CRFS

RFeye Guard

Continuous real-time Technical
Surveillance Counter Measures (TSCM)
for sensitive or secure facilities

What is RFeye Guard?

The RFeye® Guard continuous TSCM (Technical Surveillance Countermeasures) monitoring system is a cost-effective alternative to bug sweeping strategies with guaranteed detection 24 Hours, 365 days a year.

If you are concerned about potential threats to the security of your facility, your private conversations, your plans and secrets, why settle for partial assurance when you can have complete assurance? RFeye Guard is an integrated continuous monitoring and threat geolocation system using indoor and outdoor RFeye sensors, high accuracy wired synchronization system and automated software for building and facility security control.

Typical applications for autonomous in-place monitoring systems include:

Embassies and Diplomatic Buildings

In a world of constantly shifting social and political landscapes, it is important that nations have safe-spaces to discuss ongoing events and policy both at home and outside home borders. Safe-spaces must exist without fear of bugging, interception or eavesdropping technologies. These secure spaces exist within government buildings as well as embassies and other diplomatic buildings such as diplomatic residences. These environments need a solution to ensure those spaces are continually free from transmitting devices and assure absolute freedom to discuss ongoing policy, strategy or intelligence.

National Critical Infrastructure

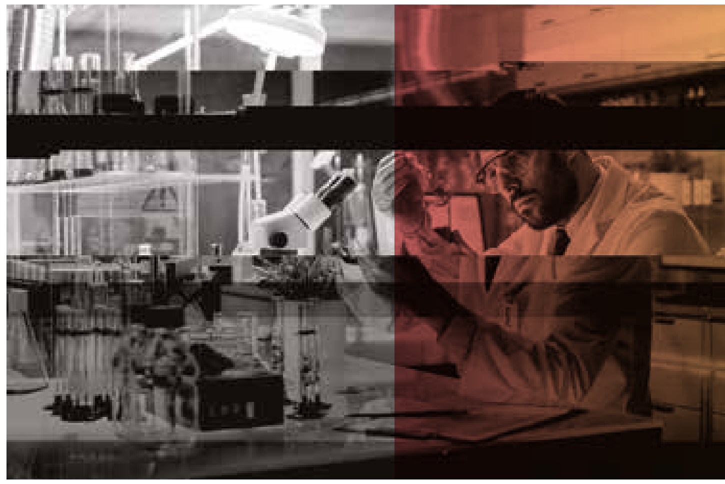
Infrastructure related to energy, transport, communications and public health are essential to a nation's safety, prosperity and wellbeing and this has increasingly made them a target for both physical and cyber attacks. Critical Infrastructure Protection (CIP) measures are vital to key assets such as nuclear reactors, water treatment plants and dams. Protection from electromagnetic threats needs to fit seamlessly into the infrastructure environment alongside physical and cyber measures to ensure that operation is both smooth and secure.

Secure Offices

Companies win commercial business through their employees ability to talk, develop, design and plan. From board rooms to engineering labs, critical tactical and strategic decisions are made and discussed in great detail. This is why, in modern business, security has to be a key area of focus. We are all familiar with the need for network security to keep intrusions out, which is perhaps why so many security breaches take place inside the organization.

Pharmaceutical/Medical

Cyber IP theft is a growing threat with the pharmaceuticals and biotech industries some of the hardest hit. Estimating the cost of IP theft is notoriously difficult, since the financial impact relates not only to the immediate loss of sales, but also factors such as brand reputation and willingness to invest in R&D. With increasing awareness of the need to protect IP from external cyber attacks, it is important to make sure that innovative companies are also looking closer to home. This means ensuring the office environment itself is not compromised by transmitting devices which might make a sophisticated cyber attack unnecessary.



Banking & Financial Institutions

Banks and other financial institutions are entrusted with a vast amount of consumer and business money and data. In the event of a security breach, the consequences for the affected institution will be loss of reputation and custom in the best case. In the worst case, there could be financial liability into millions of dollars. Even where data breaches are not related to negligent or malicious activities by employees, the organization can still be found liable if regulatory authorities find that best efforts have not been made to protect data. Comprehensive cyber, electromagnetic and physical security measures are essential to minimize risk.

Data Centers

Data center operators trade in trust. The ability to maintain services and assure data continuity alongside security is essential. Owner operated data centers need to deliver the same level of service, and also consider security as a primary function. Internal data services are more likely to be used for IP or business critical data and processing. Reliance on centralized infrastructure is growing as cloud services and virtual desktops becomes the default computing medium, making security and continuity increasingly dependent on data center resilience.

