Tim Guardian

La sicurezza delle connessioni

TIM ENTERPRISE

Contesto di mercato della Cybersecurity nel Mercato Enterprise

Il Problema dei Clienti oggi

Oggi l’80% del traffico Corporate viaggia ormai da/verso Internet.
Molte aziende sono costrette a raccogliere sulla sede principale tutto il traffico della periferia per applicare le policy di sicurezza , con sensibile incremento dei costi di gestione

Con il Cloud e lo Smart Working non esiste più un perimetro trusted nella rete privata. La protezione delle singole sedi e dei dipendenti in smart working è sempre meno efficace e gli investimenti salgono in modo poco sostenibile.

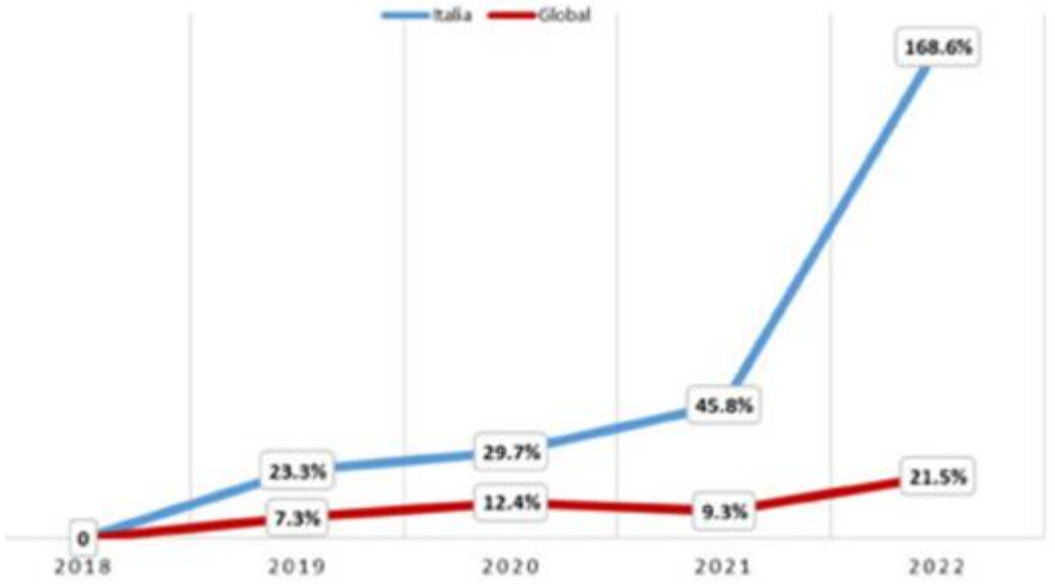
Il numero di attacchi in Italia è di 4 volte superiore al dato medio mondiale (clusit 2023).
E’ sempre più difficile proteggere tutti gli asset dell’azienda su architetture distribuite e in continua evoluzione.
La PMI e la PPAA sono i più bersagliati e vulnerabili.

Tim Guardian

Michele Vecchione, Marketing Enterprise Offerta Cybersecurity

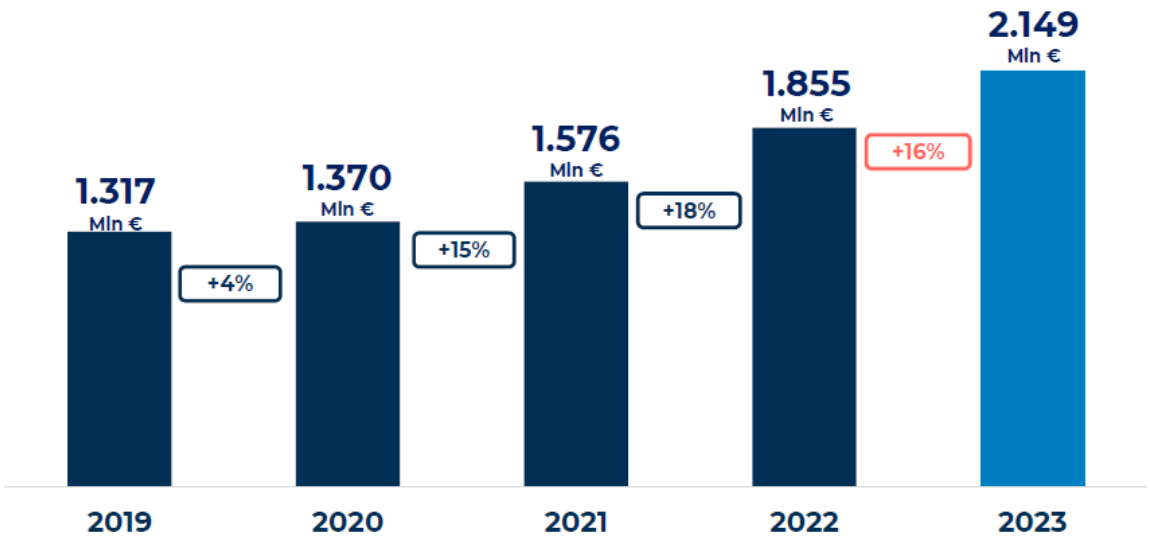
Scenario in Italia: Spesa Cyber ed Efficacia

