the cloud group | iSHIELD

CASE STUDY
MINING NETWORK SECURITY

Deep underground. Fully secured.

How Cloud Group's iShield Unified Threat Management Device secures remote mine sites, contractors and operational technology networks

The challenge

Mining operations and resource extraction groups function in demanding, harsh environments across vast geographical footprints. A single enterprise typically relies on a complex web of interconnected infrastructure linking remote extraction sites, processing plants, regional depots and corporate headquarters. Managing communication across these multi-site operations requires **absolute perimeter security** for industrial networks while maintaining reliable connectivity for contractors, engineers and staff.

Heavy industry faces an escalating wave of **sophisticated cyber threats** from international espionage rings and ransomware syndicates. Locally, South African mining houses have targeted network intrusions aimed at exfiltrating proprietary surveying data, commercial tender documents and payroll databases. These high-stakes threats place intense operational and compliance pressures on mining executives to safeguard critical **operational technology (OT)** and corporate data networks under **POPIA** frameworks.

Operationally, remote mine sites are plagued by **connectivity vulnerabilities.** Relying on isolated primary links in rural areas means that network outages can instantly halt core operations, cutting off real-time telemetry from underground equipment, interrupting weighbridge applications and freezing supply chain systems. Furthermore, mining environments host a constant influx of external contractors who require internet access. Without strict segmentation, allowing these third-party devices onto the primary network introduces massive liabilities, as a single infected contractor laptop could serve as a **beachhead** to migrate laterally into critical industrial systems.

"A single infected contractor laptop could become a beachhead for malware to migrate laterally into critical operational systems."

The solution

iSHIELD DEPLOYMENT

Cloud Group works closely with its extensive network of IT professionals and resellers to deploy iShield—a next-generation Smart Access Unified Threat Management Device—across the industrial and mining sectors. These highly scalable deployments are engineered to withstand the logistical challenges of remote industrial environments, cleanly uniting deep-level mining operations and surface facilities under a unified security architecture.

Partners receive comprehensive training, certification and remote technical assistance to execute seamless, phased installations designed around strict operational windows, ensuring limited disruption to live production lines, safety tracking or logistics systems. iShield combines robust on-premises hardware control with a centralised cloud-based management platform, giving mining operators absolute command over their operational boundaries.

KEY FEATURES IMPLEMENTED (VIA PARTNER-LED DEPLOYMENTS)

- **Secure guest and contractor perimeters:** Deploying controlled captive portals utilising strict session lifetime limits to grant temporary, isolated internet access to visiting engineers and contractors, keeping them entirely separate from core mine systems.
- **Multi-site WireGuard VPN architecture:** Interconnecting geographically dispersed mine shafts, processing facilities, regional depots and corporate headquarters via high-speed, heavily encrypted site-to-site WireGuard VPN tunnels to ensure seamless, real-time data syncs.
- **Agile remote firewall management:** Empowering IT partners and central corporate administrators to monitor and assign a DynDNS for remote access to firewalls across all remote sites via a single cloud dashboard, virtually eliminating the need for expensive and time-consuming physical technician callouts to remote operations.
- **Automated link failover for continuous production:** Provisioning redundant dual-WAN connections to guarantee that if a primary satellite or fibre link drops, the system instantly and transparently switches to a backup cellular or microwave connection, keeping telemetry and safety systems online.
- **Strict operational technology (OT) isolation:** Utilising advanced VLAN and network segmentation to cleanly separate public-facing guest access from administrative networks and critical industrial control systems (ICS/SCADA), preventing lateral threat migration.
- **Intelligent industrial traffic shaping:** Implementing strict bandwidth rules that automatically prioritise mission-critical communication channels, safety monitoring systems and ERP links over recreational browsing in staff living quarters.

The results

OUTCOMES & NEXT STEPS

01
Flawless multi-site network integration: Encrypted site-to-site WireGuard tunnels maintain rapid, secure communication across all national operations, allowing on-demand updates to production counts, safety metrics and shipping logistics without latency.

02
Drastically reduced operational overhead: Centralised cloud management allows IT partners to resolve local network bottlenecks, adjust firewall policies and troubleshoot issues completely remotely, minimising costly on-site technical callouts to remote branch locations.

03
Uninterrupted operational continuity: Automated link failover protects remote extraction sites from localised internet outages, keeping automated machinery tracking, weighbridges and logistics platforms online and operational 24/7.

04
Assured guest and contractor security: Clean network separation mitigates the possibility of an infected contractor's device influencing the core mining database, operation infrastructure and corporate network.

05
Controlled and fair-use access: Captive portal session limits give mine managers the power to regulate network usage in common areas and staff camps fairly, naturally mitigating long-term network drainage while ensuring baseline connectivity for guests.

06
Streamlined compliance and robust audit trails: Structured identity logging, secure network segmentation and robust access rules provide seamless alignment with POPIA and critical industrial safety data standards, shielding the mining group from data liability.

For an MSP, servicing remote mining clients in rural areas is usually a major drain on profitability. iShield changed the economics: we deployed an encrypted WireGuard mesh across all their shafts, automated link failover keeps telemetry online, and a centralised dashboard lets us manage everything remotely—virtually wiping out emergency callouts.

— Cloud Group IT Partner & Industrial Enterprise Infrastructure Specialist

Ready to secure your mining network?

Contact Cloud Group to learn more about our partner programme or to book a demo.

www.cloudgroup.net
010 593 4493
sales@cloudgroup.net