Why Is RF Security Important?

Common Eavesdropping Approaches

Modern surveillance technologies are highly discreet, highly capable and very difficult to locate. Even the smallest device can pack in a considerable amount of technology. They can be integrated into USB cables, light bulbs, or any number of other common objects.

When not in use, the device will lie dormant. If connected to a mobile network, it may only need to handshake momentarily once every 8 hours (network defined); at other times it remains RF invisible.

Video: Video may be gathered for any number of reasons. For example, identifying people, observing security measures, capturing passwords on air gapped devices or for use as leverage in blackmail or social engineering.

Data: Data may be targeted by interception keystrokes or installation of devices that give remote 'at desk' access to a compromised computer, allowing for transmission of files, network alteration or data destruction.

Audio: Audio intelligence can reveal a lot of information in a short time. It is generally immediate and context based. Audio eavesdropping is not just limited to the transmission or buffer-transmission of sound files. Modern devices allow for speech recognition meaning only small text files need to be transmitted, very quickly, and at intervals which may be weeks, or longer.

All Three: Organizations are becoming ever more aware of the dangers that mobile devices carry. Almost any smartphone can provide video, audio, data, GPS location, angle data, movement confirmation and more. A compromised phone or tablet is very hard to spot for the average user, and carries very little risk for the threat actor. It is common sense to keep your safe areas free from mobile devices.

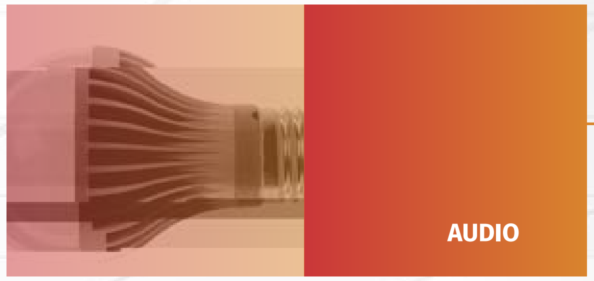
How Do Devices Defeat Common Countermeasures?

Eavesdropping technologies need to able to hide in several ways. Physically they need to integrate with their surroundings, while technically they need to hide their electronic signatures, be that power consumption, physical junction architecture or RF emissions.

TSCM sweep teams carry out a vast array of tests and inspections to uncover hidden devices, but rely upon the device being physically discoverable, reactive to non linear junction tests, or emitting identifiable RF signals.

Devices can often lie dormant until they are triggered by sound, light or movement. They may operate on a defined schedule matched to an individual's diary or they may use other techniques for low power operation.

Location can also be a factor; an eavesdropping device may hide beside or even within a high power device. A TSCM sweep team would thus need to open the high power device in order to visually identify the eavesdropping device, a measure which adds time and further complexity.



What About Data Facilities?

Wireless Advanced Persistent Threats (Wireless APT)

The idea of an Advanced Persistent Threat (APT) is by no means a new one. An APT is the infiltration of networking systems by a specific threat actor over a sustained period of time. This type of attack originates chiefly from hacktivist or state sponsored entities and is designed to extract information slowly and carefully without detection and with minimal risk of exposure. APT often makes use of social conditioning tactics amongst others to gain a foothold into internal systems and security.

As technology has advanced, so have the number of possible attack vectors open to the threat actors. One of the more recent methods of exfiltration of data from a secure facility is the use of wireless technology including Bluetooth, Wifi, GSM, LTE and bespoke frequency carriers designed to hide within the existing RF landscape. This gives rise to the Wireless APT threat vector.

Traditional APT attacks have been hampered by advances in technology designed to secure software environments and physical hardware, making the attacks more likely to suffer mission failure.

Anatomy of a Wireless APT attack

There are two primary components of any Wireless APT attack.

1: A technical implant designed to interface with physical hardware whilst avoiding detection

2: A Command & Control (C2) vector designed to communicate with the technical implant and the threat actor.

First, the technical implant needs to be placed in your facility. This could be done in a number of ways which circumvent internal security. The exploitation of supply chain vulnerability is a low-risk method of delivering an implant into a server, router, patch panel etc. The implant may even be applied at the point of manufacture. It may make use of zero-day vulnerability that is deliberately introduced into the design, or discovered after launch.