Incidenti Cyber Italia vs Mondo



* Fonte Clusit

Spesa Cyber Italia



* Fonte Osservatorio Cybersecurity e Data Protection - PoliMI

- Cresce la spesa per la difesa ma crescono anche gli incidenti. C'è un chiaro problema di efficacia degli investimenti Cyber
- L'IT è sempre più frammentata, complessa e distribuita (v. Cloud), servono architetture di sicurezza che semplifichino la vita delle Imprese e della PPAA, rispetto alla semplice protezione perimetrale di una volta
- Gli attacchi vengono portati attraverso la Rete Internet e le risorse da proteggere sono spesso nativamente esposte su Internet, occorrono dei Security Service Edge (SSE) che rendano più sicure le connessioni di Rete e semplifichino l'applicazione di policy di sicurezza valide per tutti gli endpoint indipendentemente dalla connessione usata

Le principali minacce per l'Azienda

- Smartphone e Postazioni dei lavoro dei dipendenti possono essere infettate mediante Phishing, Malware o siti malevoli.
- Non sempre i dipendenti hanno la consapevolezza dei rischi Cyber e possono compromettere la sicurezza dell'azienda con errori umani

- Applicazioni, Database, Server contenenti dati sensibili possono essere compromessi da gang criminali sfruttando vulnerabilità SW (CVE) provocando perdita o l'esfiltrazione di dati vitali per il Business

- Alcuni Malware possono criptare le postazioni di lavoro e i dati aziendali; Il Business dell'azienda viene interrotto
- Normalmente l'azienda viene ricattata mediante richiesta di riscatto e minaccia di divulgazione dei dati carpiti.

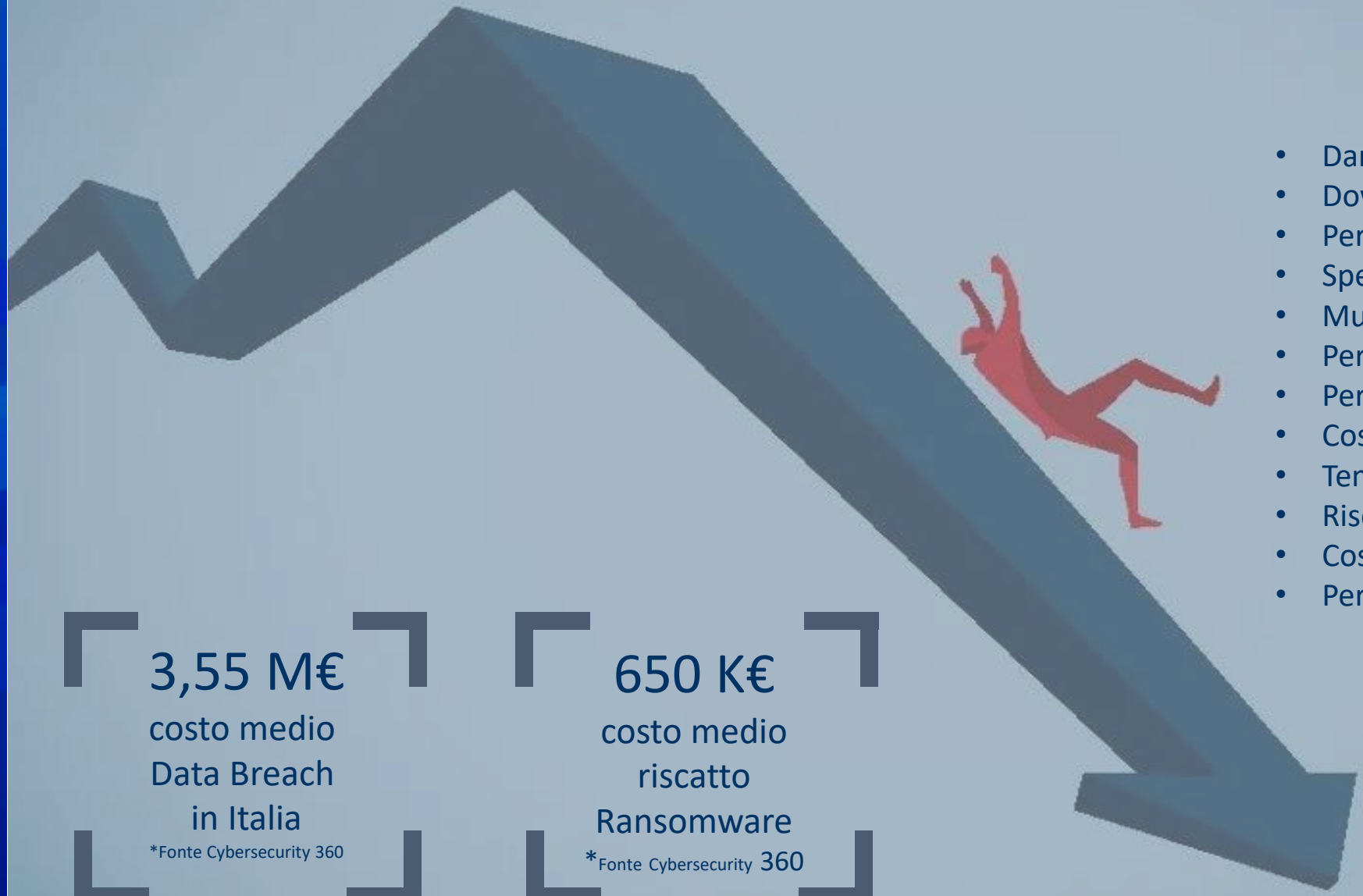
La morsa si va stringendo: Regole più severe sulla Security

