Sentinel Node Security Solutions

Comprehensive Business Plan: Anti-Duress AI for Remote Enterprise IT in South Africa

1. Executive Summary

In the evolving landscape of remote work, High-Privilege IT workers (System Administrators, DevOps, Security Engineers) have become high-value targets for physical extortion and home invasions, particularly in South Africa. **Sentinel Node Security Solutions** provides an innovative hardware and software ecosystem designed to protect both the employee and the enterprise from duress-based cyberattacks.

By utilizing local, AI-driven visual monitoring (facing the user and the office entrance), the system automatically detects unauthorized physical presences in the workspace. Upon detecting an anomaly (e.g., an intruder forcing the employee to access systems), the protocol instantly revokes corporate access, neutralizes the compromised endpoint, and dispatches private armed response units, ensuring the safety of personnel and the protection of critical enterprise data.

2. Problem Statement & Deep Reasoning Context

South Africa faces a unique intersection of high physical crime rates and advanced corporate IT infrastructure. Traditional cybersecurity focuses entirely on digital perimeter defense (Firewalls, MFA, Zero Trust), assuming the endpoint user is acting freely.

- **The Vulnerability:** An IT administrator with access to Active Directory, payment gateways, or customer databases working from home is a walking backdoor. Threat actors recognize that bypassing MFA is easiest when using physical force against the authorized user.
- **The Risk:** Theft of proprietary business plans, exfiltration of highly sensitive PII and PCI-DSS data (credit cards, CVV), or the deployment of ransomware via trusted SSH keys.
- **The Gap:** Standard panic buttons require manual activation, which is impossible under direct gunpoint or physical threat. A fully automated, zero-touch duress detection system is required.

3. The Proposed Solution: Core Architecture

The solution is an integrated appliance combining edge-AI hardware, Identity and Access Management (IAM) API hooks, and physical security dispatch.

3.1. Hardware & AI Detection

The physical setup consists of two wide-angle, 1080p edge-AI cameras positioned strategically:

- **Camera 1 (Entry Focus):** Monitors the door/entrance to the home office.
- **Camera 2 (Workspace Focus):** Monitors the area immediately surrounding the employee.

The AI model utilizes advanced Computer Vision (YOLOv8 + Facial Recognition) running locally on an edge device to ensure zero video latency and maximum privacy (no video leaves the house unless an incident occurs). The AI continuously counts persons in the room. If *Count > 1* or an *Unrecognized Face* is detected, the Duress Protocol triggers.

3.2. Automated Duress Protocol (The "Kill Switch")

Once a threat is visually confirmed by the AI, the system executes a rapid, automated response in milliseconds:

- **Access Revocation:** Immediate API calls to Azure AD / Domain Controllers to suspend the user account.
- **Credential Neutralization:** Revokes active SSH keys and kills active VPN/Zero-Trust sessions.
- **Endpoint Lockdown:** The local machine is isolated from the network, rendering it entirely useless to the threat actors.

3.3. Physical Extraction & Reporting

- **Armed Response Integration:** Silent API trigger to partnered private security firms (e.g., Fidelity ADT, Tracker) dispatching tactical units to the GPS coordinates of the home for extraction and arrest.
- **Evidence Preservation:** The system begins securely streaming encrypted video evidence to an off-site enterprise vault for SAPS (South African Police Service) investigation.
- **Post-Incident Review:** Generates an automated incident report detailing timeline, actions taken, and access logs. Access remains suspended until manual HR/Security clearance is provided.

Deep Reasoning System Logic: To prevent threat actors from simply destroying or unplugging the cameras to gain access, the system operates on a "Dead Man's Switch" principle. If the heartbeat from the local AI device is lost while the employee is logged in, access is immediately throttled or suspended pending secondary verification.

4. Market Analysis & Target Audience

The primary market comprises mid-to-large South African enterprises that handle sensitive data and employ remote IT staff.

- **Financial Sector:** Banks, FinTechs, and Payment Gateways (e.g., Standard Bank, Discovery Bank, Yoco).
- **Telecommunications & Data Centers:** Vodacom, MTN, Teraco (NOC and SOC analysts).
- **Healthcare & Insurance:** Entities storing sensitive PII protected under the POPI Act.

5. Operational & Risk Management Plan

5.1. Handling False Positives

The biggest operational hurdle is family members entering the office space. To mitigate this:

- **Safe Zones & Scheduling:** AI can be trained on household members, allowing brief "safe" interactions (e.g., spouse dropping off coffee).
- **Aggression Analytics:** Integrating pose-estimation AI to detect aggressive stances, raised hands, or weapons, differentiating a family member from an attacker.
- **Warning Buffer:** A 5-second silent countdown on the user's screen requiring a safe-word or PIN stroke if a non-authorized face enters, before the full lockdown initiates.

5.2. Privacy and POPIA Compliance

To adhere to the Protection of Personal Information Act (POPIA) and maintain employee trust, the system guarantees that cameras never record the employee's computer screen. All baseline AI processing occurs on the local edge device. Video is strictly discarded unless a duress event is actively triggered, at which point it becomes legally permissible evidence.

6. Financial Model & Revenue Streams

Revenue Stream	Description	Estimated Pricing (ZAR)
Hardware Appliance (CapEx)	Edge AI module, 2x Cameras, local installation.	R 8,500 once-off per user
SaaS Core License (OpEx)		R 650 / month / user

	API integrations (AD, VPN, IAM) and AI updates.	
Armed Response API Markup	Integration fee with private security networks.	R 350 / month / user

By selling B2B to large enterprises, the cost is easily justified as an insurance policy against multi-million Rand data breaches and immense reputational damage.

7. Conclusion

As the perimeter of the corporate network shifts to the residential homes of its employees, the definition of cybersecurity must expand to include physical duress. Sentinel Node Security Solutions provides the ultimate bridge between physical safety and digital access control. By deploying intelligent, automated lockdown procedures, South African enterprises can protect their most valuable assets: their data, and their people.