SOLUTION BRIEF

IT-Security for
IGEL-powered Endpoints

DriveLock

1   Introduction

Server-based computing, in particular terminal services and the provision of VDI environments in conjunction with Thin- and Zero-Clients, is becoming increasingly popular in small and medium-sized companies. It offers the possibility of a central, easy-to-manage system environment. With the Universal Management Suite (UMS), which is supplied free of charge, IGEL provides a sophisticated endpoint management solution with automated backend control for IT, while delivering a trouble-free environment to users. UMS offers a wide-range of features which enable the devices to be adapted to specific needs via zero touch deployment, thus conserving resources and reducing costs. In order to allow trouble-free efficient work IGEL is constantly working on improvements and optimizations with a particular focus on security. The partnership with DriveLock is proof of both companies' desire to improve security within networks.

When it comes to protecting existing USB interfaces, a lot of administrators contemplate how they can implement corporate IT security requirements without obstructing processes and the productivity of employees. Turning off this interface is often the administrator's solution of choice, even if this requires special thin-clients to be subsequently switched on again in a complex manner. The flexibility - in particular access rights exactly coordinated with the user or a user group - is often missing along with the option to encrypt copied data on external drives to protect the files from unauthorized access if the medium is lost.

2   Multi-Dimensional Interface Control

DriveLock offers the precise solution that restores lost flexibility to the company and simultaneously provides an optimal data security. In connection with IGEL-powered endpoints, the unique interface control provides comprehensive protection for the USB interface and can just as easily configured as normal workplaces.

The DriveLock Virtual Channel is already included in IGEL's Linux based firmware. IGEL OS simplifies access to virtualized desktops and applications and standardizes endpoints. It runs on any compatible 64-bit, x86 device and enables adaptive configuration and granular control. As a result, access rights and security settings for external storage devices can be configured with great detail, even for the serial number of an individual USB stick.

With the help of the central DriveLock Management Console and guidelines you can specify which user is allowed to use which USB drives and if write access or only read access is possible. Using the integrated file filter, you can stipulate what types of files may be read from or written to an external drive. As an optional extra, accurate logging of access to files is also available.

3 DriveLock actively improves the employees' security awareness

DriveLock also helps to improve the security awareness of employees. For example, you can allow access to external interfaces only after the user has first read and accepted the company directives or a security notice.

Employees can receive specific information on the correct behavior, and the necessary security measures that should be applied during certain activities, for example, when inserting a USB stick or connecting to a Bluetooth device (Security Awareness Campaigns may be presented). Through this direct connection, the illustrated regulations will be ingrained in user's behavior. A simple method to improve the security awareness of your employees is to conduct Security Awareness Campaigns once a week or one a month, automatically displayed on the computer after login.

You can flexibly set up the DriveLock Security Awareness Campaigns according to your needs: targeting specific user groups, network environments, computer groups or specific time period. Thereby, allowing the option to select the most suitable communication format from a variety of delivery forms: Unformatted or formatted text, images or graphics, PDF documents, videos or existing websites from the intranet or internet. If you already have your own security training content, you can integrate them quickly and easily. This ensures a target-group-oriented, and thus effective communication. You can decide whether an employee can skip the displayed content, or whether it must first be viewed completely, and even if it needs to be confirmed.

Therefore, employees and DriveLock become important components of your future-oriented security strategy.

4 Data security also on-the-go

In connection with DriveLock Encryption 2-Go - already included in DriveLock Smart DeviceGuard - external drives can be automatically and transparently encrypted for the users. Therefore, the information on a USB stick is protected from unauthorized use in case it is lost. In comparison to other solutions, the encryption in DriveLock is closely interlinked with the drive control.

DriveLock encryption in turn enables a highly-simplified handling of the central policies for the secure handling of data and external storage devices. DriveLock provides the user with an additional network drive within their working environment when a storage device previously encrypted with DriveLock is used on a Thin-Client.

This network drive allows files to be saved encrypted without requiring any further actions by the user. In addition, the intelligent management ensures that access to the unencrypted area is not possible.

5   Innovative Analysis Options and Reporting

With the DriveLock Control Center you can analyze and monitor the usage of removable devices as well as data transfers through flexible reporting and dynamically created requests.

In case of legal requirements regarding the transfer of personal data you can prohibit access to personal data or encrypt such data in line with corporate policies. Additionally, the DriveLock Control Center offers a quick overview of all DriveLock agents within your environment and delivers current results about status and licensing. But the DriveLock Control Center can do a lot more.

In case of an emergency, the advanced forensics options of DriveLock can be used to analyze an incident from different perspectives and angles to find a possible data breach. With a simple drill down methodology you will know from which computers a certain file was copied to which USB stick, if it was renamed and what other files were transferred at the same point in time.

Need to go deeper? DriveLock Control Center will show you all computers on which a USB stick was used - making finding the "needle in the haystack" faster and easier than ever.

6   Supported solutions

DriveLock is supported by all

- IGEL Universal Desktop Thin Clients
- endpoints converted by IGEL Universal Desktop Converter (Thin Clients, Fat Clients, Noteboks)
- endpoints temporary converted by IGEL UD Pocket.

For further information, visit kb.igel.com.

About DriveLock

DriveLock SE, is headquartered in Munich, Germany with offices in Sydney, Australia and has become one of the leading Endpoint Protection Platform software vendors over the past 15 years.

The Endpoint Protection Platform from DriveLock is particularly strong when used in the extremely granular environment of Device Control for USB protection, as well as for the encryption of hard disks, SSD's or USB memory devices. Applications and their associated devices can be comprehensively protected with the Smart AppGuard based on integrated Artificial Intelligence with Predictive Whitelisting and Machine Learning functionality.

DriveLock supports various operating systems, devices, and is available as a hybrid solution either on-premise or from the cloud.

Facts & Figures:

✓ Multiple awards as an endpoint protection solution

✓ Honored as a TOP 100 innovator in 2017 and 2018

✓ More than 3000 customers in 30 different countries across the world

✓ Customer environments with up to 180,000 endpoints supported

✓ Made in Germany, "without a backdoor"

To download and test the DriveLock Endpoint Protection Platform visit www.drivelock.com/free-trial-business

About Igel

IGEL delivers powerful unified endpoint management software that is revolutionary in its simplicity and purpose-built for the enterprise. The company's world-leading software products include the IGEL OS™, Universal Desktop Converter™ (UDC), IGEL Cloud Gateway™ (ICG), IGEL UD Pocket™ (UDP) and Universal Management Suite™ (UMS).

These solutions enable a more secure, manageable and cost-effective endpoint management platform across nearly any x86 device. Additionally, IGEL's German engineered and manufactured thin, zero and all-in-one client solutions deliver the industry's best warranty (5 years), support (3 years after end of life) and management functionality.

IGEL enables enterprises to precisely control all devices running IGEL OS as well as Windows OS from a single dashboard interface. IGEL has offices worldwide and is represented by partners in over 50 countries.

To download the IGEL UMS or the IGEL Universal Desktop Converter™ (UDC) visit www.igel.com/download.

CONTACT:

DriveLock SE
Landsberger Str. 396
81241 Munich
GERMANY

+49 89 546 36 49 0
info@drivelock.com
www.DriveLock.com