Enguild

Security Solutions

MagNOS Secure Client System

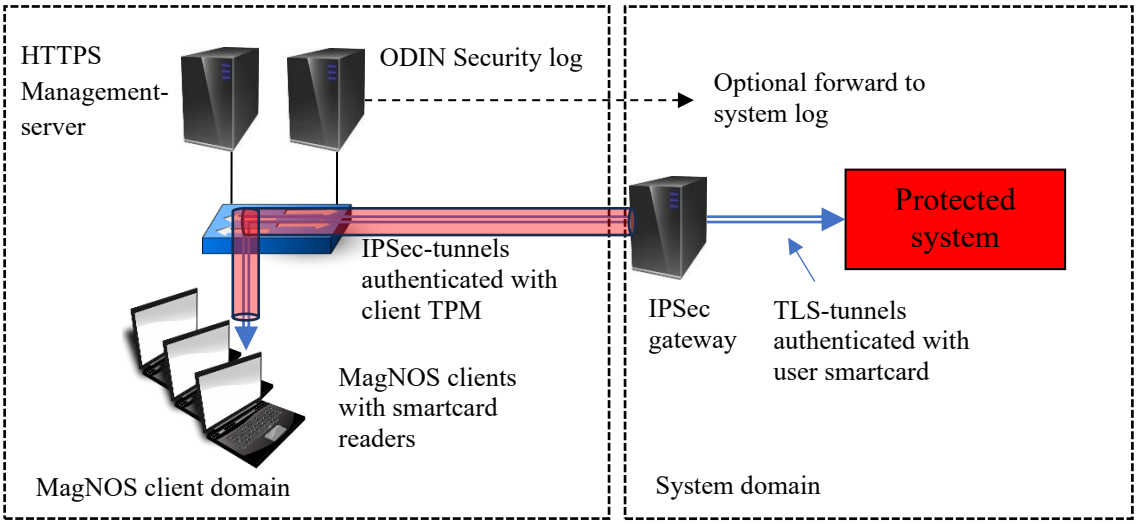
Product Information

Key Features

- Built on a minimized and hardened (according to military standards) Linux-based platform, the same base as used in the proven solution ODIN Security Log but completely stripped of all unnecessary packages
- Running in a diskless computer, i.e. no part of MagNOS is stored on the client in any form to protect it from manipulation. The image is only executed in volatile memory on the client.
- Secure boot via a certificate authenticated HTTPS-server for maximal integrity of boot-image
- Optional boot from a write protected encrypted USB-memory which is carried by the user
- No access to ANY protected system resources (not even authentication channels) without the use of a smartcard or other PKCS#11 compatible token.
- The token is used to set up encrypted TCP-tunnels, thus fulfilling strong authentication of a user
- Provides only a software client window such as RDP, VNC, BLAST, etc. towards a node in the protected system. The customer can define which protocols and clients are needed for the specific solution.
- Single-Sign-On. Note: Not compatible with all tokens
- Security logging and boot-image integrity in real-time provided by ODIN Security Log as part of the complete solution
- Optional IPSec tunnel towards a gateway in the protected system. This tunnel is authenticated with the TPM-module in the hardware, thus enforcing client authentication on top of strong user authentication.
- Optional 802.1X and MACSec network authentication/encryption
- All configuration and management is performed on a central server. Configuration of a client doesn't even require it to be powered on. The individual configurations are protected by each client's TPM-module key.
- Fully configurable monitor setup with up to 4 monitors
- Whitelisting of all USB-devices that are attached to the client
- Support for sound devices forwarded from the client to the protected system
- Compatible with PKCS#11-compatible COTS tokens
    - Tested with different Thales NATO-used smartcards
    - Tested with OpenSC-compatible smartcards such as Aventra MyEID.
    - Tested with Yubikey tokens
- Optional integration of KrAPI for use of Swedish TAK/TEID smartcards
- Optional support for password based authentication with limitations in assurance level of the security functions.
- Hardware manufactured/modified by ISO 9000 / 17025 certified companies
- Available with SDIP 55 certificate for NATO/EU Tempest compliance

