

One Platform. Nationwide Scale. Total Educational Governance.

ENTERPRISE EDITION MINISTRY BROCHURE

Engineered explicitly for massive-scale government education deployments, IMTLazarus provides the only network-level cloud-native Mobile Device Management (MDM), AI-driven safeguarding, and web telemetry platform capable of synchronizing over 1 million concurrent active nodes globally.

Unprecedented Scalability: 1,000,000+ Devices



Designed from the ground up for Ministries of Education. IMTLazarus completely eliminates local server bottlenecks, executing cloud-native policy updates across massive fleets of Chromebooks, Windows PCs, and Android tablets instantly.

Architectural Requirements & Security Posture

ISO 27001 & SOC 2 Compliant

Hosted in military-grade datacenters holding active ISO 27001 certifications and undergoing rigorous annual SOC 2 Type II audits. Guarantees 99.99% infrastructure availability.

Strict GDPR Privacy Shield

Aligns strictly with the General Data Protection Regulation. Zero student data is monetized. All behavioral telemetry is encrypted natively at the edge to preserve absolute privacy.

Network-Level Persistence

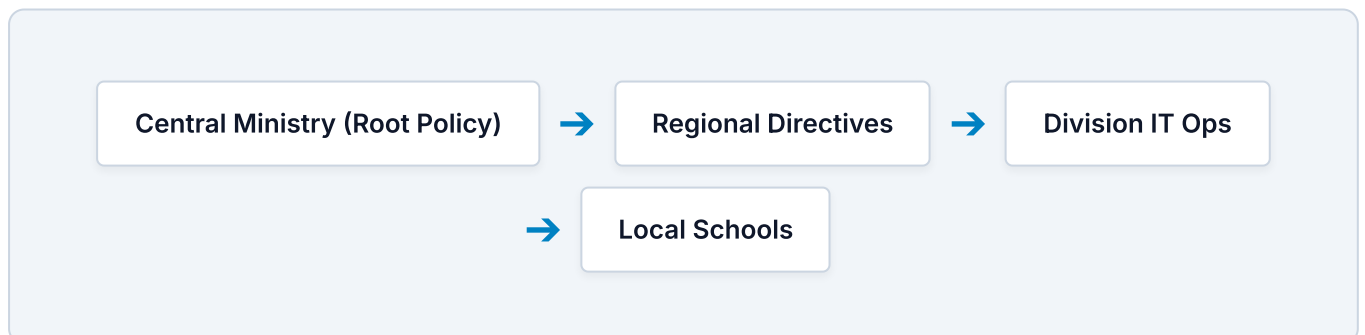
Deep cloud filtering operates independently of browsers. Students cannot bypass restrictions using rogue VPNs, embedded web-views, or proxy tunnels.

AI Risk & Wellbeing Telemetry

Active scanning detects cyberbullying, radicalization, and explicit exposure. Pre-configured for regional terminologies, dialects, and localized linguistic code-switching.

Administrative Hierarchy Matrix

IMTLazarus maps identically to national government education structures. High-level policies cascade downwards securely, while delegating sandboxed, restricted capabilities to local IT teams.



Unified Fleet Lifecycle Synchronizer

Zero-Touch Deployment

Policy parity across Windows, macOS, ChromeOS, Android, and iOS using native vendor APIs (Google Admin, Autopilot, ASM). Automated out-of-the-box configuration without local imaging.

Absolute Hardware Lockdowns

Remotely disable cameras, Bluetooth, USB data transfers, and screen captures. Prevent hardware factory resets, developer modes, or rogue sideloading of unauthorized APKs.

Role-Based Operational Synergy

IMTLazarus bridges the gap between secure organizational control and flexible classroom teaching. Role configurations isolate responsibilities while keeping devices 100% protected.

