Ovum
TMT intelligence | informa

Igel's Security Enhancements for Thin Clients

Secure Boot, MDM essentials, encrypted keyboard traffic, and contextual awareness are on the roadmap

Publication Date: 01 Feb 2018 | Product code: INT003-000038

Rik Turner

Summary

Catalyst

Thin client vendor Igel is enhancing the security capabilities of its products, both under its own steam and in collaboration with technology partners. Ovum sees these developments as important for the next wave of thin client computing, which will be software-based – particularly if the desktop-as-a-service (DaaS) market is to take off.

Ovum view

With hardware-based thin client shipments in the region of 4–5 million units annually, this market is still a drop in the ocean compared to the 270 million PCs shipping each year, though the latter figure has been declining since 2011. And within the thin client market, Igel is in fourth place behind Dell and HP (each at around 1.2 million units annually) and China's Centerm, which only sells into its home market.

However, the future for thin clients looks bright, in that the software-based segment of the market (which some analyst houses refuse to acknowledge) is expanding, particularly for Igel. Virtual desktop infrastructure (VDI) technology has stimulated this growth, but the greatest promise is probably in the embryonic DaaS market, whereby enterprises will have standard images for their workforce hosted by service providers.

Security will clearly be crucial for the success of any such evolution. As thin clients become more mainstream, they will become more of a target for hackers and threat actors generally, as has already happened with devices running Apple's operating systems. As we discuss in this report, there are good reasons for hackers to target thin clients, despite the inherent security of their having no local storage.

Thus, the security initiatives both at Igel itself and its partners are to be welcomed. Ovum sees a clear requirement for increased security in this market, particularly as thin clients go mobile and as users seek to access their desktop environments from anywhere, at any time, and from any device.

Key messages

- Thin clients are desirable targets for hackers.
- Igel is beefing up its security functionality.
- Partners are adding further security capabilities.

Recommendations

Recommendations for enterprises

If you are considering a refresh of your desktop and/or laptop estate, particularly for employees performing more standard functions, thin client technology is a cost-effective alternative and, as this report highlights, an increasingly secure one. Igel's central management capability for its technology is already strong and is gaining further muscle as it adds more security capabilities, including some

mobile device management (MDM) functionality, making it a compelling candidate for any thin client project.

Recommendations for service providers

The DaaS market is still in its infancy, but with ever more corporate employees working remotely for all or part of the time, and with increasing amounts of enterprise applications residing in the cloud, this way of delivering desktop functionality makes ever more sense. Multitenancy and secure central management will be fundamental for DaaS to take off, and Igel is already mindful of these requirements in the way that it is developing its offering.

Thin clients are desirable targets for hackers

Data theft and DDoS attacks are two of the inherent risks

Thin client sales are already often driven by security concerns, since their inability to store data locally makes them a safer option than desktop or laptop machines for some companies. However, there are still good reasons for threat actors to hack into them:

- Thin clients can be an on-ramp for an entire corporate network, from which a hacker can steal the credentials of legitimate users and access back-end systems with valuable information.
- They can be a useful platform from which to carry out reconnaissance, gathering intelligence on the structure of the victim's network, user, and server names.
- Data can be exfiltrated from a corporate infrastructure via their USB port.
- Distributed denial-of-service (DDoS) attacks can be mounted from thin clients, slowing or even stopping legitimate traffic across an entire network, by plugging in a USB drive that pretends to be a keyboard and forwards bogus instructions to the endpoint.

Igel develops security internally and with partners

Thus, Igel is developing further security functions and features beyond the standard absence of a hard drive, both on its own and in collaboration with some of its security-focused partners. Some of them were on show at the company's recent Disrupt EUC customer and partner event in Bremen, Germany (www.disrupteuc.com).

Igel is beefing up its security functionality

UEFI Secure Boot is coming

In terms of the enhancements Igel is making to security in its thin client portfolio, there are several initiatives underway.

The company's proprietary Linux distribution, Igel OS, is inherently more secure than others, not only because it is read-only, but also on account of its modular nature. This means that when the IT department is configuring a new thin client, it can choose not to enable types of functionality that the end user won't need.

Igel is going beyond such capabilities, however. It is, for instance, introducing a Secure Boot mode, enabled by the Unified Extensible Firmware Interface (UEFI) specification, such that signatures on the bootloader can be checked, and any Secure Boot–enabled hardware that does not bear a signature, or whose signature does not tally with what the system expects, can be blocked.

The company will include this feature in the UD Pocket product it launched last year, whereby a software thin client running Igel OS can be booted up from a USB drive and create a secure environment independent of the native OS and applications running on an endpoint. It is also building it into its hardware thin clients and readying a version of Igel OS that will check the signature on the shim boot loader. For the future, Igel also plans to check signatures at the partition level, giving increased granular control of what will and will not be blocked.

Mobile device management essentials are coming to UMS

Another additional security feature Igel plans to introduce is a subset of mobile device management (MDM) capabilities, focused specifically on the control of data rather than any device functionality. This feature will be added into the company's Universal Management Suite (UMS), the central management console for all its thin clients, both hardware and software ones.

A stripped-down Firefox is in preparation

Igel is also working on a stripped-down version of the Firefox browser for its thin clients, the idea being to deliver a browser that, for greater security, does not have access to certain assets on the device, such as its local file system.

Pen testing and CIS Secure Suite integration

To certify the security of its products, the vendor is currently using the services of two independent penetration testing firms, namely Compass Security from Switzerland and Secuvera in Germany. Beyond that activity, it is now building security into the continuous integration system it uses for software development.

To this end, Igel has joined the Center for Internet Security (CIS), a nonprofit that develops best practices and benchmarks for cyber defense and is integrating the CIS SecureSuite tools into its engineering workflow.

Partners are adding further security capabilities

Keylogger-proof keyboards are in development

Cherry GmbH, a manufacturer of data input devices (keyboards, mice, card readers, and so on) has a proof-of-concept of a secure keyboard, which encrypts data traveling from keyboard to thin client as a means of defense against keyloggers installed on the site for reconnaissance.

The project requires collaboration between Igel and Cherry because the security function is triggered by code residing on the endpoint, and thus integrated into the manufacturer's proprietary Linux distribution, called Igel OS. This code is also able to verify that the input device is a genuine keyboard rather than a USB stick posing as one.

The encryption capability comes at a premium

Cherry says it is currently sounding out potential customers for the keylogger-proof keyboard in the Igel user base, bearing in mind that the 8-bit chip that controls conventional keyboards must be replaced by a more powerful 32-bit one to handle the encryption, resulting in a price increase of around 30% vis-a-vis standard keyboards.

While the project is still at this tentative stage, Cherry says it foresees taking the security capability still further at a later date. This will entail encrypting the data all the way from the keyboard to the thin client server, without decrypting it in the endpoint at all, and will mean the code that triggers the process will then reside on the server.

Contextual awareness comes to Igel thin clients

Another Igel partner, deviceTRUST GmbH, has added contextual awareness to Igel's products. This means the Igel system can now identify the hardware used and any software that has been loaded onto it, as well as determining the device's location (e.g., on or off the corporate network), its geolocation, and whether any wireless connection the traffic is traversing is secure (i.e., whether it encrypts).

This capability relies on some of deviceTRUST's code residing on the thin client server and an agent that is integrated into Igel OS. Information on the endpoint device's context is then relayed from the agent so that the server can take appropriate action, such as restricting what data can be accessed if a Wi-Fi connection is insecure, for instance.

Appendix

Further reading

On the Radar: IGEL enables secure thin client use anywhere, IT0022-000991 (May 2017)

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum
TMT intelligence | informa

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo