



HELIOS COUNTER-SURVEILLANCE

Privacy Intelligence + Digital Hardening + Professional RF Integration

A clear client guide to what you are buying, how it works and how it helps protect sensitive environments.

MicroSec-managed • Secure device controls • Vendor-neutral RF architecture • Evidence-led reporting

Designed for environments where confidentiality matters

Boardrooms, executive offices, legal and financial practices, high-value residences, sensitive commercial sites and organisations handling information that cannot simply be replaced if exposed.

Prepared for client discussion • South Africa • October 2026

1. What you are buying

Helios Counter-Surveillance is not sold as customer-owned software. It is a MicroSec-managed privacy intelligence platform licensed for authorised use for the agreed term.

The customer receives a managed right to use the approved Helios modules. MicroSec retains ownership of the platform, source code, intellectual property and unrestricted deployment rights.

In plain English

You are buying an ongoing privacy-protection capability, not a downloadable software file. MicroSec installs it, configures it, keeps it updated, integrates approved RF equipment and supports the system.

Managed Helios software licence Access to the approved Helios Counter-Surveillance features for the agreed devices, users, sites and licence term.	Secure setup and provisioning MicroSec controls installation, device approval, activation, roles, security settings and supported integrations.
Privacy intelligence workflow Trusted baselines, change detection, wireless/network indicators, risk scoring, evidence history, incidents and reporting.	MicroSec technical support Configuration changes, upgrades, escalation and approved integration work remain under MicroSec control.

What remains yours

Your organisation's own information, authorised records, evidence and customer-created content remain your information, subject to the agreed privacy, retention and service terms. Helios remains the MicroSec platform used to process and protect it.

2. How Helios protects the environment

Helios works by creating an authorised picture of what is normal in a protected environment and then helping identify meaningful changes. It is designed to reduce guesswork and create a defensible record of what was observed and what action was taken.

BASELINE	OBSERVE	COMPARE	CORRELATE	ESCALATE	REPORT
1. Trusted baseline MicroSec establishes the expected environment: approved wireless/network context, protected rooms, devices and authorised operating conditions.		2. Ongoing observation Helios receives supported privacy-risk indicators from the platform and, where commissioned, from professional RF equipment.			
3. Change detection New, changed or recurring indicators are compared against the trusted baseline instead of being treated as isolated alerts.		4. Risk correlation Helios groups related observations, tracks recurrence and gives the technical team context for prioritisation.			
5. Evidence & incident history Authorised observations, notes and system events are preserved into an auditable workflow for follow-up.		6. Executive reporting The client receives understandable findings, risk context and recommended next actions instead of a raw list of radio signals.			

Important evidence rule

A wireless identifier, signal strength, RF peak or software alert is not automatically proof that a hidden camera, microphone or other covert device exists. Helios separates indicators, correlations and verified physical findings.

2A. How Helios helps protect phones, accounts and Wi-Fi

Counter-surveillance is not only about finding radio signals. Modern privacy threats can also target phones, user accounts, Wi-Fi and network access. Helios therefore combines privacy intelligence with controlled access, device trust, encrypted local data and supported cyber-risk context. The purpose is to reduce the opportunities an unauthorised person has to reach sensitive Helios information and to make suspicious changes easier to investigate.

In plain English

A stolen password should not automatically equal trusted access. A new phone should not automatically be accepted. Sensitive offline information should not sit on the device as ordinary readable files. A new Wi-Fi device, network service or wireless indicator should not simply disappear into the background. Helios is designed around those principles without exposing the underlying security implementation.

Feature	What the client experiences	Why it is there
MicroSec-managed device approval	Only approved devices are provisioned for the licensed Helios environment. New devices can be held pending until MicroSec authorises them.	Helps reduce the risk of stolen credentials being used from an unknown device and gives MicroSec a controlled route to revoke access.
Biometric protection on supported devices	Supported devices can use the operating system biometric security layer before sensitive Helios access/actions.	Adds a second physical-user check when a phone or tablet is lost, borrowed or accessed by someone else.
App and device trust checks	Helios can verify supported integrity and device-trust information before allowing protected functions.	Helps reduce the risk of an untrusted or altered app/device being treated the same as an approved deployment.
Protected sessions and remote revocation	Helios sessions are managed, time-limited and linked to approved access. MicroSec can revoke a device or entitlement when required.	Helps contain access after a lost device, staff change, expired licence or suspected account compromise.
Encrypted offline assessment data	When authorised assessment information must remain available offline, Helios stores supported	Helps reduce exposure if the device or local application files are

	local data in encrypted form with protected device keys.	accessed without authorisation.
Trusted Wi-Fi / network baseline	Helios records the expected authorised environment and can flag supported new or changed wireless/network indicators, devices or services.	Makes rogue or unexplained changes easier to notice instead of relying on memory or a one-off scan.
Bluetooth and nearby-device awareness	Supported Bluetooth/BLE observations can be compared with known devices and previous assessments.	Helps surface new or recurring nearby indicators that deserve explanation or physical verification.
Permission and device-risk indicators	Helios can include supported privacy-permission, exposed-service and device-risk observations in the assessment.	Helps identify conditions that could unnecessarily expose camera, microphone, network or application data.
Helios Shield / cyber context where authorised	Where supported and authorised, cyber-security context can be correlated with Counter-Surveillance findings.	A wireless anomaly and a cyber alert together can be more meaningful than either observation on its own.
Audit trail and security-event history	Important access, assessment and escalation events are recorded for authorised review.	Helps the client understand what happened, when it happened and what was done about it.

Examples of the risks these controls are designed to reduce

- **Stolen or guessed credentials:** An attacker may obtain a password through phishing, reuse or another breach. Device approval, trusted-device controls and revocation mean credentials alone should not be treated as sufficient trust.
- **Lost or stolen phone/tablet:** Biometric access, protected local storage and the ability to revoke a managed device help limit what can be reached through that Helios installation.
- **Suspicious Wi-Fi or network changes:** A new access point, hotspot, endpoint or service can be compared with the trusted environment instead of being assumed legitimate.
- **Spyware or malicious software concerns:** Helios can surface supported integrity, permission, behaviour and Shield indicators, but it does not claim to detect every form of malware or spyware. Specialist endpoint/forensic investigation may still be required.
- **Unauthorised camera/microphone exposure:** Supported permission and privacy-risk observations help identify conditions that may expose sensitive device capabilities or data and require remediation.
- **Wireless spy equipment:** Wi-Fi, Bluetooth and professional RF observations can be correlated with the room baseline and evidence history, then escalated for physical verification where justified.

What we deliberately do not publish

Client material explains the protection layers and the outcome, but not the detailed internal detection logic, security thresholds, server rules, keys, integration secrets or response playbooks. Those remain MicroSec-controlled.

Helios reduces risk and improves detection, evidence and response. No responsible security platform can promise that every hacker, spyware strain or covert device will always be detected or blocked.

3. How the professional RF interface adds another protection layer

RF means radio frequency. Many legitimate systems use RF - Wi-Fi, Bluetooth, access-control equipment, telemetry and other wireless technologies. A professional spectrum analyser gives the authorised technical team visibility into radio-frequency activity across the equipment's supported range.

Why this matters

Helios does not rely on one brand of RF analyser. MicroSec can integrate supported professional RF sensors that provide a documented manufacturer SDK, API or approved control interface, then feed their spectrum observations into the same Helios evidence and risk workflow.

RF SENSOR

HELIOS RF EDGE

HELIOS
INTELLIGENCE

EVIDENCE

MICROSEC ACTION

Professional RF sensor

Measures supported spectrum activity such as frequency, signal level, timestamps and spectrum/waterfall observations.

Helios RF Edge

The MicroSec integration layer normalises the approved sensor data so different supported manufacturers can feed a consistent Helios format.

Correlation with the room baseline

RF observations can be compared with the authorised environment baseline and other supported Helios indicators.

Evidence-led escalation

Unusual or recurring activity can be documented, prioritised and escalated for further professional inspection when justified.

Vendor-neutral by design

The client is not forced into one RF manufacturer. The appropriate analyser or sensor is selected according to the environment, frequency coverage, sensitivity, integration interface, availability and budget.

RF hardware, SDK/API licensing, adapter configuration, commissioning and integration are separately quoted. Final RF integration pricing is subject to the selected product, technical compatibility, site requirements and written client approval before procurement or integration.

Helios Verified

A particular RF model is only described as Helios Verified after MicroSec has physically commissioned and tested that exact analyser, driver and interface combination.

3A. Examples of privacy threats Helios and RF integration may help identify

The examples below are not a promise that every device will be found. They show the types of authorised privacy-risk indicators that Helios, supported wireless/network observations and a commissioned professional RF sensor may help surface for further investigation.

The key idea

Helios looks for unexpected changes, recurring unknown indicators and unusual RF activity. A finding becomes stronger when several independent observations point to the same concern. A signal alone is not proof of a surveillance device.

Possible device / threat	What may be observed	How Helios helps
Wireless hidden camera	An unexpected Wi-Fi or other wireless transmitter, a new network-connected device, or RF activity that does not match the trusted room baseline.	Helios records the indicator, compares it with the baseline and can escalate it for authorised physical verification.
Wireless microphone / audio transmitter	Unexplained or recurring RF activity from the protected area that appears during sensitive periods and is not linked to approved equipment.	The event can be correlated with location, timing and previous assessments before further professional inspection.
Cellular / GSM / LTE / 5G transmitting device	Unexpected cellular-band activity or a previously unknown transmitting device associated	Helios can preserve the observation and risk context; MicroSec then decides whether

	with the protected environment.	specialist investigation is justified.
Bluetooth / BLE tracker or beacon	A new, unknown or recurring Bluetooth/BLE identifier appearing in or around an authorised protected environment.	Helios can track recurrence and compare the indicator against known devices and prior assessments.
Rogue Wi-Fi access point or mobile hotspot	A new wireless network, hotspot or infrastructure change that was not part of the approved environment.	The change is logged, assessed against the baseline and escalated if it cannot be explained.
Unauthorised network-connected IoT device	A new network device, service or wireless endpoint that does not match the approved environment.	Helios can classify the change and create an auditable follow-up workflow.
Unknown RF beacon / transmitter	Repeated RF energy or a recurring signal pattern from an authorised sensitive area with no known business purpose.	The signal is treated as an indicator - not proof - and can trigger deeper RF localisation or physical inspection.
Vehicle or asset tracker in an authorised scope	An unexpected wireless or cellular tracking indicator associated with a company-owned vehicle, asset or other explicitly authorised target.	Helios can preserve the evidence trail and support escalation to an authorised technical inspection.

What may require a different inspection method

Some threats may transmit nothing at the time of the assessment. Examples include wired microphones, local-recording devices, dormant or powered-off equipment and certain specialised devices. These may require physical inspection and other professional TSCM methods in addition to RF analysis.

What Helios does not do

Helios does not listen to, decode or intercept third-party communications. It uses authorised metadata, environment changes and evidence-led correlation to help identify what deserves closer investigation.

4. What Helios does - and what it does not claim

Helios is designed to	Helios does not claim to
Build trusted privacy baselines	Guarantee detection of every covert device
Identify supported Wi-Fi, Bluetooth, network and device-risk changes	Treat one RF or wireless observation as proof of surveillance
Ingest supported professional RF spectrum metadata	Decode or intercept third-party communications
Track recurrence and correlate multiple indicators	Replace specialist physical inspection where it is required
Preserve evidence and incident history	Pretend every RF analyser is automatically compatible
Support executive reporting and professional escalation	Transfer Helios ownership or source code to the client
Reduce unauthorised access risk through managed device trust, encrypted local data and revocable access	Guarantee that every hacker, malware strain or compromised network will be prevented

A typical client deployment

1. Confidential scope MicroSec and the client agree which rooms, sites, devices and objectives are authorised.	2. Managed licence The selected Helios plan and approved users/devices are provisioned by MicroSec.
3. Baseline The protected environment is documented and an initial trusted baseline is established.	4. RF selection if required The RF technology is agreed according to the client's needs and approved before procurement/integration.
5. Commissioning MicroSec installs, configures and tests the approved platform and RF interface.	6. Ongoing protection Helios provides the agreed monitoring/assessment workflow, evidence history, reporting and escalation.

5. Managed licence options

The figures below are the current Helios Counter-Surveillance managed licence structure. Prices exclude VAT. RF hardware, RF integration, travel, specialist physical TSCM work and site-specific requirements are quoted separately.

Plan	Managed licence	Secure setup	Annual licence	First annual total
Personal	R495 / month	R2,950	R4,950 / year	R7,900
Business	R2,950 / month	R7,500	R29,500 / year	R37,000
Professional	R6,950 / month	R14,950	R69,500 / year	R84,450
Enterprise	From R14,950 / month	From R29,950	From R149,500 / year	From R179,450

Enterprise and RF projects are scope-led

Enterprise pricing is a base starting point. Multi-site deployments, higher user/device counts, special integrations, RF sensor hardware, RF adapter licensing and professional commissioning are confirmed by quotation and written client approval.

6. What happens next

A client does not need to choose technology blindly. MicroSec first establishes the confidentiality requirement and authorised scope. We then recommend the appropriate Helios plan and, if RF spectrum visibility is required, the professional RF technology that best fits the environment.

CONFIDENTIAL DISCUSSION	SITE / RISK SCOPE	RECOMMENDATION	CLIENT APPROVAL	MICROSEC COMMISSIONING
-------------------------	-------------------	----------------	-----------------	------------------------

The outcome

A professionally managed privacy-intelligence environment that gives decision-makers clearer visibility, a repeatable assessment process, an evidence trail and a defined route for escalation when something deserves closer investigation.

Request a confidential Helios assessment | www.microsec.co.za