- Entro il 17 Ottobre 2024 lo Stato Italiano deve recepire la normativa NIS 2.0 che impone standard di sicurezza elevati a molti settori industriali e enti pubblici e privati
- I fornitori dei soggetti NIS o della PPAA dovranno a loro volta garantire i medesimi standar ai loro clienti
- Sono previste sanzioni e ispezioni da parte dell'ACN per chi non adempirà alle obbligazioni per la gestione del rischio Cyber

- Entro il 2024 è prevista l'approvazione definitiva del Cyber Resilience Act EU, che imporrà ad ogni prodotto commercializzato con il marchio CE di rispettare specifici requisiti di sicurezza informatica

- Attraverso l'azione dell'ACN l'attenzione alla Cyber Security della PPAA sarà innalzata
- Nel DDL sulla sicurezza sono imposti obblighi specifici sulla resilienza cyber per gli appalti della PA centrale e Locale
- Certificazioni come la ISO 27001 2022 sulla Cybersecurity saranno abilitanti per partecipare a forniture pubbliche

Quanto costa trascurare la sicurezza?

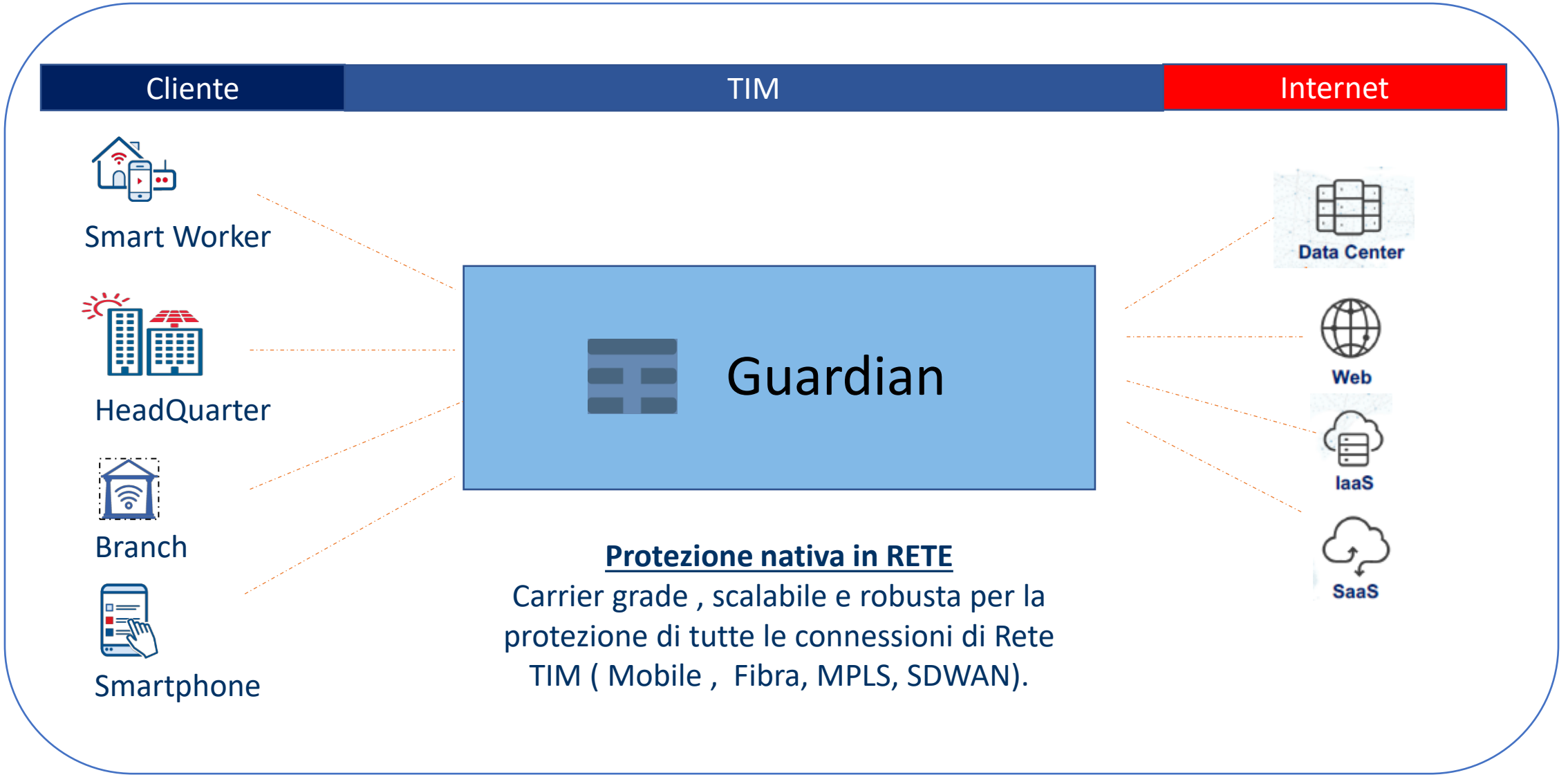


- Danni Reputazionali
- Downtime
- Perdite di Ricavi
- Spese Legali
- Multe o Sanzioni regolatorie
- Perdita di dati
- Personale fermo
- Costi di gestione dell'Incidente
- Tempo e Costo Analisi Forense
- Riscatto
- Costi di ripristino
- Perdita di relazioni commerciali

