

## Provaia Appliance

The Provaia Appliance boots directly from a live CD. When finished it provides the user with an encapsulated interface (kiosk terminal) – combining ease of use and maximum protection against tampering with the system.

Moreover the main stronghold of a live CD is that it guarantees a trustworthy environment for analyzing mobile media. Also there is no secret data stored on the Provaia Appliance.

Depending upon the scenario chosen, up-to-date antivirus signatures can be updated over the Internet (live update), from a server within the local network or manually – using removable storage devices.

- Ease of use
- High user acceptance
- Perfect process integration
- Very high security level

## And additionally ...

... we are of course glad to be of service:

- Integration of Provaia into your existing infrastructure
- Individual customization and connectors to additional security services
- Helpline, maintenance and support
- Update service with quality-assured updates
- Support for your IT security management
- Assistance with creating or improving your Incident Response capabilities

## Contact



**PRESENSE** Technologies GmbH

Sachsenstraße 5

20097 Hamburg

Germany

Tel.: +49-40 -2442 407 -0

Fax: +49-40 -2442 407 -24

[www.pre-sense.de/provaia](http://www.pre-sense.de/provaia)

[provaia@pre-sense.de](mailto:provaia@pre-sense.de)



# Provaia

Perimeter Security for Mobile Media



The Provaia Appliance marks the arrival of a new security product. It finally addresses the large majority of the most recent risks concerned with the exchange of data over mobile media such as USB keys, flash cards etc.

## Firewall for Mobile Media

In today's networks borders are already secured by Perimeter Security such as packet filters. But exchanging data via mobile media involves high risks for your corporate IT networks. Almost always only an antivirus scanner at the end user's workstation is trying to keep malware from mobile media at bay.



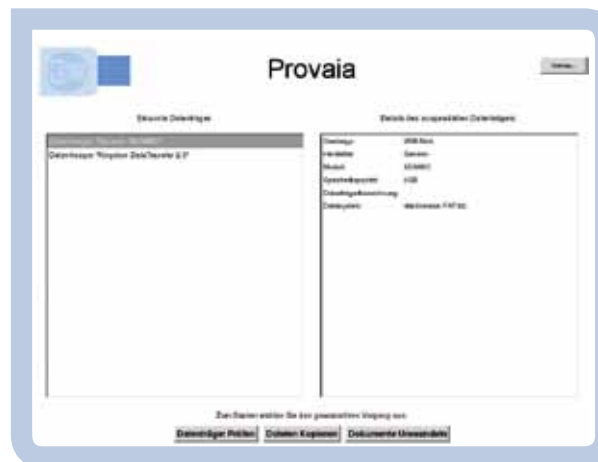
Mobile media and manipulated documents are current attack vectors. This is exactly where standard security measures meet their limits. It was shown for the first time by the collateral damage inflicted by „Conficker“. With „Stuxnet“ – which experts consider a cyber weapon – even cascading effects are possible. Stuxnet can completely paralyze critical infrastructures. It therefore is irresponsible for sensitive environments to perform data transfers without perimeter security. Security measures at the endpoint computer are not sufficient – especially when thinking about future attack vectors.

For securing an Internet connection firewalls are being put into place – not without a reason.

## Approaching a Solution

Provaia provides a „firewall“ for mobile media. Its features include:

- Scanning devices with at least two different antivirus products for malicious code - also inside of TrueCrypt containers of course
- Recognition – and if desired deactivation – of AutoRun and AutoPlay functions
- Recognition – and if desired removal – of potentially harmful files
- Removal of active and invisible content in documents. Conversion from commonly used file formats into open formats (ODF, PDF or PDF/A)
- Import and export for scanned/converted files from and to portable devices or network drives
- Secure deletion of mobile media
- Support for crypto USB flash drives, e.g. SafeStick



## Provaia Management



The Provaia Management System can either be supplied as rackmount appliance or as managed service. Administration is easily accomplished through a web browser. The Provaia MS offers a great variety of possible configurations to optimally adapt the Appliance to your organization's security needs:

- Individual customization for your infrastructure
- Management of any number of appliances
- Reporting, logging and quarantine functions
- Integration with IT security management
- Interaction with additional Security Systems

Finally, the live CD needed for the operation of Provaia can be newly generated in the Provaia MS at any time.