

How we protect your company, layer by layer

We run IT for 70+ companies in Romania, most of them with between 10 and 300 employees. For all of them, security comes in the same subscription as IT support. **Five layers of security we set up, run and answer for, with round-the-clock monitoring.**

Attacks come from two directions. The software guarding the endpoints sees nothing of the accounts, and the one guarding the accounts sees nothing of the endpoints.

ENDPOINTS

Laptops, desktops, servers, work phones

- Ransomware starting to encrypt files.

ACCOUNTS

Microsoft 365, passwords, browser sessions

- A sign-in from another country, at 4am.

Both reach the same analysts, on shift around the clock

They confirm it really is an attack and stop it spreading.

8 min**AVERAGE
RESPONSE TIME**

From the alert to
the attack being
stopped

24/7**SOC
MONITORING**

Specialist analysts
we work with,
nights and
weekends included

5**SECURITY
LAYERS**

Included in the
subscription, for
every client we
manage

25+**YEARS OF
EXPERIENCE**

Managed IT since
2001, based in
Bucharest

**ISO/IEC
27001:2022**

Certificate
RO231109006,
externally audited
yearly, verifiable in
IAF CertSearch

**Microsoft
Solutions
Partner**

For Modern Work: we
run your company's
Microsoft 365
environment directly

70+ companies

In Romania, most
with between 10 and
300 employees

**8 Google
reviews**

All five stars, public
on the company's
Google profile

What changed in Romania. The 2025 activity report of Romania's National Cyber Security Directorate (DNSC) shows a 353% rise in compromised accounts and a 153% rise in ransomware incidents.

NIS2 is transposed into Romanian law through Government Emergency Ordinance 155/2024, approved by Law 124/2025. If your company falls under it, security measures are no longer a choice, and the responsibility sits with management, not with the IT department.

The five layers of security, plus two optional ones

The further down you go, the less the software does and the more a person does.

01

Files already known to be dangerous **ANTIVIRUS**

It blocks what is already on the known-threat lists. Every company has it, but ours does not stay on the default settings: we manage it centrally, and its detections go to the analysts, around the clock.

ANALOGY *The list of known faces at the door.*

ENDPOINT

02

What happens on the endpoints **EDR**

It watches behavior rather than files: which programs start, ransomware beginning to encrypt. It blocks clear patterns on its own, such as an attack that uses no file, and flags the rest. A computer is isolated only after an analyst confirms it is an attack.

ANALOGY *The motion sensors inside the building.*

ENDPOINT

03

Who signs in to the Microsoft 365 accounts, and what they do next **ITDR**

It learns what is normal for each account, then flags the deviations: access from another country at 4am, stolen sessions, sudden administrator rights. A sign-in with a stolen password, or a hidden rule for invoice emails, it blocks on its own.

ANALOGY *The doorman who checks the badge on the way in and watches what the person does once inside.*

ACCOUNTS

04

Somebody watching, around the clock **SOC**

The telemetry from layers 02 and 03 arrives together at the monitoring center. Specialist analysts we work with confirm it really is an attack and stop it spreading: they take the computer off the network or lock the account.

ANALOGY *The dispatch room, staffed in shifts, around the clock.*

BOTH ZONES

05

Somebody who comes and fixes it **OUR IT SUPPORT TEAM**

We check what the attacker touched, clean the computer, reconnect it and explain to you what happened and what we changed. This is where the chain closes, which is why it is last.

ANALOGY *The crew that turns up on site and puts everything back in order.*

BOTH ZONES

The two optional layers

They are not part of the subscription by default. We recommend them to most companies.



Every log, in one place **SIEM**

Layers 02 and 03 see only the endpoints and the accounts. This layer adds the records from Windows, the firewalls, the VPN and the other connected devices. With more sources, the analysts see more and can catch earlier an attack that would otherwise surface late. On its own, it stops nothing. It also leaves a written record, kept for years, useful for an audit.

