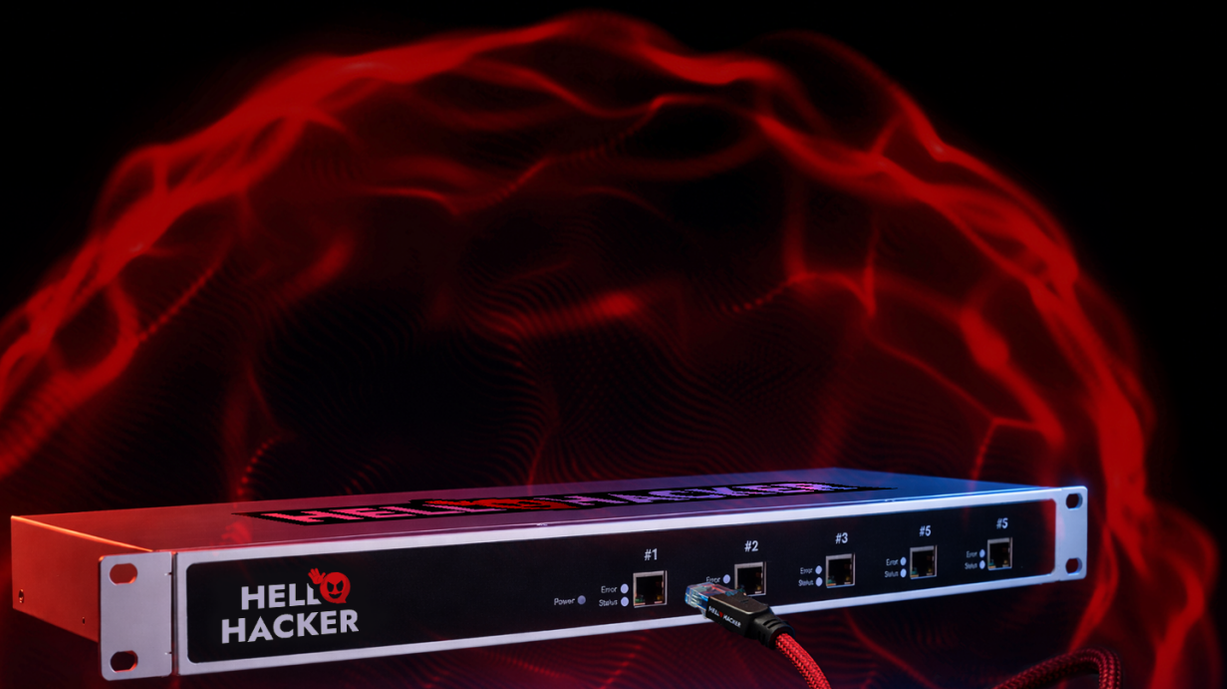
HELLOHACKER

TECHNICAL DATASHEET



Block hackers before they strike

An intelligent ecosystem, without complexity.
Simple to deploy. For quick cybersecurity gains.

Passive detection & lateral movement

WHAT IS HELLOHACKER ?

HelloHacker is a passive threat detection platform.

Unlike traditional solutions based on signatures or periodic scans, HelloHacker detects behaviors, network anomalies, lateral movements, and exploitation attempts without interrupting your users' activity.

Designed to reveal suspicious activity in real time within your internal network, your DMZ, or your BYOD environments.

WHY HELLOHACKER ?

Organizations must deal with threats that are :