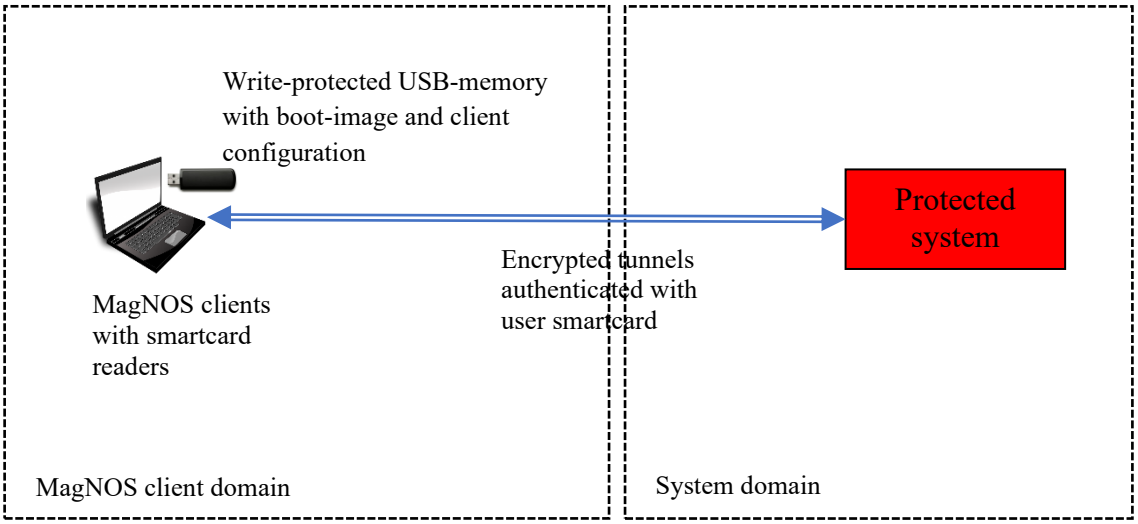
System context

The system is built with a management-server (SSC-server), any number of MagNOS clients and a security log (ODIN Security Log) for security logging and system integrity control of the nodes in the MagNOS domain.



The management-server can synchronize data with other management-servers using TLS-tunnels over a WAN to allow for central management of several client sites.

For smaller installations (Point-to-Point to the real client), it is possible to use the MagNOS client without a log server and boot the image from a write-protected, optionally encrypted, USB-memory which can be carried by the user.



Security

All connections from the client towards the protected system are protected by TLS. By default an IPSec tunnel is also created that encapsulates all traffic from the client to prevent anything from leaking. TLS-tunnels are authenticated with the user's token certificate and validated against installed CA/CRL.

By default, no USB-support is active in the client but the administrator can control this from the management-server and enable specific devices and allow mass-storage, sound-devices etc. This is enforced both in the client's executing operating system AND the forwarding protocol to the protected system. This gives the protected system a very high assurance level with regard to illegal data import/export. In short, this means that no matter which client or other device a possible attacker use to connect to the system, nothing will be accessible unless the attacker has a valid token with the correct PIN-code. The outer IPSec-tunnel with its TPM-module that has been intitiated on a secure network before using the client in production guarantees that only authorized hardware can be used for communication with the protected system. The integrity of the network booted operating system is guaranteed by authenticating the management-server using pre-staged certificates and TLS-tunnels as well as the special customized secure hardware from Amulet Hotkey that are used as client endpoints.

The included ODIN security log can optionally forward logs to a customer system log server compatible with the Syslog-protocol.

The MagNOS hardware is a preconfigured Amulet Hotkey diskless computer in which the only persistent media is the UEFI/BIOS-firmware settings storage and TPM-module. The UEFI configuration is to boot via HTTPS and the customer must load their own certificates to the bootloader during a staging phase of the client before it is installed on the production network. The MagNOS clients can be delivered in versions compliant with TEMPEST Level A or B according to the signal protection requirements of the installation.

Comparison with other client technologies, e.g. “zero-clients”

There are mainly two other technologies used for thin/zero-clients:

1. A slimmed and hardened (to some level) operating system installed on a persistent disk with some clients for remote access such as VNC, RDP, Citrix, etc.
2. A firmware based solution (no persistent disk) often based on the PCoIP-protocol which in effect forwards the video card output and USB-bus to the Zero-Client. This protocol is as of 2025 not maintained anymore and thus not an option.

Technology number 1 suffers from the problem with an internal persistent media that can be manipulated and often inadequate hardening of the operating system. It is also often not an option to use a smartcard for authentication since not all installed clients support it which means that strong authentication of the user is not possible. Note that even if the operating system is installed as “read-only” manipulation is possible if an attacker has physical access since there must be some method for updating the operating system, thus proving that the media is not really “read-only”.

Technology number 2 solves the problem with the internal disk since it is a firmware based solution but has the drawback of forwarding the entire USB-bus which opens a number of attack vectors that can be used. Many such installations suffer from configurations vulnerabilities that makes it possible to create a network to the protected system via the USB-bus and thus bridge the protected system to the attacker without authentication. Hardening a USB-bus-access is very difficult and new technologies means that new vulnerabilities may appear when upgrading the protected system. It has also proven difficult to use some smartcard types in these solutions. The software based solutions for PCoIP suffers from even more severe vulnerabilities that may allow unauthenticated attackers to gain access to the protected system. The PCoIP-protocol is not maintained anymore so it is really not an option.

Even if a new “firmware”-based solution will be presented on the market it is very often just a slimmed real operating system installed on a persistent media with some software based “read-only” flags set. The assurance level of such solutions are always questionable for high security environments. The term “firmware” is often misused in security products. MagNOS on the other hand has nothing of its operating stored on the client but instead relies on the security of the TPM-module, which has a proven high assurance level, to load the operating system in a secure manner from a remote server that is physically protected.

Our solution has the following pros compared to oher techonologies:

- Built on a Linux OS => maintainable and future proof
- Using standard Intel-based HW, no special chips => future proof
- Can run ANY type of software display client compatible with RedHat Linux
- ”Bolt-on security”, i.e. you can use your server/virtual infrastructure as-is and just introduce this client system on-top
- Both client (hardware) and user authentication based on a PKI
- Both layer 2 and layer 3 encryption to avoid any data leak in side channels and strong encryption of all traffic
- Compatible with several of the major smartcards used in NATO
- Everything is maintained on a central server, no need to configure individual clients anywhere else
- Scalable to multi-sites by inter-connecting the management-/boot-servers

Licensing and Price

For more information, please contact:

Enguild Security Solutions AB
Phone: +46 708 233 933
Email: info@enguild.com