gaps that are the very reason to move to cloud infrastructure. By simplifying and securing the endpoint with IGEL, FSI organizations can simplify the endpoint security requirements required to secure payment card industry (PCI) and PII information and meet compliance regulations.

Retail

Leading retailers are regularly targeted due to the vast amounts of customer and financial payment information that they hold. The disruption of service through a ransomware attack can cost retailers hundreds of millions in lost business, reputational damage and impact on the organization's stock price.

Retail has a broad set of use cases that require endpoints to be positioned in relatively unsecured locations including point of sale (POS), stock room and other logistical settings in addition to the back office, call center and other office centered roles.

The IGEL Preventative Security Model in conjunction with VDI, DaaS and SaaS applications play a critical part of a retail IT security strategy, securing the PCI, PII, logistical and financial information required for retailers to function.

Manufacturing

The convergence of IT and operational technology (OT) systems is creating significant security challenges for manufacturing organizations. This convergence has exposed formerly air-gapped networks to exposure from attacks emanating from the IT networks.

IGEL helps manufacturing organizations significantly reduce the risk of ransomware and malware by significantly reducing the risk of a cyber-attack at the endpoint. In conjunction with desktop virtualization and cloud workspace solutions, IGEL can enable distributed teams to collaborate on complex design, logistical and administrative tasks while securing the organizations intellectual property and financial information. In addition, as a secure Linux based OS, IGEL can be implemented in OT networks to further reduce the attacks surface of these vulnerable devices.

Government

Due to the increasing challenges of nation state attacks and cyber-warfare there is a global drive for governments to improve cybersecurity. Threats range from highly coordinated attacks on critical infrastructure to the targeted theft of political leaders' laptop devices. In the United States, the White House's Executive order (EO14028) on improving the nations cybersecurity accelerates the adoption of cloud services and a Zero Trust architecture. The Whitehouse office of Management and Budget has set a deadline of September 30, 2024, for federal and civilian agencies to adopt some level of Zero trust architecture with a goal to reach full zero Trust by 2027.

The IGEL preventative security model is a critical part of a Zero Trust approach to security not only by directly addressing the device pillar but also partnering with leading vendors across other pillars of the architecture to support an integrated approach across the organizations entire IT estate.

Integration with 90meter provides support for CAC/PIV and High Assurance smartcards.

IGEL OS - The Secure Endpoint OS for Now & Next

The IGEL OS Preventative Security Model takes a secure by design approach, replacing the outdated model of monitor, detect, remediate with a model of prevent. The Preventative Security Model eliminates the vulnerabilities that bad actors target, significantly reducing the threat of ransomware and malware.

By securing the enterprise endpoint, reducing TCO, enabling the fast repurposing of existing devices and delivering a first-class user experience, IGEL can add value to a broad range of enterprise-wide initiatives including:

- Data protection and compliance
- Digital employee experience (DEX)
- Hybrid work
- M&A
- Sustainability initiatives

IGEL's focus is on providing the ultimate endpoint OS for cloud and digital workspaces. Security and data protection are at the forefront of our IGEL OS design and development efforts. The above information represents an ever-growing set of integrated capabilities designed to reduce the endpoint attack surface and provide the strongest possible endpoint protection.

Connect with IGEL to stay informed about the very latest developments and features from IGEL to help fortify your endpoints and ensure that your transition to the cloud is as easy and secure, as possible.

Demo IGEL on your own devices

Download free licenses on **IGEL.com/form-download**
Find more information **IGEL.com**
Follow us on
@IGEL_Technology I igel.technology I IgelTechnologyTV I igel-technology I IGEL.com

IGEL is a registered trademark of IGEL Technology GmbH.
All hardware and software names are registered trademarks of the respective manufacturers.
Errors and omissions excepted. Subject to change without notice. © 05/2024

Visit us at igel.com