the cloud group | iSHIELD

CASE STUDY
CAFE NETWORK SECURITY

The modern café is a micro-office. Secure it like one.

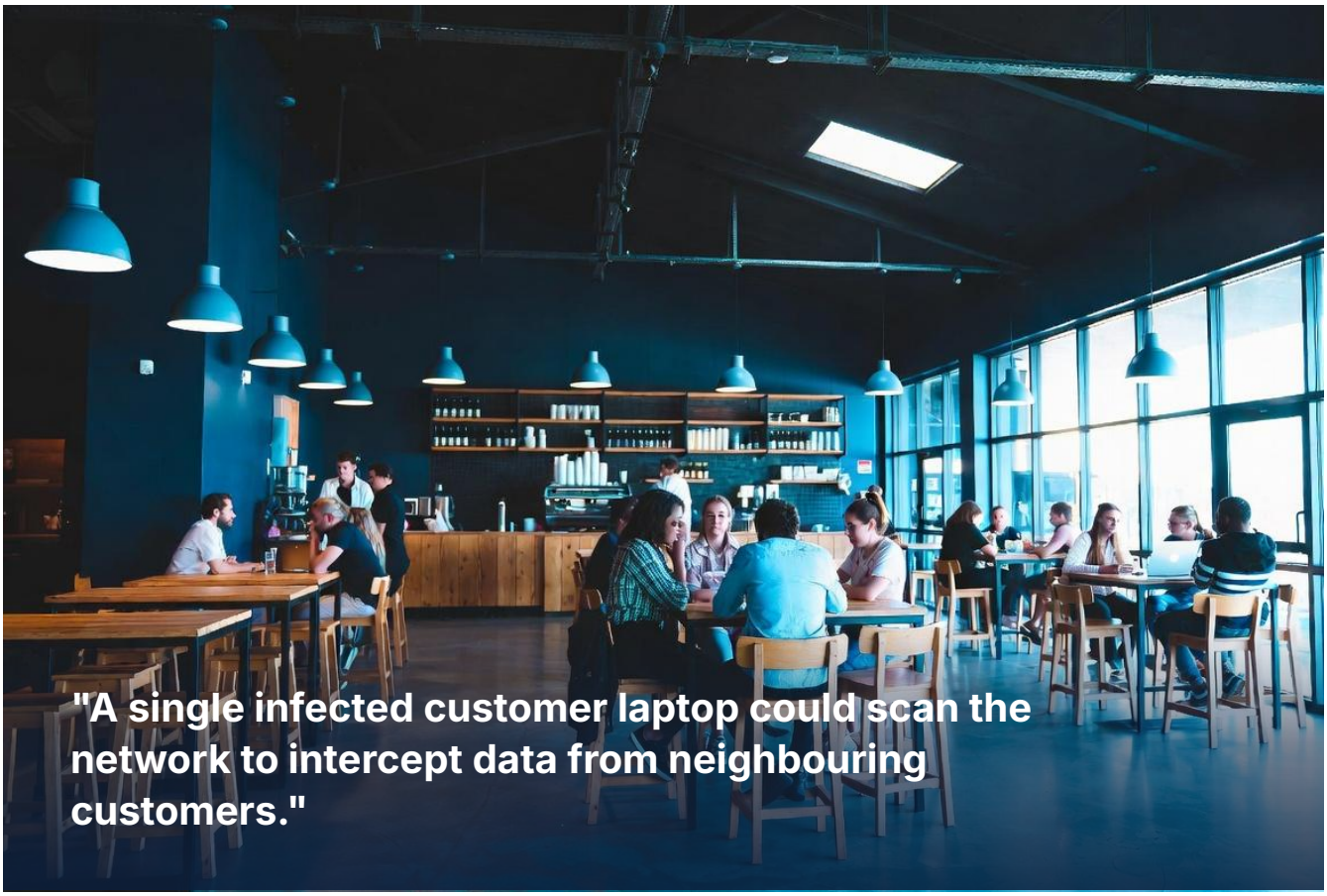
How Cloud Group's iShield Unified Threat Management Device protects payments, patrons and connectivity across coffee shop networks.

