

TEHTRIS ZTR is the TEHTRIS ZTNA solution that provides you with automatic incident response options and enhanced low-level detection capabilities.

USE CASES

- Threat detection
- Limitation of incidents
- Hunting threats
- Cybersecurity investigation
- Forensic investigation
- Reduction of the leading surface

ALL BENEFITS

- Reduction of MTTD (Mean time to detect)
- Reduction of MTTR (Mean time to respond)
- Integration with TEHTRIS XDR Platform
- Centralized and remote management (SaaS)
- Easy to deploy and use

TEHTRIS ZTR is a tactical Zero Trust Network Access solution that **provides real-time protection for all network flows** on client machines, and offers monitoring based on **metadata flow capture mechanisms** (NetFlow) and other protection features such as **automatic incident response** and **DNS protection**.

TEHTRIS ZTR is part of the **Zero Trust** security principle, which allows us to offer you **complete cyber monitoring**, both inside and outside your information system. With an optimized positioning in your network, TEHTRIS ZTR will be able to monitor both north/south flows (perimeter entries and exits) and east/west flows (lateral movements).

The **detection** part of TEHTRIS ZTR enables your security operations center to **identify normal or abnormal traffic elements**. Equipped with several modules, TEHTRIS ZTR bases its detections on signatures, and focuses its techniques on behavioral data. Not only that, our tool is also able to detect extremely varied suspicious elements, such as slow stealth scans. All flows are continuously being learned in order to perform advanced analyses and detect network anomalies.

Thanks to the **recording of metadata** in NetFlow mode, TEHTRIS ZTR offers the possibility to create log wells and carry out Forensic-type investigations as soon as it proves necessary.

Moreover, TEHTRIS ZTR is able to **react** thanks to an **automatic incident response engine**: TEHTRIS ZTR is the **first solution in the world to integrate SOAR in a ZTNA tool**. Where many ZTNA/SASE solutions require the use of a SIEM to be fully effective, TEHTRIS ZTR gives you direct access to a real **synergy between your security solutions**, as well as **powerful automation capabilities** thanks to its native integration with the TEHTRIS XDR Platform. As a result, if TEHTRIS ZTR listens to the circulating flows, studies them and looks for elements that could be used by a cyber attacker, it can also implement proportionate automatic actions, such as isolating machines, redirecting them to computer decoys (honeypots), blocking certain flows, and so on. This process offers the possibility of limiting your attack surface, in a proxy way, without even launching an operation on the machines concerned, which is very practical for all environments that cannot have an agent or local firewall, as in OT or IoT networks.

Choose a global and rigorous cybersecurity with TEHTRIS Zero Trust Response.

LEARN MORE ABOUT **TEHTRIS SOLUTIONS**

Test our products or contact us
<https://tehtris.com>
business@tehtris.com

— ZTNA's first global offer with automatic attack response —

KEY FEATURES

- ZTNA, VPN
- FWaaS (Firewall as a Service)
- DNS protection
- Detection via signatures
- Network Forensics
- Integrated SOAR

SUPPORTED PLATFORMS

- Cloud & On-Premise
- Windows
- Linux
- MacOS
- iPhone/iPad
- Android
- IT/OT

FEATURES

TEHTRIS ZTR offers you **DNS protection** features, such as anti-phishing, anti-spyware, anti-malware and anti-backdoor protection.

TEHTRIS ZTR includes **VPN protection** and a **Firewall as a Service** solution.

TEHTRIS ZTR allows you to **detect intrusions in real time** by analyzing network flows via signatures and behavioral analysis (NIDS).

TEHTRIS ZTR enables you to conduct **Forensic investigations** by performing tactical autopsies centered on network discussions using metadata from recorded streams to find out who talked to whom, when and how.

TEHTRIS ZTR **identifies the abnormal peaks** in network activity and analyses certain behaviors such as lateral movements.

TEHTRIS ZTR is **easy to maintain**: signature and threat databases are updated automatically and continuously via our **Cyber Threat Intelligence** (CTI).

TEHTRIS ZTR is a **virtual machine easily deployed** on the client hardware (VMware ESXi hypervisor), or in the TEHTRIS Cloud.

TEHTRIS ZTR is connected via the Internet to its **TEHTRIS XDR Platform** (centralization and monitoring of traces) and can be **remotely managed** by TEHTRIS in SaaS mode.

TEHTRIS ZTR can be deployed **on-premise**, in the **cloud**, or in **hybrid** mode.

LEARN MORE
ABOUT **TEHTRIS SOLUTIONS**

Test our products or contact us
<https://tehtris.com>
business@tehtris.com

<TEHRIS>

FACE THE UNPREDICTABLE

