

TelsyEDR

Endpoint Detection and
Response



L'evoluzione degli attacchi cyber in termini di frequenza e modalità nonché il processo di digitalizzazione in corso, espone le organizzazioni a vulnerabilità che indeboliscono i piani di continuità, la protezione dei dati, il monitoraggio delle infrastrutture critiche e, più in generale, il business.

TelsyEDR è rivolta alle organizzazioni che hanno necessità di migliorare la protezione delle postazioni di lavoro e dei server (endpoint) con strumenti che permettono di rilevare e bloccare automaticamente le minacce note o sospette.

Sicurezza avanzata per gli endpoint

TelsyEDR è una soluzione che integra il modulo di protezione antimalware con l'analisi del comportamento e delle attività che vengono eseguite sulle postazioni di lavoro e sui server (endpoint). È erogata dall'iSOC ed offre la possibilità di identificare, contenere e rimuovere le minacce note o sospette.

La soluzione lavora in duplice modalità:

PRE-EXECUTION Fornisce un primo livello di protezione grazie ad un motore anti-malware che difende da minacce note:

- **Discover** – scansione delle vulnerabilità con virtual patching;
- **Prevent e Block** – motore antimalware, sandbox e web filtering.

POST-EXECUTION Rileva e blocca in tempo reale gli artefatti e gli attacchi più avanzati:

- **Detect e Defuse** – analisi del comportamento, aggiornamento delle firme con feed di threat intelligence, blocco delle applicazioni corrotte, prevenzione dagli scenari di data loss;
- **Response** – visualizzazione della modalità dell'attacco e gestione degli endpoint.

Il **Security Operation Center** di Telsy interviene in:

- Supporto nella fase di installazione;
- Monitoraggio e raccolta di dati sulle attività svolte;
- Risposta automatica alle minacce identificate per rimuoverle o contenerle;
- Reporting settimanale.

Requisiti minimi

Windows XP SP2/SP3, 7, 8, 8.1, 10, and 11 (32-bit and 64-bit versions)

Windows Server 2003 SP2, R2 SP2, 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, and 2022

MacOS Versions: El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14), Catalina (10.15), Big Sur (11.x), and Monterey (12.x)

Linux Versions: RedHat Enterprise Linux and CentOS 6.x, 7.x, and 8.x, Ubuntu LTS 16.04.x, 18.04.x, 20.04.x server, 64-bit only Oracle Linux 6.x+, 7.7+, and 8.2+, Amazon Linux AMI 2 SuSE SLES 15.1

VDI Environments: VMware Horizons 6 and 7 and Citrix XenDesktop 7

I plus di TelsyEDR

- *Completo monitoraggio del pacchetto di endpoint*
- *Rapido rilevamento di attività malevoli*
- *Riduzione dei tempi di response*
- *Supporto ai fini della business continuity*



A TIM ENTERPRISE BRAND

telsy.com

contact@telsy.it

2023 © Telsy - Tutti i diritti riservati