The challenge

Modern coffee shops and premium café chains have become **essential remote-working hubs**—high-density micro-offices where a single location must seamlessly accommodate remote professionals, casual diners, POS terminals and IoT-connected kitchen equipment on the same localised footprint.

Globally, the threat was underscored by the growing prevalence of **"DarkHotel"** and public Wi-Fi intercept tactics, where threat actors exploit unmanaged hospitality networks to harvest user data, alongside system intrusions targeting restaurant chains that **compromised thousands of customer records**. Locally, the risk of data leakage remains high under **POPIA**, which mandates strict protection for customer profiles, loyalty details and card transactions.

Operationally, remote workers occupying tables for hours **saturate networks** with video calls, downloads and streaming—starving the business of bandwidth, lagging cloud POS apps, dropping reception lines and disrupting supplier ordering. Without proper isolation, a single infected customer laptop on open Wi-Fi could scan the network to intercept neighbouring data or **compromise the shop's financial backend** .



"A single infected customer laptop could scan the network to intercept data from neighbouring customers."

The solution

iSHIELD DEPLOYMENT

Cloud Group works closely with its extensive partner network of IT professionals and resellers to deploy iShield—a next-generation Smart Access Unified Threat Management Device—across various café environments. Deployments scale dynamically, protecting independent boutique coffee shops up to nationwide café franchises operating high-volume, multi-site branches.

Partners receive comprehensive training, certification and remote technical assistance to deliver quick, non-disruptive installations that integrate cleanly with existing hospitality hardware. iShield combines robust on-premises threat prevention with an agile, cloud-based remote management platform, giving café owners absolute command over their wireless perimeters.

KEY FEATURES IMPLEMENTED (VIA PARTNER-LED DEPLOYMENTS)

- **Dynamic bandwidth throttling:** Aggressive traffic shaping lets guests browse smoothly while automatically throttling individual download speeds, so single users can't saturate the café's primary internet line.
- **Strict tenant network isolation:** Advanced VLAN segmentation cleanly separates public guest Wi-Fi from operational networks, keeping accounting software, staff systems and card terminals hidden from customer view.
- **Captive portal session management:** Standard captive portal authentication regulates public guest connections with automated session lifetime limits—e.g. a 60-minute automated disconnection cycle—to prevent unmanaged network camping.
- **Malicious behaviour and proxy blocking:** Network restrictions block unauthorised proxy/VPN tools and prevent communication between devices on separate networks, limiting lateral movement across the organisation.
- **Automated link failover:** Dual-WAN configurations guarantee that if a primary fibre line drops, the café instantly switches to an alternative LTE/backup connection, so credit card machines never go offline.
- **Centralised multi-branch management:** Franchise owners and IT partners can monitor connection status as well as setup automated email notifications in the event of ISP downtime, along with being able to assign a DynDNS to remotely access and manage each firewall.

The results

OUTCOMES & NEXT STEPS

01 **Protected and predictable operations:** Traffic shaping guarantees that credit card terminals, cloud-ordering apps and administrative systems receive prioritised bandwidth, ensuring instant payment processing even during the busiest trading hours.

02 **Ironclad digital safety for patrons:** Network isolation and threat prevention controls help protect customers from packet interception attempts, credential theft, and malware spreading to the core network

03 **Optimised table turnover and fair use:** Tailored captive portals let owners manage Wi-Fi usage fairly, preventing "bandwidth squatting" while still offering premium wireless access as a customer incentive.

04 **Uninterrupted retail uptime:** Integrated link failover protects the business against local internet outages, ensuring zero lost revenue from failed card payments or interrupted digital orders.

05 **Simplified compliance and oversight:** Structured identity logging and built-in audit trails provide clear visibility, helping café groups align seamlessly with POPIA data handling expectations.

06 **Reduced IT maintenance costs:** The all-in-one hardware and cloud architecture allows IT partners to resolve network bottlenecks and update policies remotely, removing the need for expensive on-site technical callouts.

Running a busy café group means our internet has to satisfy two completely different needs: it must be fast and secure for our business systems, yet open and welcoming for our customers. iShield gave us exactly what we needed. We've isolated our card terminals completely, put fair-use caps on guest downloads via a captive portal, and our IT partners manage all our branches from one central dashboard without any hassle.

— Cloud Group IT Partner & Retail Hospitality Specialist

Ready to secure your café 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