3,55 M€
costo medio
Data Breach
in Italia
*Fonte Cybersecurity 360

650 K€
costo medio
riscatto
Ransomware
*Fonte Cybersecurity 360

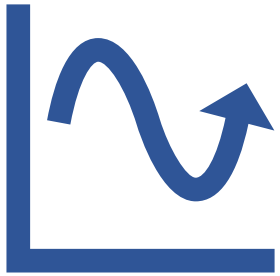
La Soluzione: TIM Guardian



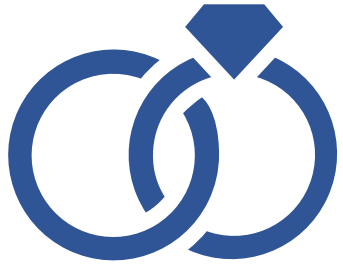
TIM Guardian – Versione «Silver»

Compra una linea protetta da TIM e metti i tuoi dipendenti e i tuoi dati al sicuro.

Offriamo per ogni SIM o Linea Fissa «Pacchetti» un upgrade di Sicurezza in modalità Op-out o estensione del contratto di connettività. Il Cliente ha un dashboard per vedere le minacce bloccate e impostare le policy di sicurezza.



Torniamo a far salire l'ARPU con servizi sui quali il cliente è sensibile e deve investire vista la crescita degli attacchi e delle minacce Cyber
Differenziamo la nostra Linea Mobile o Fissa dai competitor



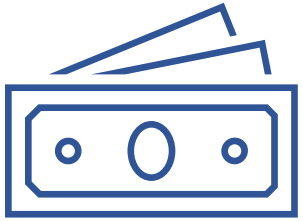
Si fidelizza il Cliente in quanto è più difficile commutare il servizio su un altro operatore

SEMPLICITA: ATTIVAZIONE ZERO TOUCH

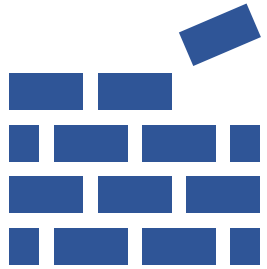
TIM Guardian – versione «Gold»

Compra una RETE protetta da TIM e metti le tue infrastrutture e i tuoi dati al sicuro.

Rendiamo intrinsecamente sicura l'uscita su internet di reti complesse per clienti Multisede che connettono Sedi aziendali, Cloud e Smart Worker (SDWAN, MPLS, Internet Profesional Profili)



Facciamo risparmiare il Cliente evitandogli di investire in sovradimensionamenti dovuti a centralizzare la raccolta del traffico nelle proprie sedi per l'uscita su Internet



Agiamo come Player COMPLETO con tutti i servizi necessari alla Digital Transformation: Rete, Cloud, Sicurezza,Applicazioni, PSN,…

A partire da 200€/mese

TIM Guardian – Profili di servizio

Una unica piattaforma in grado di proteggere singoli dispositivi mobili, single sedi connesse a Internet oppure tutta l'organizzazione indipendentemente dal tipo di tecnologia di accesso. O dalla collocazione delle risorse accedute

TIM Guardian

In base alla dimensione della Company, si possono scegliere varie opzioni di servizio

Lancio Maggio 2024

Silver Mobile

Offerta
Tim Guardian Mobile

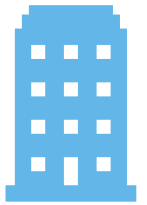
- DNS Sicuro
- Unified Threat Protection
- Dashboard
- URL Filtering
- Privacy e AD Blocker (Trackers)
- Opzione Moble Data Control

Lancio Luglio 2024

Silver Fisso

Offerta
Tim Guardian Siver Fisso

- DNS Sicuro
- Unified Threat Protection
- Dashboard
- URL Filtering
- Privacy e AD Blocker (Trackers)



Lancio Ottobre 2024

Gold

Offerta
Tim Guardian Gold

- DNS Sicuro
- Unified Threat Protection
- Malware Protection
- Secure Internet GW a banda garantita
- FW as a Service
- ZTNA per smart Workers
- MFA
- VPN con Indirizzi Privati dedicata

