ZeeTerm endpoint solution: VDI & DaaS endpoint security done right

At ZeeTim, security by design is a key pillar in everything that we do. Aspiring to achieve the most secure cloud endpoint is what drove us to developing our endpoint solution ZeeTerm, comprised of the operating system ZeeOS and the management console ZeeConf.

Whether your ZeeTerm runs on our hardware, or is a PC that you repurposed using ZeeTransformer, the security standards will be exactly the same.

Beyond regular and well-known security reinforcements that a Thin or Zero client Operating System brings to an endpoint infrastructure, ZeeTim's endpoint offering stands out in terms of security.

Here is why.

No action can be done locally by anyone

- Read-only operating system, no possible action on the thin client from anyone
- No local configuration allowed for anyone
- User can only launch a program that is allowed: if users download some binaries from the internet, these binaries will not execute
- No data can be downloaded or stored locally

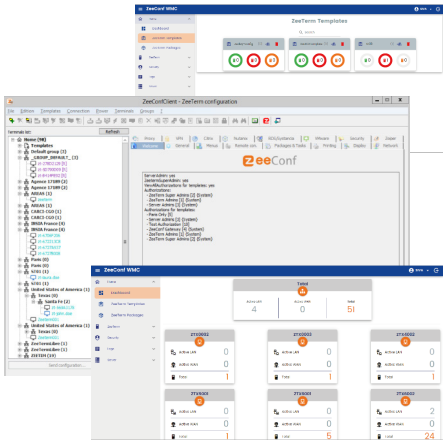
A powerful and patented operating system

- Linux based OS
- Hardened operating system with patented structure: each application package runs in its dedicated sandbox rather than in a single file. Therefore updates can be done in a very granular way, reducing potential attack surface during upate process.
- No need for antivirus

All communications are encrypted

- Client – Server connection is secure via HTTPS
- Connection to endpoint is ensured via SSH by default, one of the most robust security protocols on the market today, secured by a pair of certificates and cypher keys. There is no other way to connect to a ZeeTim endpoint out if this connection flow secured with SSH. This architecture prevents most network attacks such as "Bagle malware"
- All of our VNC communications are encrypted with SSH, so no need to use Teamviewer to access an endpoint, the communication is already 100% secure
- PXE deployment and update / upgrade is possible via the Internet, no need to use low-level protocols made for LAN such as DHCP or TFTP

A management console to manage endpoint security centrally, with action accountability



- On Premise management console to avoid any attack coming from the cloud
- The server part of the management console acts like a trust base, checking the package list on the operating system at frequent intervals and automatically replacing suspicious files when detected. Role-based administration with two levels of admin access
- Admin Authentication based on Active Directory
- Possibility to choose the settings that an admin can access, the ZeeTerm or group of ZeeTerms that can be managed, based on Active Directory security groups
- Accountability of admin actions with possibility to record and check who did what, when and on what endpoints
- Reporting options with graphs, featuring endpoints status and key information for admins
- With home office becoming the norm these days, ZeeTim ensures secure BYOD thanks to USB drive-based solution ZeeTransformer
- Native support of VPN protocols such as Cisco Anyconnect, Open VPN, wireguard
- Secure management of remote endpoints thanks to ZeeGateway

Hardware security

- Ability to disable USB devices
- Physical security - We provide Kensington lock on devices

Last but not least, ZeeTim adresses security with other tools including:

ZeeOTP

Multi Factor Authentication built for VDI first

ZeeKey

USB Credentials Vault for quick access & disconnection to virtual workspaces on ZeeOS and Windows based endpoints

ZeePrint

Print optimization technology which compresses, speeds up & secures printing flows