

## Active eavesdropping protection

---



We provide sweeps, which are active anti-bugging measures that involve the inspection of a secure area with technical equipment by specialists. The service includes the regular inspection of rooms to check for technical eavesdropping devices, as well as continuous monitoring during a conference or meeting. For many security managers, the initial question is whether an external service provider should be commissioned with the eavesdropping prevention test or whether the appropriate resources should be set up internally and equipped with the necessary technical tools. The benefits of using of an external service provider include rapid response at short notice as well as lower costs.

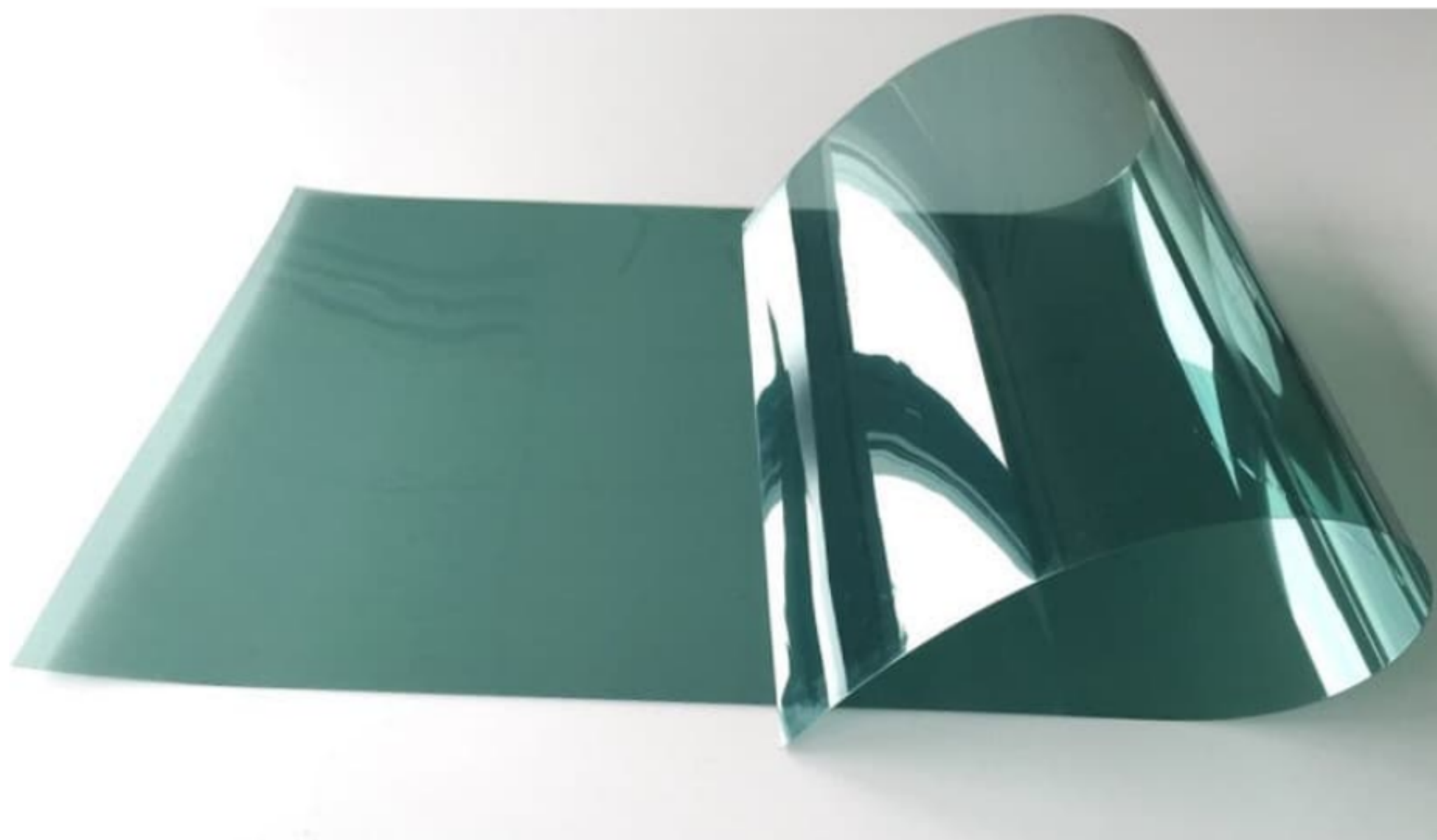
In the long term, however, you may decide that it's worthwhile to build up an internal eavesdropping defense system – partly for cost reasons and partly to mitigate the risks that may arise if you entrust the protection of your highly confidential information to an external service provider. In the following sections, you can find out about our range of devices and technologies for active eavesdropping protection. However, please note that your staff will need professional technical