Descrizione della soluzione
Tim Guardian Mobile

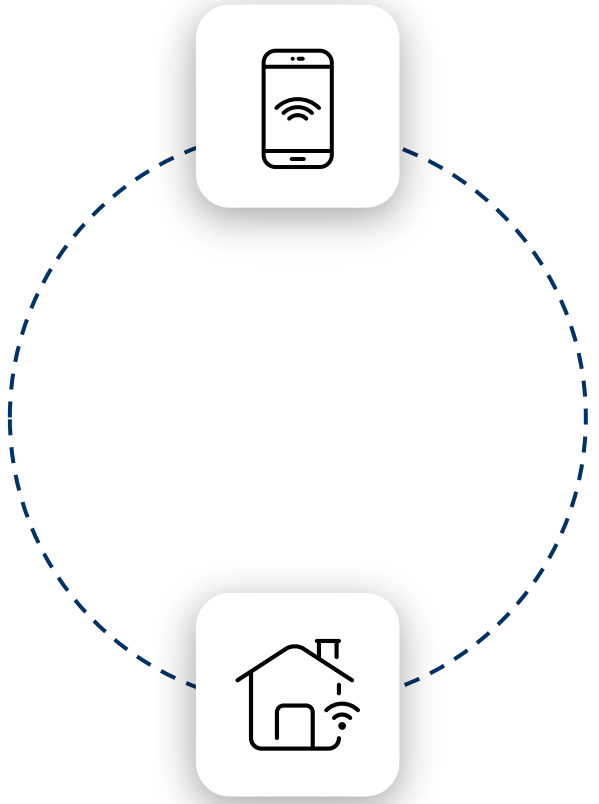
Proteggi e governa le tue connessioni aziendali

Soluzione Semplice
Progettata specificatamente per il mondo SME ed Enterprise.

Zero Touch
Protezione nativa nella rete senza software o configurazioni su Terminali o Apparati lato cliente

Sicurezza affidabile
Funzionalità avanzate di difesa contro le principali minacce informatiche.

Governance unificata
Linee fisse e mobili gestite da un'unica console, muti-tenant e self-managed.



TIM Guardian Mobile

La sicurezza del Mobile

Su tutte le SIM del cliente può essere attivata la protezione TIM Guardian direttamente nella rete mobile di TIM. Ogni pacchetto dati scambiato dallo smartphone verso Internet sarà protetto dal POP di sicurezza TIM con basi dati di Threat Intelligence e algortimi di Intelligenza Artificiale per bloccare automaticamente potenziali minacce Cyber. Inoltre il Cliente potrà impostare delle policy più o meno restrittive rispetto ai contenuti navigabii dai dipendenti e permettere o meno l'effetto dei Tracker sui siti WEB. Con una opzione aggiuntiva , Il cliente può restringere l'eventuale consumo di dati su siti non di interesse per il Business quando la SIM è in roaming in base alla Zona (EU o resto del mondo)

Zero Touch

L'amministratore del Cliente verrà abilitato su una WEB Application dove troverà automaticamente tutte le SIM su cui ha sottoscritto il contratto. Le SIM potranno essere anagrafate con I dati dell'organizzazione del cliente (Team, Nome dipendente, ..) e le policy potranno essere applicate su base organizzazione, team o singola SIM.

L'attivazione del servizio avviene automaticamente su base sottoscrizione e funziona sugli APN commerciali (ibox e wap) senza bisogno di cambiare APN o di installare SW a bordo dello smartphone.

Il Cliente potrà osservare su un dashboard tutte le minacce bloccate dalla piattaforma TIM Guardian e quelle inerenti I contenuti permessi o disiabilitati.

TIM Guardian Mobile

Target

Aziende con connettività Mobile TIM

Valore del servizio

Protezione dai rischi Cyber su tutto il traffico verso Internet

Perché TIM

Protezione nativa nella rete senza impatti sui dispositivi e sulla gestione

Perché Acquistare

i dispositivi mobili sono uno strumento di lavoro soggetto a infezioni , presentano vulnerabilità SW e rischi di intrusione e furto di dati.

Cosa puoi Fare

- Associare un solo dispositivo alla SIM
- Controllare il Traffico con algoritmi di Intelligenza Artificiale (UTI)
- Bloccare le singole categorie di URL pericolose
- Bloccare l'uso di applicazioni non utili ai fini lavorativi (es Tik Tok..)
. Bloccare i Tracker per la Privacy
- Avere una consolle con le statistiche e le impostazioni della tua azienda