OPTIONAL



The people who click the links **SAT · SECURITY**

AWARENESS TRAINING

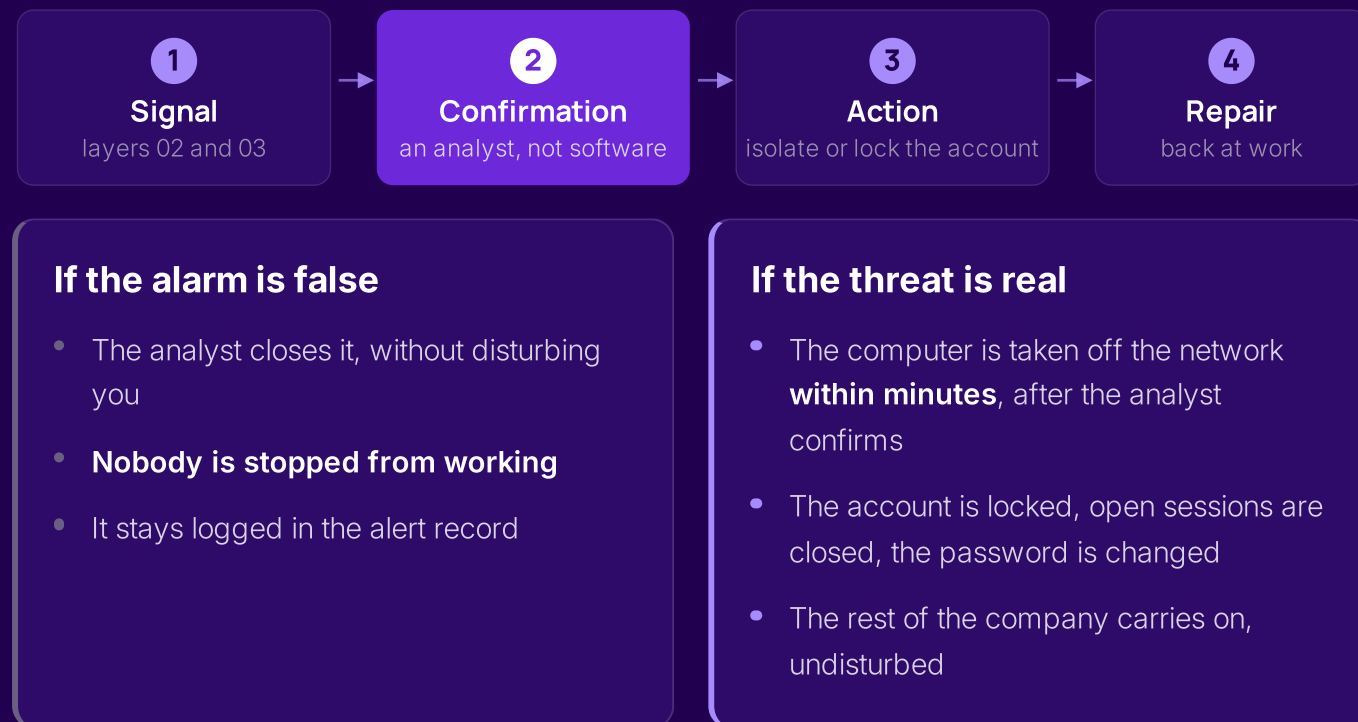
Short, interactive monthly training, followed by simulated phishing emails. The theory gets checked in practice: you see who learned it and who still needs help. It replaces no technical layer, but it stops some attacks before they start.

OPTIONAL

We set up, run and answer for these two just as we do for the five included layers. They are added to the subscription only if you choose them.

What happens, step by step

The order matters: **nothing is isolated before a person confirms it.** That way we do not stop the company for a false alarm.



MTTR from the alert to the attack being stopped. Clean-up comes afterwards.

8 min

Our average response time.

It includes the triage an analyst does, not just automatic detection.

Eight minutes means an attack that starts at three in the morning is stopped before daybreak.

Monitoring runs at any hour, including a Saturday night or Christmas Day.

Want to know where you are exposed?

The free 45-minute assessment, online. Afterwards, you get the offer in writing. Pick a time in the calendar, no obligation.

risksoft.eu/cybersecurity