training to ensure they use the devices correctly.

## Solutions

---



### Defense against acoustic attacks

Our noise generation system prevents conversation monitoring using laser systems or structure-borne microphones. The transducers installed on the panes, in the walls and ceilings and on the pipes, as well as the connected noise generator, are superimposed with randomly generated noise waves of the conversation. With the appropriate software, the systems can be set so precisely that there are only minimal impairments in the room. In order to protect your room against penetrating laser beams, we recommend that you also apply laser protection film on the windows.

Alternatively, or as a supplement to this, soundproofing can also be integrated into the room architecture.



## Defense against attacks via radio transmission

### Locating active transmitters

There are several ways to protect yourself from technical eavesdropping devices. A proven method is the use of intelligent test receivers. These are radio receivers/spectrum analyzers that cover a very wide frequency band and can also detect and analyze infrared signals from the air and long wave signals from power lines. Their analytical capability is based on complex algorithms and advanced computer capacities to locate even the complicated eavesdropping transmitters



described above.

### Locating passive transmitters and semiconductor components

Passive transmitters and semiconductor components, such as eavesdropping devices that are not currently transmitting or switched-off mobile phones, are detected by a so-called semiconductor detector or non-linear-junction detector (NLJD). This uses a specially polarized antenna to emit a frequency in the range of 880 to 2.4 GHz and simultaneously receive the respective harmonic of this frequency. Harmonics are integral harmonic oscillations of the original frequency that occur with every wave movement. Thus, the second harmonic is 880 MHz (1760 MHz;  $880 \times 2$ ) and the third harmonic is 2640 MHz ( $880 \times 3$ ). If the radio wave emitted by the NLJD antenna strikes an electronic component, each semiconductor (transistor, diode, integrated circuit, etc.) causes a strong reflection of the second harmonic. Semiconductors, however, do not always have to be electronic in nature.

Even a lever handle that has not been operated for a long time forms more or less well conducting (= semiconducting) transitions between its moving metal surfaces. These corrosive transitions cause a strong reflection of the third harmonic. From the ratio of the second and third harmonics shown on the NLJD's display, you have reliable information as to whether you are dealing with a threat from electronic eavesdropping devices in the wall, or a piece of rusty structural steel in the concrete.




### Checking network, telephone and power lines

Once the rooms have been examined for active transmitters and for all semiconductor components, the lines installed in the room still pose a security-related risk. To close this gap, all lines are measured and checked with the appropriate measuring instruments. The following devices are required for such a check: a multimeter, audio amplifier, line distribution, time domain reflectometer,



digital audio demodulator and an oscilloscope. More recently, multifunctional devices specially adapted to this application have been used, such as the TALAN line analyzer, which covers the all the above functionality. This device combines the required functions in a single tool and also offers the detection of eavesdroppers on lines with frequency domain reflectometer measurement. The TALAN has 80% of the ISDN protocols available worldwide and can demodulate them.

© 2018-2019 EMshield GmbH, Bretonischer Ring 12, 85630  
Grasbrunn/München, +49 89 4545482-0

[Home](#)[Downloads](#)  [inf](#) [Sitemap](#)  
[Impressum + Datenschutzerklärung](#)