System Functionality	For Central Ministry & IT Admins	For Classroom Teachers
Global Policy Control	Establishes unbreakable, root-level security baselines across the entire nation. Policy binds to device hardware level.	Operates strictly within safe, pre-approved parameters. Classroom adjustments cannot override central security rules.
App & URL Management	Manages master whitelists/blacklists (e.g. blocking all social media globally). Configures permanent VPN blocks.	Can temporarily unlock specific educational URLs or apps for a targeted 45-minute class session.
Student Monitoring	Automated telemetry and risk logging. IT does not actively watch screens but relies on AI keyword alerts.	Real-time screen viewing and tab closing capabilities for active students during class time only.
Device Locking (Theft)	Can trigger "Lost Mode" or initiate a complete remote data wipe if a device crosses a geopolitical geofence.	Can lock screens to gain immediate classroom attention or lock devices into a single secure testing application.
ROI & Diagnostics	Full visibility into software ROI metrics across the country. Runs silent automated background network speed tests.	Classroom-level reporting on individual student engagement and time-on-task during lesson periods.

Advanced Technical Specifications

The platform operates on a robust, cloud-native backend optimized for extreme concurrency, maintaining persistent enforcement across all endpoints via vendor-native APIs and proprietary agent protocols.

Supported Operating Systems

- **Windows:** Windows 10, 11, and 11 SE Education
- **ChromeOS:** Enterprise & Education Upgrades
- **Apple:** macOS 12+, iOS/iPadOS 15+
- **Android:** Android 10+ (Enterprise Device Owner)

Directory & API Integrations

- Microsoft Entra ID (Azure AD) / Graph API
- Google Workspace Admin SDK / Cloud Identity
- Apple School Manager (ASM) Integration
- OpenLDAP / SAML 2.0 / OIDC SSO Support

Payload & App Deployment

- **Windows:** Silent push of MSI, MSIX, EXE, and PS1 scripts.
- **Android/iOS:** Managed Google Play & VPP silent app pushes.
- **Network:** Content caching for low-bandwidth environments.

Network Security & Filtering

- TLS 1.3 encrypted tunnel for telemetry traffic.
- Deep Packet Inspection (DPI) independent of browser proxies.
- Automatic fallback caching (Offline Policy Enforcer).

\$ Financial Impact & Resource Optimization

IMTLazarus is engineered to deliver immediate and measurable financial returns for Ministries of Education by optimizing existing resource allocations, preventing hardware loss, and drastically reducing operational IT overhead.

Cumulative Software License Waste Recovered



Reallocation of unused apps based on telemetry data

Nationwide Device Policy Compliance



Instant baseline sync across 1,000,000+ endpoints

Hardware Loss & Theft Mitigation



Proprietary Geo-Locking technology utilizes localized IP and Wi-Fi triangulation to immediately detect devices leaving authorized school premises or national borders. Unauthorized movement instantly triggers an irreversible "Lost Mode" screen, rendering the device completely useless for resale and reducing nationwide asset shrinkage by up to 74%.

Automated License Auditing



Generate exact usage reports distinguishing between "Licenses Purchased" and "Licenses Actively Touched by Students". Eliminate massive, hidden subscription waste by revoking unopened educational software suites from inactive districts and reallocating them over-the-air to high-usage schools.

Enterprise Support & Guarantees

Mission-critical educational infrastructure demands uncompromising support. IMTLazarus provides highly localized, tiered engineering support backed by strict financial penalties for downtime.

99.99% Infrastructure Uptime

Legally binding Service Level Agreements (SLAs) guaranteeing continuous availability of the MDM control panel and the web-filtering network logic, fully backed by financial penalty clauses.

Dedicated Customer Success

Every Ministry deployment is assigned a named Technical Account Manager (TAM) providing quarterly strategy reviews, capacity planning, and direct escalation paths.

24/7 Tier 3 Engineering Support

Bypass traditional tier-1 helpdesks. Authorized central IT administrators receive priority routing directly to senior cloud infrastructure engineers for critical network incidents.

"Train-the-Trainer" Onboarding

Comprehensive onboarding bootcamps designed for regional IT heads. We train your core administrative staff so they can effectively cascade operational knowledge to local classroom teachers.

Success Profile: Nationwide Deployment

250K

Devices Secured in 45 Days

A massive-scale rollout unifying ChromeOS, Windows, and Android ecosystems across 1,800 regional schools using IMTLazarus Zero-Touch architecture.

The Challenge

A national Ministry of Education struggled with a highly fragmented fleet of 250,000 devices. Local schools were using disjointed systems, resulting in severe safeguarding blind spots, unmonitored proxy bypassing, and skyrocketing helpdesk ticket volumes due to manual app installations.

