



## XDR/ EDR OPTIMUS

### Endpoint Protection Detection & Response

Trojan horses, spyware, ransomware: your antivirus can't protect you from unknown threats. Defend all your endpoints with **OPTIMUS EDR** and its autonomous technology.

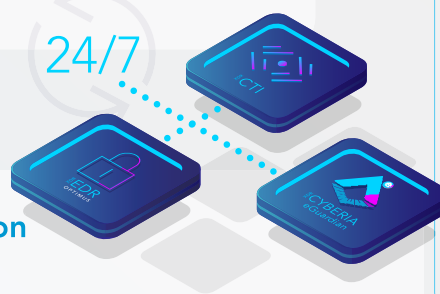
#### INDUSTRY RECOGNITION

TEHTRIS recognized as a Representative Vendor in the 2022 Gartner® Market Guide for Network Detection and Response\*.

Traditional antiviruses are outdated in comparison to the **OPTIMUS EDR** technology. Our EDR ensures an optimal protection and a full visibility of your IT assets and is directly integrated into the Windows Security Center.

#### 24/7 monitoring of your endpoints

All your endpoints and servers are protected thanks to our real-time detection and neutralization, without any action being required on your part. **OPTIMUS EDR** combines the features of an EDR and a Next-Gen Antivirus. Hyper-automate your analyses, detections, isolations and remediations with our EDR to achieve a full protection of your infrastructure.



#### Unmatched detection and neutralization

**OPTIMUS EDR** blocks attacks before they can reach your IT assets. Our artificial intelligence **TEHTRIS CYBERIA**, made of several neural networks (Deep Learning), is unmatched in its detection accuracy of known and unknown threats.

Our EDR also comes with **TEHTRIS CTI**, our Cyber Threat Intelligence. **TEHTRIS CTI** gives you all the tools needed for a full protection of your infrastructure: instant

analysis, sandboxing and hunting. Combine it with all the remediation features of our EDR (suspend, quarantine, kill and regular disk scans) to neutralize threats in real time.

- ↓ Detection and neutralization 24/7 without human intervention
- ↓ ScanDisk: static files analysis
- ↓ Detections based on AI and/or signatures
- ↓ Remote script execution in a secured mode
- ↓ Suspend, quarantine, kill
- ↓ Neural networks (Deep Learning)
- ↓ Customizable automation of the features
- ↓ Access to the TEHTRIS XDR Platform and its augmented technology (SOAR, CTI, CYBERIA)
- ↓ Dashboards and reporting
- ↓ Available in Cloud & on-premises
- ↓ Compatible with existing ecosystems: In & Out APIs

#### Orchestrate your cybersecurity

Choose playbooks or create scenarios with **TEHTRIS SOAR** (integrated in our EDR) and keep your teams focused on tasks that really matter.

**OPTIMUS EDR** is hyper-automated and protects you from cyberattacks 24/7, without human intervention.

#### BENEFITS

- ▶ Integrated into the Windows Security Center
- ▶ Complete overview to monitor all your endpoints and servers
- ▶ Compatible with your IT & OT environments (ICS, PLC...)
- ▶ Uninterrupted overview of your infrastructure
- ▶ Centralized and remote management
- ▶ Easily and quickly installed and deployed
- ▶ Low CPU, RAM and storage consumption

# KEY FEATURES

## Govern and manage risk

- Augmented & customizable dashboards
- Endpoint vulnerabilities audits & compliance
- Detection of unprotected assets (ShadowIT)
- Ticketing & reporting



Reduce your reaction time

Detect threats automatically

Customizable filters that can be shared between teams / users

Prioritization of alerts with Soc in the Box

Grouping of alerts

Default and customizable configurations (application policies, blacklists & whitelists...)

Specific modules for any type of threat (powershell, ransomware...)

Device management (USB monitoring, etc.)

Integrated ScanDisk

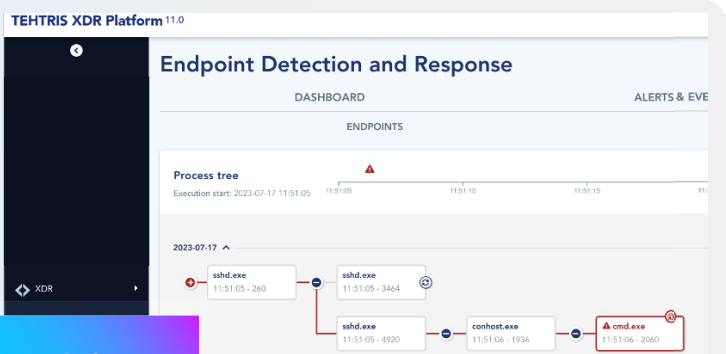
CYBERIA (Deep Learning)

## Respond instantly to attacks

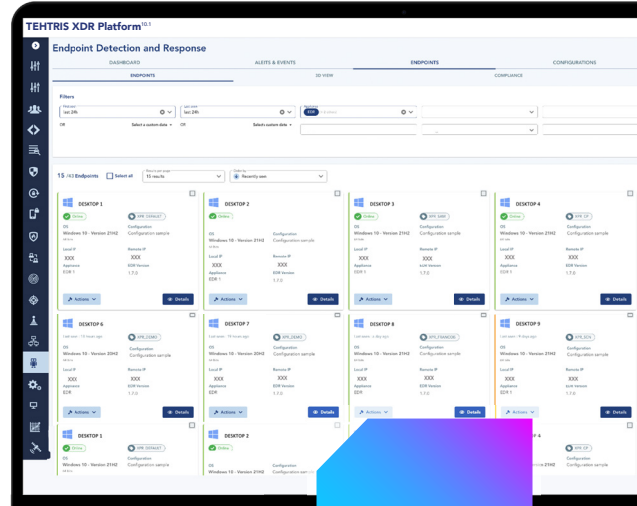
- Customizable remediation: kill, isolation, quarantine...
- Automated remediation actions (SOAR and playbooks compatible with your third-party solutions)
- Remote script execution
- Investigation & IOC Hunting
- TOF analysis

## Supports all the OS

Windows XP to Windows 11, Windows Server 2003 to 2022  
 macOS Sierra, High Sierra, Mojave, Catalina, Big Sur, Monterey  
 Linux



Focus on the Process Line



TEHRIS XDR Platform is 100% compatible with

**MITRE ATT&CK**

Gartner, Market Guide for Mobile Threat Defense, January 2023, Market Guide for Network Detection and Response, December 2022, Hype Cycle for Endpoint Security, 2023, August 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and HYPE CYCLE is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Ask for a demonstration

TEHRIS XDR Platform

CONTACT US



business@tehtris.com  
 tehtris.com