+

Cosa puoi Aggiungere

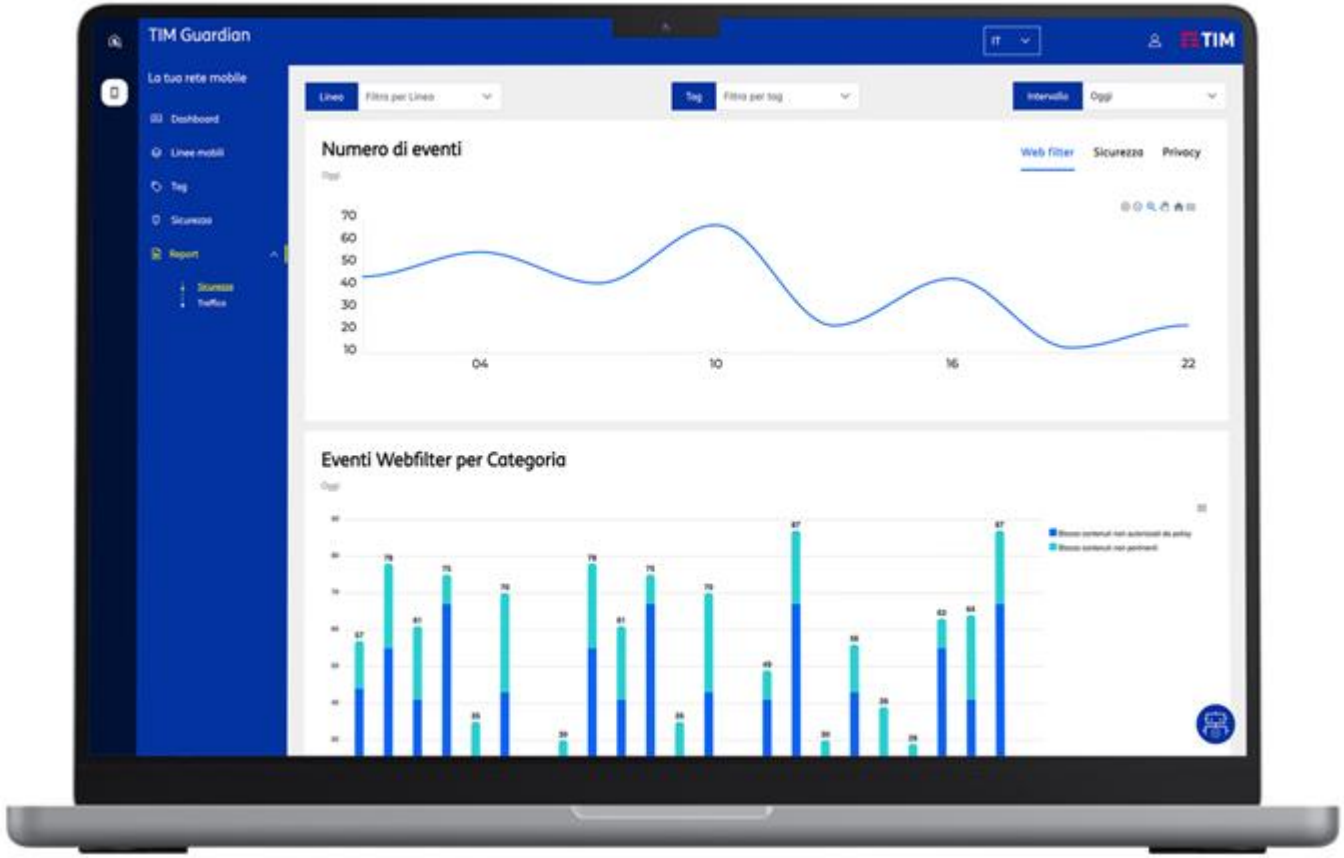
Mobile Data Control, una suite per il controllo del consumo dati sulle singole linee o Gruppi di Linee con policy applicabili sul Roaming UE e Resto del Mondo per disabilitare i consumi di applicazioni non importanti per il Business

TIM Guardian – Consolle di Gestione

Tim Guardian si configura come un'unica console per la gestione delle connessioni aziendali e la protezione dei dispositivi business da attacchi cyber.

Il cliente con le sue credenziali ai portali MyBusiness o Tim Business ha accesso a due sezioni principali, ciascuna dedicata a un aspetto specifico dell'infrastruttura aziendale:

- **La tua rete mobile**
- **La tua rete fissa**



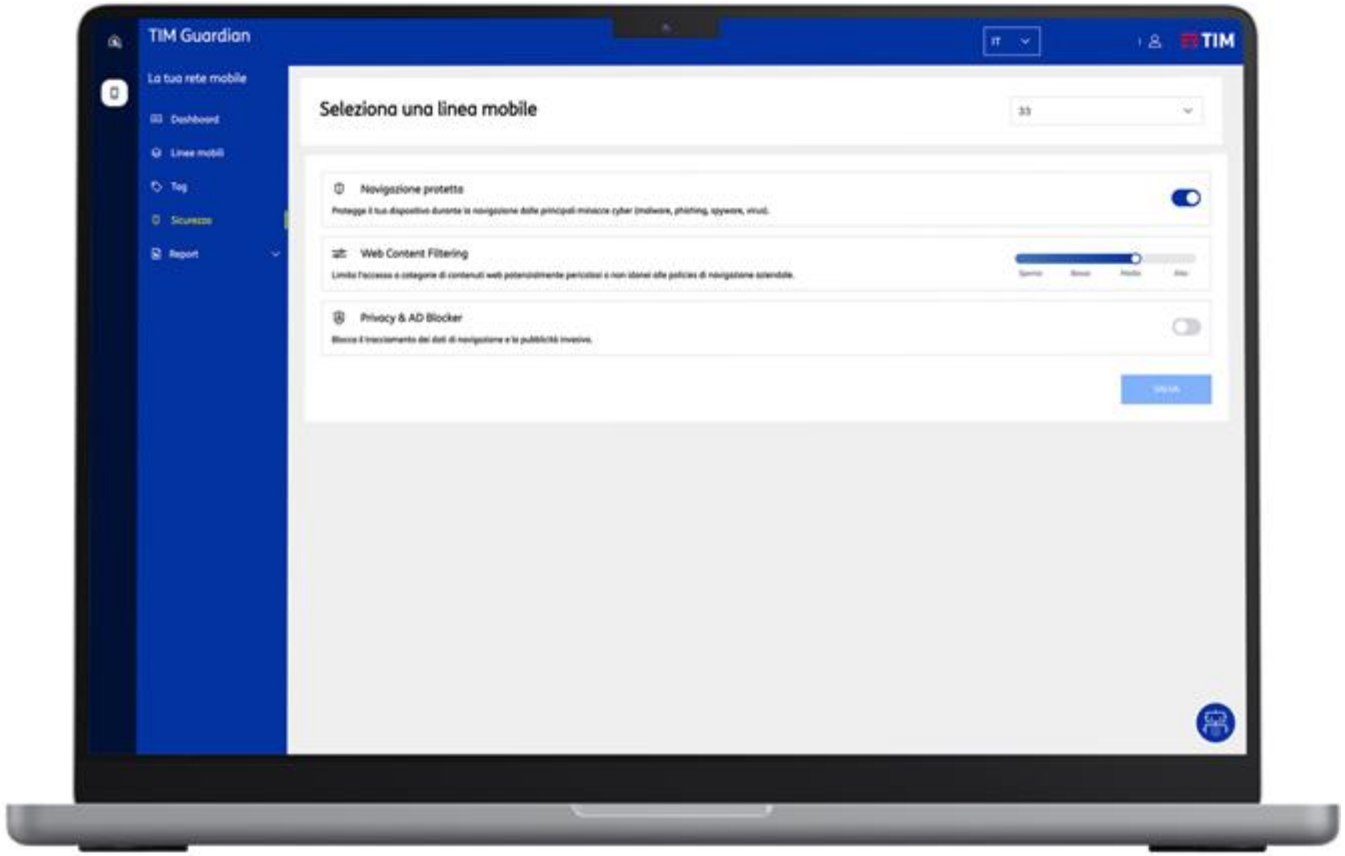
TIM Guardian – Configurazione delle Policy