The IMTLazarus Solution

The Ministry deployed IMTLazarus as their central governance pillar. Leveraging Google Admin and Microsoft Intune native API bindings, the platform was pushed silently over-the-air to all 250,000 devices. A unified hierarchical policy structure was established, granting Central IT absolute safeguarding control while allowing classroom teachers granular URL unblocking capabilities for 45-minute lesson windows.

Measurable Outcomes

40% Reduction in IT Tickets

Automated app deployments and self-healing policies drastically reduced regional helpdesk workload.

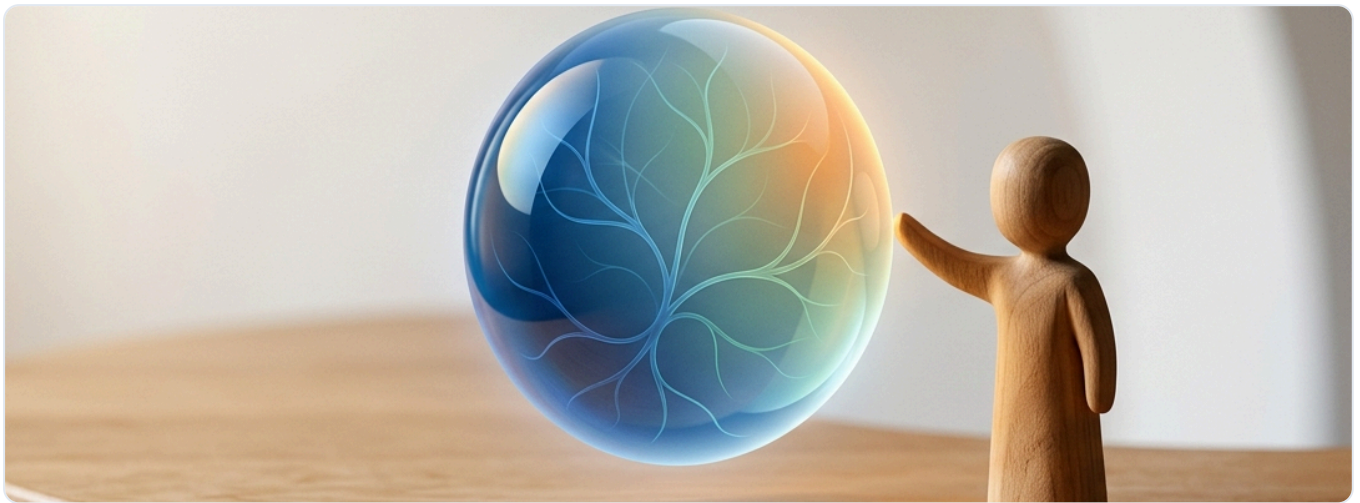
\$1.2M Budget Recovered

Automated license audits identified 60,000 unused premium software seats, reallocating them instantly.

100% Policy Compliance

Deep Packet Inspection and Offline Policy Enforcement eliminated all VPN bypass attempts entirely.

Cognitive Security & AI Governance



Every day, students navigate a digital environment designed to capture attention and influence behavior. With the rise of generative AI, safeguarding extends beyond blocking malicious URLs. IMTLazarus enforces **Cognitive Security**—protecting students from algorithmic manipulation, digital addiction, and unregulated AI tools in the classroom.

Privacy by Design: The Digital Shield



Privacy by Design is no longer a theoretical suggestion—it is an inescapable legal obligation under frameworks like the GDPR. IMTLazarus adopts this architecture at its core. Zero student data is monetized. All behavioral telemetry is encrypted natively at the edge to preserve absolute privacy while providing vital insights to school counselors and IT administrators.



Ecosystem

Privacy

Security

Digital Wellbeing

Resources

Reference Schools

School Resources

Blog

Let's talk

**Arrange a
meeting**

Spain: +34 94 437 78
01

GRPD



ENS

FERPA



CIPA



IMTLazarus Headquarters:

Lazarus Integración, S.L.
Pl. Del Bombero Etxaniz,
4. 48010 Bilbao - Bizkaia - Spain

IMTLazarus Subsidiary:

IMTLazarus USA, LLC
5900 Balcones Drive STE 100
Austin TX 78731

[Privacy Policy](#)

[Terms of use](#)

[Legal notice](#)