ZeeTim endpoint solution: Endpoint security done right

Security Architecture and Technical Foundations

At ZeeTim, security is a fundamental principle that guides every stage of our product development. Our ambition to deliver one of the most secure endpoint operating systems on the market is what led us to create ZeeOS and its Web Management Console.

While thin and zero client operating systems already offer clear security advantages compared to traditional desktop OS environments, our approach goes significantly further. ZeeOS introduces architectural reinforcements, strict control mechanisms and an infrastructure designed to minimize risk across the entire endpoint lifecycle.

This document outlines the core elements that make ZeeOS a highly secure and reliable endpoint solution.

1. Hardening the Endpoint Operating Environment

ZeeOS has been designed from the ground up to prevent local attack vectors and ensure that endpoints remain tamper resistant.

- Read only operating system with immutable partitions.
- No local data storage and no ability for users or apps to write files.
- No local configuration changes permitted at the endpoint.
- No local authentication (LDAP, …) client stored on the device.
- Strict application whitelisting. Only approved binaries can run and downloaded executables cannot be launched.
- Patented modular architecture where each application package runs in an isolated sandbox, reducing risk during updates and making patches more granular.
- Structural mitigation of local threats including malware installation, tampering and persistence.

2. Robust and Encrypted Communication Architecture

ZeeOS relies on a robust connection architecture designed to ensure confidentiality, integrity and strong endpoint validation.

- Client to server communication secured with HTTPS.
- Endpoint access restricted to SSH operations secured with certificate pairs and encryption keys.
- All remote assistance sessions, including VNC, fully encrypted through SSH.
- No dependency on legacy LAN protocols for deployment. PXE installations and updates can be performed securely.
- Reduced exposure to common network level attacks such as session hijacking or protocol spoofing.

3. Centralized Control and Integrity Assurance

The Web Management Console acts as the trust anchor that validates, supervises and secures each endpoint.

- Secure and verify deployment of updates.
- Continuous integrity monitoring. The WMC checks package lists on endpoints and automatically replaces altered files.
- Log collection and performance monitoring with export to SIEM platforms.
- Multi-level role-based administration integrated with Active Directory authentication possible.
- Full RBAC and granular permission assignment that can be based on Active Directory groups.
- Detailed accountability of activities securely logged in an immutable manner, in accordance with security standards (RGPD, ISO/IEC 27001, NIS/NIS2 …).
- Visual reporting with status dashboards and key operational metrics.
- Built in support for VPN protocols including Cisco AnyConnect, OpenVPN and WireGuard.
- Secure remote management of offsite endpoints through ZeeGateway.
- USB boot mode for secure BYOD scenarios.
- Secure remote control and troubleshooting with authenticated and encrypted sessions.
- Secure shadowing process using an SSH tunnel, one-time password verification and complete session logging.
- Modular update system reducing package size, deployment time and exposure windows.

4. Powerful add-ons to secure and simplify end user experience

ZeeOS integrates with additional ZeeTim solutions that reinforce identity security, workflow integrity and operational efficiency.

- ZeeOTP for multi factor authentication available in SaaS or on-premise environments.
- ZeeKey for secure credential storage and fast user switching in virtual desktop scenarios.
- ZeePrint for optimized end encrypted print operations with reduced bandwidth usage and stabilized print servers.
- ZeeScan for secure, seamless document scanning within remote workspace sessions.

ZeeOS delivers a hardened and controlled endpoint environment designed to reduce risk at every stage of the device lifecycle. Its read only architecture, secure communication model and centralized integrity enforcement create a platform that is both robust and predictable. Combined with advanced management capabilities and complementary security tools, ZeeOS provides organizations with a reliable foundation for securing modern digital workspaces whether on site, remote or in hybrid environments. Learn more on www.zeetim.com.