Navigazione Protetta

Grazie a questa funzionalità il cliente può configurare security policy per ogni linea fissa e per ogni linea mobile censita a sistema, proteggendo tutti i dispositivi da malware, phishing, virus e botnet.

AD&Privacy Blocker

L'attivazione di questa funzionalità consente al cliente di bloccare i domini di web analytics che tracciano le attività online, i network pubblicitari e gli Ad server utilizzati per erogare contenuti di advertising invasivi.



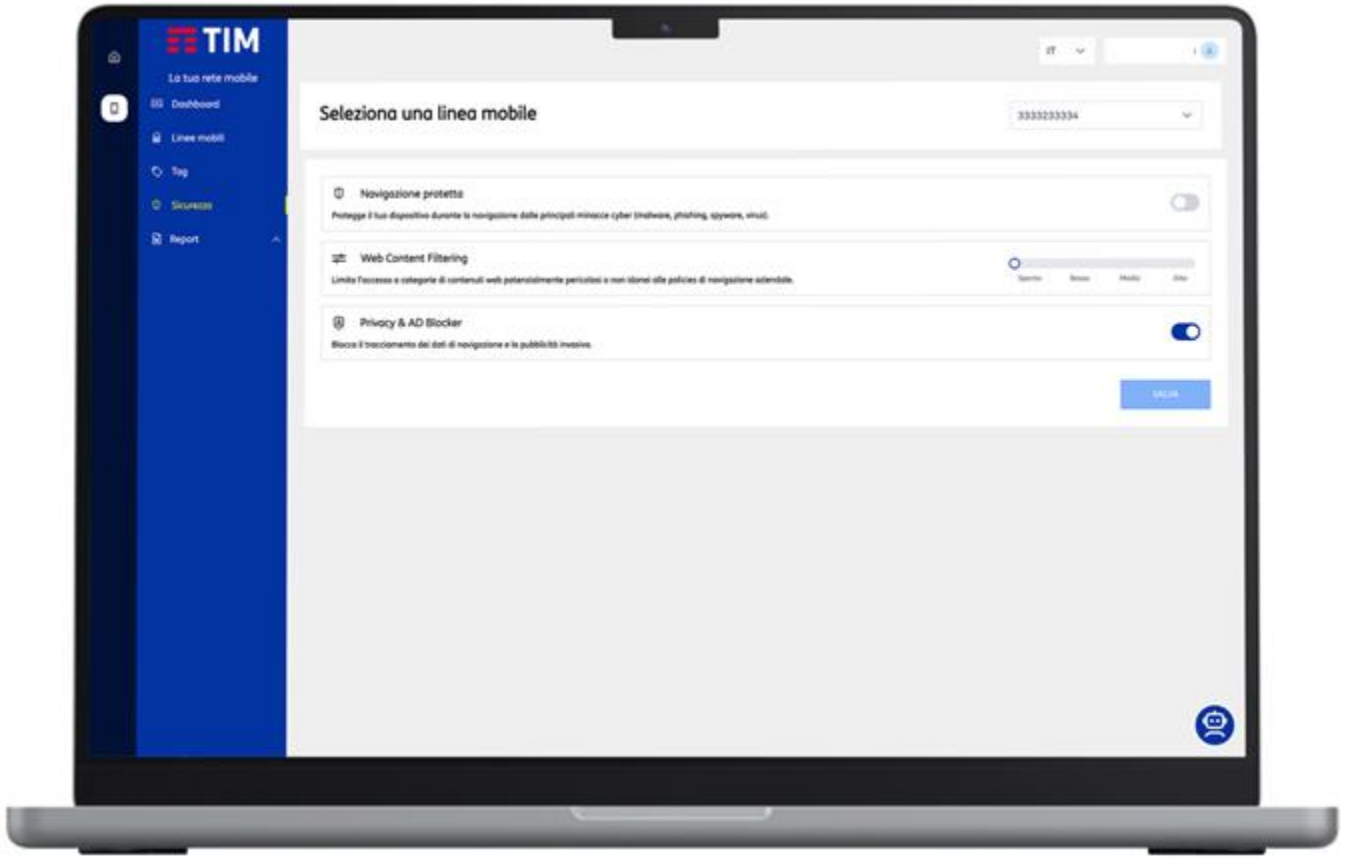
TIM Guardian – Configurazione delle Policy

Web Content Filtering

Attraverso questa funzionalità è possibile creare regole di web content filtering per le linee fisse e mobili, limitando l'accesso a tipologie di contenuti web potenzialmente pericolosi o non idonei alle policy di navigazione aziendali.