Once the implant is in place and active, the C2 component comes into play. The C2 sits at the security periphery giving communication access to the threat actor, who for example may arrive in a utility truck once a month to manage the devices and collect data. Even a compromised mobile phone, tablet or laptop inside the facility can communicate target instructions to the implant, and recover stored data for later transmission back to the threat actor, in essence becoming a middleman C2 device.

Once in place, the threat actor can traverse your network looking for data, or additional vulnerabilities that permit access to further infrastructure.

Because these types of attack vector are intended for long term information gathering, they are designed to leave no destructive trail, and will not show up in a device audit designed to look for peripheral devices or operational signatures in an OS.

In practice, wireless communications can take place at almost any frequency. They may sit alongside existing emissions or could be designed to hop frequency regularly or move as a sweep.

Technical implant milled-in below existing chip-set during overnight storage in warehouse

How RFeye Guard forms an essential part of your TSCM strategy

GSM bugging devices are available today from well-known online retailers for less than $50. Meanwhile, non-commercial devices are becoming increasingly sophisticated and harder for traditional TSCM (Technical Surveillance Countermeasures) operatives to detect. The consequences of undetected RF surveillance and data transmission include: financial losses to corporate organizations, compromise of law enforcement and intelligence agency operations and eavesdropping on what should be secret government conversations by hostile state actors.

When addressing the RF piece in the security puzzle, the traditional approach of using sweep teams is no longer sufficient. Such sweeps can easily be defeated by a device using techniques to avoid detection, e.g. frequency hopping, hiding close to a high power signal or transmitting in short infrequent bursts. And of course, a device can be switched off during a sweep, or placed after a sweep is conducted.

To provide complete assurance against RF surveillance, there is a need for continuous real-time TSCM in the form of an In-Place Monitoring System. With many of our customers, we have found that the barriers to implementation have been the assumed cost, alongside concerns that the installation process would be invasive. They have been pleasantly surprised to discover that RFeye Guard can be installed with a minimum of distruption and at a much lower cost than expected.

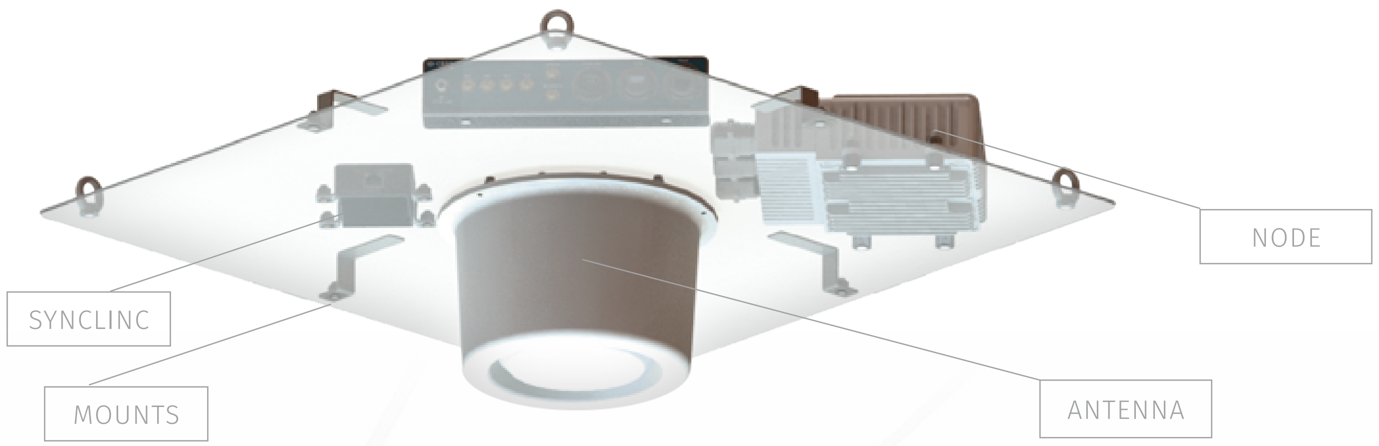
Why settle for partial assurance when you can have complete assurance?

RFeye Guard is CRFS's solution for continuous TSCM monitoring in secure buildings and facilities. It is deployed as a network of synchronized indoor and outdoor sensors to detect suspect signals, locate and alarm in real time.

It is cost effective, discreet, easy to deploy, easy to use and provides our security customers with true peace of mind 24hrs, 365 days a year.

Monitor 24/7

RFeye Guard monitors 24/7 to instantly detect suspect signals in real time. Fast sweep speeds and exceptionally low noise figures allow our RFeye sensors to detect even the lowest power and shortest duration signals. These intelligent sensors, combined with the Guard software suite, operate autonomously and can make their own decisions to conduct additional high resolution sweeps in response to detected signals.