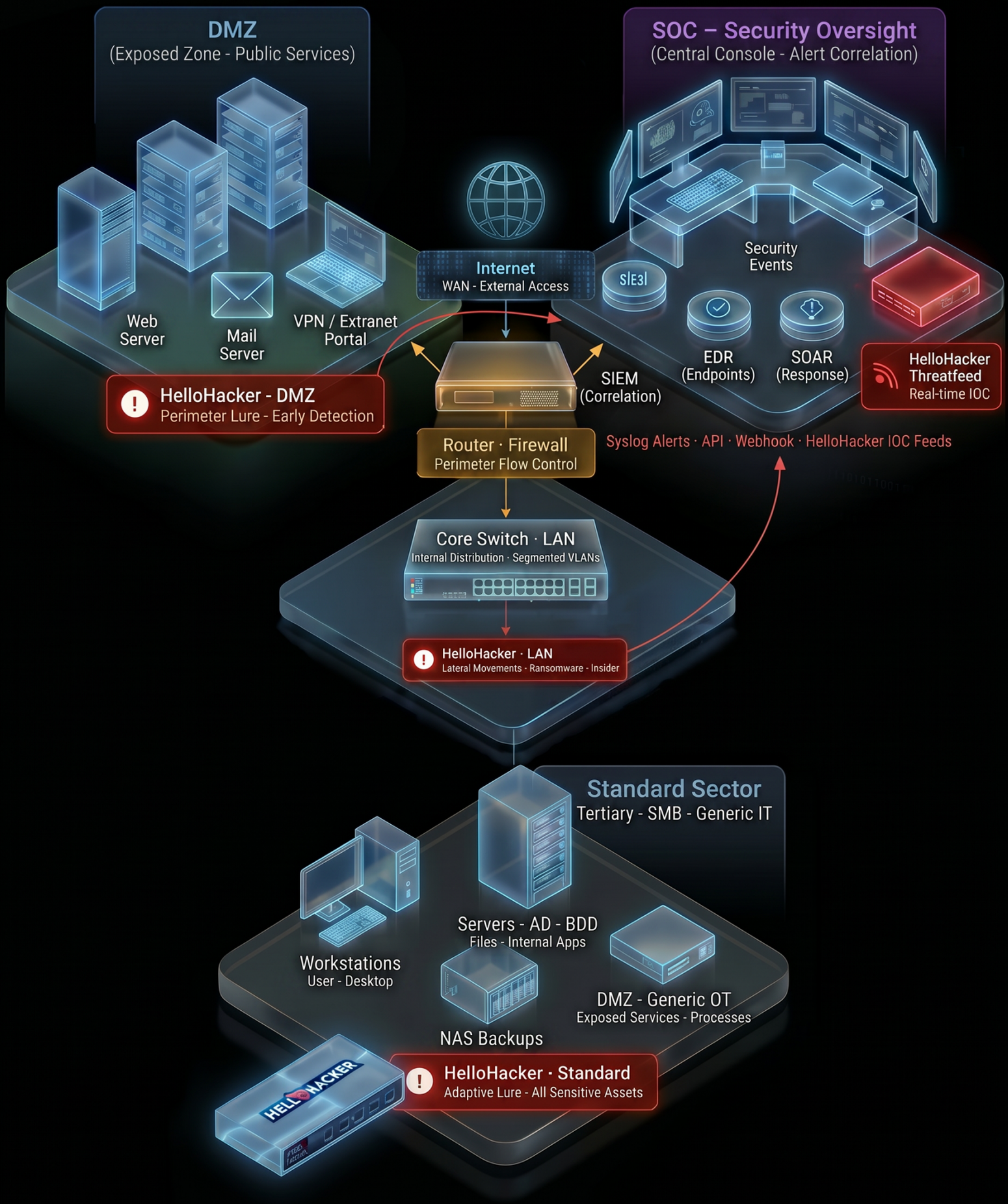
- increasingly silent
- increasingly sophisticated
- often internal or already present inside the perimeter

HelloHacker was designed to cover a blind spot that vulnerability scanners, EDRs, and firewalls cannot fully address :

Understanding what is really happening in your network, continuously, with fast installation and minimal maintenance.

HelloHacker — Deployment Locations

Standard Network Schema · Health · OT · Municipal · Tertiary - Standard



LATERAL MOVEMENT DETECTION

Detection and correlation of events

- Network reconnaissance
- Port scans
- Authentication attempts
- Remote commands
- Pivoting
- Internal escalation attempts

HelloHacker quickly identifies attack patterns observed during real-world penetration tests.

Passive detection — Zero impact

- No scanning
- No agent
- No injected packets
- 100% network observation

Built-in honeypot

- Fichiers appâts
- Services factices
- Pièges réseau
- Déclencheurs dynamiques

Each suspicious interaction triggers

- An alert
- A classification

Centralized portal — Complete visibility

- Detailed event list
- Correlation by source, destination, and user
- Dashboards
- Real-time notifications

No complex configuration

- Deployment in 5 minutes
- Simplicity designed for MSPs and internal IT teams
- No dependencies
- Support included
- Automatic updates

Optimized for educational environments and SMEs

- Low operating costs
- Simple and actionable reports
- Designed for limited or overloaded IT teams
- Proactive protection before a real attack

How HelloHacker works

1. The device observes local network traffic.
2. Suspicious events are captured and correlated.
3. The central portal applies rules, thresholds, and classifications.
4. Relevant alerts are sent to the teams.
5. Automated reports help improve the security posture.

Use cases

- ✔ Internal attack simulation
- ✔ Detection of malicious employees
- ✔ BYOD / guests / students
- ✔ DMZ security
- ✔ Firewall validation, internal/external
- ✔ Network proactivity for unmonitored environments

PERFORMANCE AND CAPACITY

TRAP services	HTTP server, HTTP Proxy, Git server, FTP server, Portscan, Samba server, SSH server, MySQL server, Redis server, SIP server, SNMP server, RDP server, TFTP server, NTP server, Telnet server, Microsoft SQL server, VNC server, Poisoning Detector

HARDWARE AND DIMENSIONS

Form factor	1 U Rackmount
Total interfaces	**5X** 1GbE RJ-45 ports
Height	1.73228 in / 44 mm
Width	17.126 in / 435 mm
Length	6.10236 in / 155 mm
Weight	1.63 kg / 3.6 lbs

ENVIRONMENTS

AC Power Source	12VDC / 3 amp
Power Consumption (Max/Average)	16.5 W / 11.8 W | 1.2 A / 1.0 A
Heat Dissipation	81.92 (BTU/h)
Operating Temperature	46 °C
Storage Temperature	-20 °C to 70 °C
Recommended Humidity	Between 40 and 60 %

OTHER INFORMATION

Product	Hacktrap
SKU	HH05
Description	...

HelloHacker Positioning

HelloHacker sits between EDR and firewalls :

It detects what scanners do not see, at a fraction of the cost of a SOC.

Included with the Subscription

- PORTAL ACCESS
- AUTOMATIC UPDATES
- TECHNICAL SUPPORT
- LIFETIME DEVICE WARRANTY
- ACTIVITY REPORT
- AND MUCH MORE

info@hellohacker.com | HelloHacker.com