Locate

GPS signal reception is generally poor inside buildings, but RFeye Guard includes our SyncLinc system for wired or optical timing synchronization in and around buildings. The use of indoor and outdoor sensors allows the system to discriminate between signals transmitting from inside and outside the building to minimize false alarms. Once it is confirmed that a signal originates inside the building, POA geolocation can then be used to locate the signal source. One or many signals can be located simultaneously.

Alarm

When a suspicious signal has been located, a quick response is needed. RFeye Guard can trigger alarms from third party security systems and provide a real-time alert and location to a security guard. Signal detection can also trigger a recording so that the signal can be analyzed in more detail after the event.

Indoor/outdoor signal discrimination and frequency masks tuned to the 'typical' RF environment for a building ensure a minimum of false alarms.

Analyze

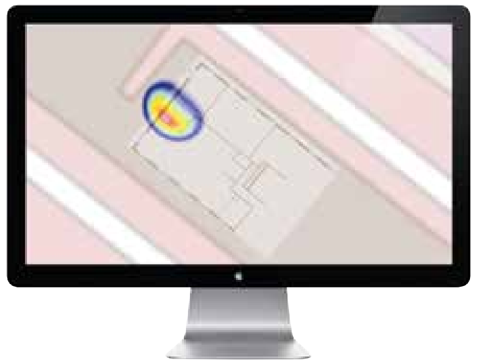
RFeye Guard provides a simple interface for those users who just need to see alarms and signal locations. For those users wishing to analyze signals in more detail the expert interface is available. This provides a suite of powerful tools for forensic signal analysis. This can be carried out in real-time or signals can be recorded for post-event analysis, including classification and demodulation.

Manage

You don't need to keep a constant watch over RFeye Guard. The system monitors 24/7 behind the scenes, and only alerts you when you need to know about a signal.

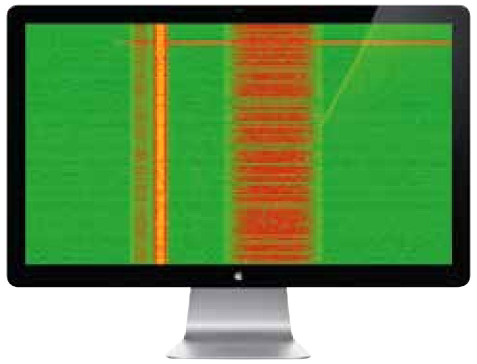
However, if you do want to manage the network and access more data you can. Database features allow you to explore historical sweep data and event logs to see the bigger picture.

Our software can also be used to manage work-flow and assign incidents to different users.



LOCATE

ALARM



ANALYZE

MANAGE

System configurations

RFeye Guard can be scaled for different customer requirements and different size facilities. All our RFeye Guard packages come with:

- Full Software suite
- SyncLinc wired timing synchronization system (Cat5 or optical fiber)

The number of sensors will depend on the size of your facility.

A typical 'small package' for a single floor or small office might include:

- 6 sensors (any combination of indoor and outdoor)

A typical 'large package' for a large building complex might include:

- 25 sensors (any combination of indoor and outdoor)

RFeye Stormcase

Our TSCM portfolio

Many of our security customers also take advantage of our portable monitoring solutions: RFeye Stormcase and RFeye Backpack. These are particularly useful for customers needing a cost-effective way to secure multiple buildings on an ad hoc basis. RFeye Stormcase and RFeye Backpack can be redeployed to different locations as required.

RFeye Backpack

External RFeye Node

To learn more about RFeye Guard, contact us at enquiries@crfs.com

We can also arrange a live demo using an existing installed office sensor network.

What makes RFeye different?

CRFS is at the forefront of new technology for distributed monitoring and geolocation featuring wideband receivers with fast sweep speeds and best-in-class noise figures. Low power and/or short duration signals which would be missed by traditional receivers and sweeping devices cannot evade RFeye technology. For our TSCM customers this means more reliable detection and confidence that their facilities will remain secure.

State-of-the-art software maximizes the ability to extract intelligence from the spectrum. This ranges from real-time alarms and locations on map displays to detailed forensic analysis of suspicious signals in real time or post event.

But RFeye systems are not just a collection of hardware and software. Our systems are truly intelligent and capable of making their own decisions in response to the spectral environment. This automation and intelligence means your building is secured in the background 24/7, with minimal need for user intervention.

These solutions give outstanding value for money without compromising performance.

Direction finding and geolocation with AOA, POA and TDOA

Portable RF Recorder / RTSA

Real-time monitoring with autonomous, rugged and intelligent RFeye Nodes

Other Products in the RFeye Range

RFeye Guard
Key Software Capabilities

Alarms
Recorder
Notifications
Sweep & Capture
Automation
Real-time
Database
POA
Power
SMS Alerts
Email Alerts
User Controlled
Script
Big Data
Modulation Recognition

Hardware
Example Node Specifications

Example based on selection of Node 20-6 hardware

RF Specifications	
Switchable RF inputs	4 x SMA connectors
Frequency	
Range	10 MHz to 6 GHz
Noise figures at maximum sensitivity	
10 MHz to 3 GHz	8 dB typical
3 GHz to 6 GHz	11 dB typical
Phase noise	
Receiver input at 2 GHz	-91 dBc/Hz at 20 kHz offset, typ.
Signal analysis	
Instantaneous bandwidth	20 MHz
Tuning resolution	1 Hz
Internal frequency reference (pre-calibration)	
Initial accuracy	better than ±2 ppm typ.
Stability	better than ±1 ppm typ.
Ageing	better than ±2 ppm per year
Programmable sweep modes	
Sweep speed - fast synth	45 GHz/s @ 1.2 MHz RBW
Sweep speed - high quality synth	18 GHz/s @ 1.2 MHz RBW
User programmable modes	free run continuous, single timed, user trigger and adaptive
Trigger-on-event modes	user defined masks, actions and alarms
Sampling	
Resolution	12 bits per channel (I&Q)
Rate	40 MS/s I&Q
Third order intercept points with AGC	
< 1 GHz	+21 dBm typical
1 GHz to 6 GHz	+22 dBm typical
Local oscillator	
Re-radiation	-90 dBm typical
Frequency references	
Selectable	Internal, GPS or external
External input	10 MHz ±1 kHz
Output	10 MHz

Processor sub-system	
CPU	Marvell 88F6281 @ 1 GHz
Main memory	512 MB DDR2
System disk	512 MB
I/O	
Network	1 x 1 GigE, with POnE
Universal Serial Bus	2 x USB 2.0
2 x IEEE1394 expansion ports configurable as:	2 x SyncLinc, trigger input, external peripheral control
GPS antenna input	1 x SMA passive or active (3.3 VDC)
Data storage	
External flash disk	via USB interfaces
Optional internal storage	512 GB SSD option
System software	
Boot firmware	U-Boot
Operating system	Linux, kernel v 2.6
RFeye Node Control Protocol	NCP Server (NCPd)
Node Apps (optional)	Logger, Recorder
Size & weight (Sensor)	
Dimensions (w, h, d)	170 x 60 x 125 mm (6.7 x 2.4 x 4.9 inches)
Weight with IP67 end plate	2 kg (4.4 lbs)
Size & weight (Ceiling tile)	
Dimensions (w, h, d)	600 x 600 x 130 mm (23.6 x 23.6 x 5.5 inches)
Dimensions (w, h, d) (US)	610 x 610 x 130 mm (24 x 24 x 5.5 inches)
Weight	6 kg (13.2 lbs)
Size & weight (Outdoor)	
Dimensions (w, h, d)	320 x 360 x 170 mm (12.6 x 14.2 x 6.7 inches)
Weight	10 kg (22 lbs)
Power	
DC power or POnE	10 to 48 VDC
Typical	15 W
Maximum	25 W
Environmental	
Operating temperature	-30 to +55 °C (-22 to 131 °F)
Storage temperature	-40 to +70 °C (-40 to 158 °F)
Sensor Ingress protection	IP67 (with end plate)

About CRFS

CRFS provides best-in-class solutions for radio spectrum monitoring, management and geolocation.

CRFS offers a new generation of technology for the detection, identification and geolocation of signals in complex RF environments.

CRFS is recognized as delivering truly "best in class" technology - our RFeye systems are deployed worldwide by regulatory, military, law enforcement and intelligence agencies.

For further information or to schedule a demonstration visit:

crfs.com

CRFS

See through the noise

CRFS Inc
Chantilly, VA, USA
+1 571 321 5470
enquiries@crfs.com

CRFS Ltd
Cambridge, UK
+44 1223 859 500
enquiries@crfs.com

bsi. ISO 9001:2015 Quality Management

UK Certificate number: FS576625