E' possibile impostare quattro diversi livelli di Web Content Filtering:

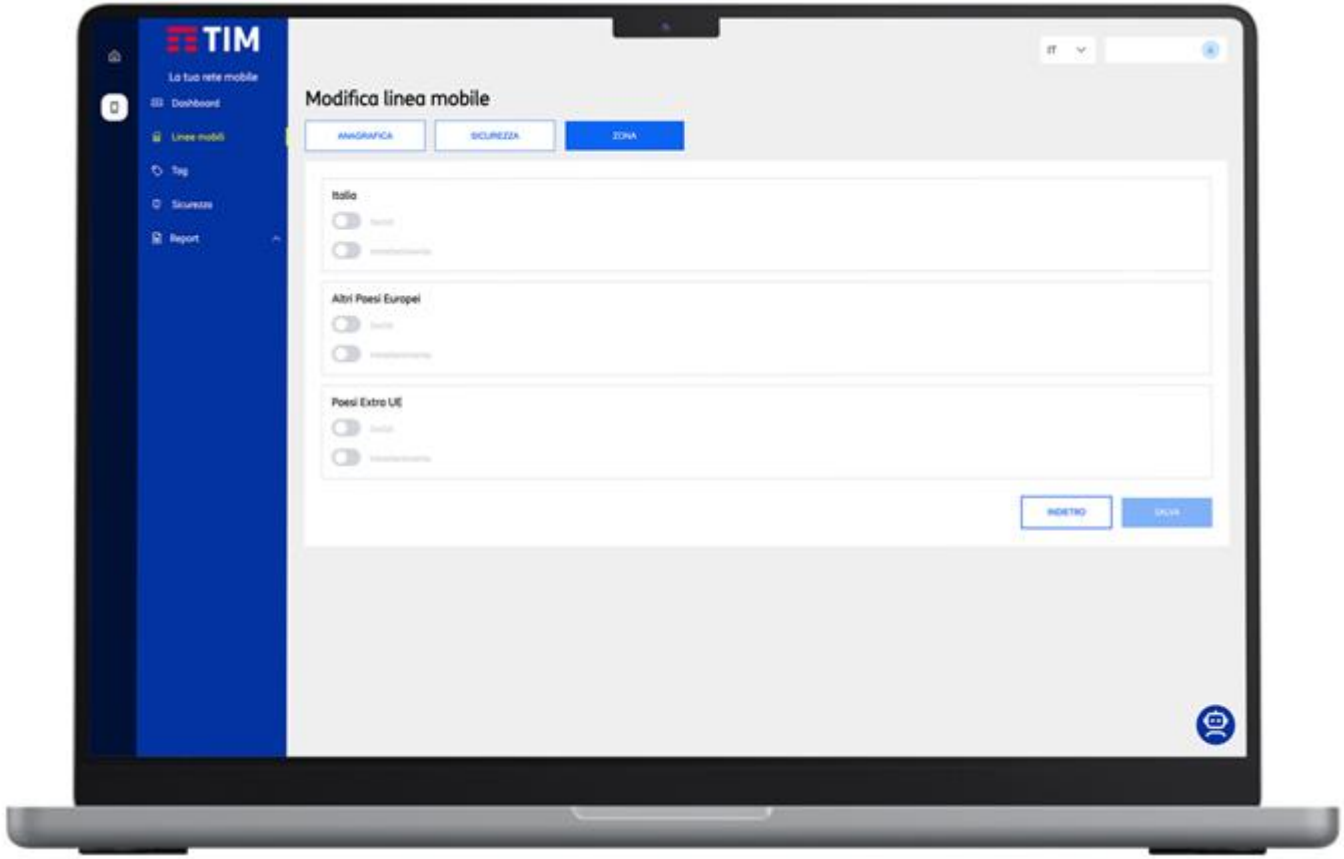
- **Livello Basso** *(default)*
  blocca l'accesso ai contenuti illegali e pericolosi, come quelli che offrono informazioni, metodi o istruzioni su azioni fraudolente o condotte illecite
- **Livello Medio**
  oltre a bloccare i contenuti precedentemente menzionati, il livello Medio impedisce l'accesso a contenuti ritenuti inappropriati per l'ambiente aziendale. Ciò contribuisce a mantenere un ambiente di lavoro professionale e conforme alle politiche aziendali
- **Livello Alto**
  questo livello, oltre a bloccare i contenuti precedentemente menzionati, inibisce l'accesso ai contenuti espliciti , garantendo un ambiente di navigazione sicuro e legale.
- **Spento**



TIM Guardian – Opzione Mobile Data Control Light

Grazie alla nostra soluzione, il Cliente può gestire in totale autonomia dei profili di blocco selettivo di categorie applicative per specifiche zone geografiche.

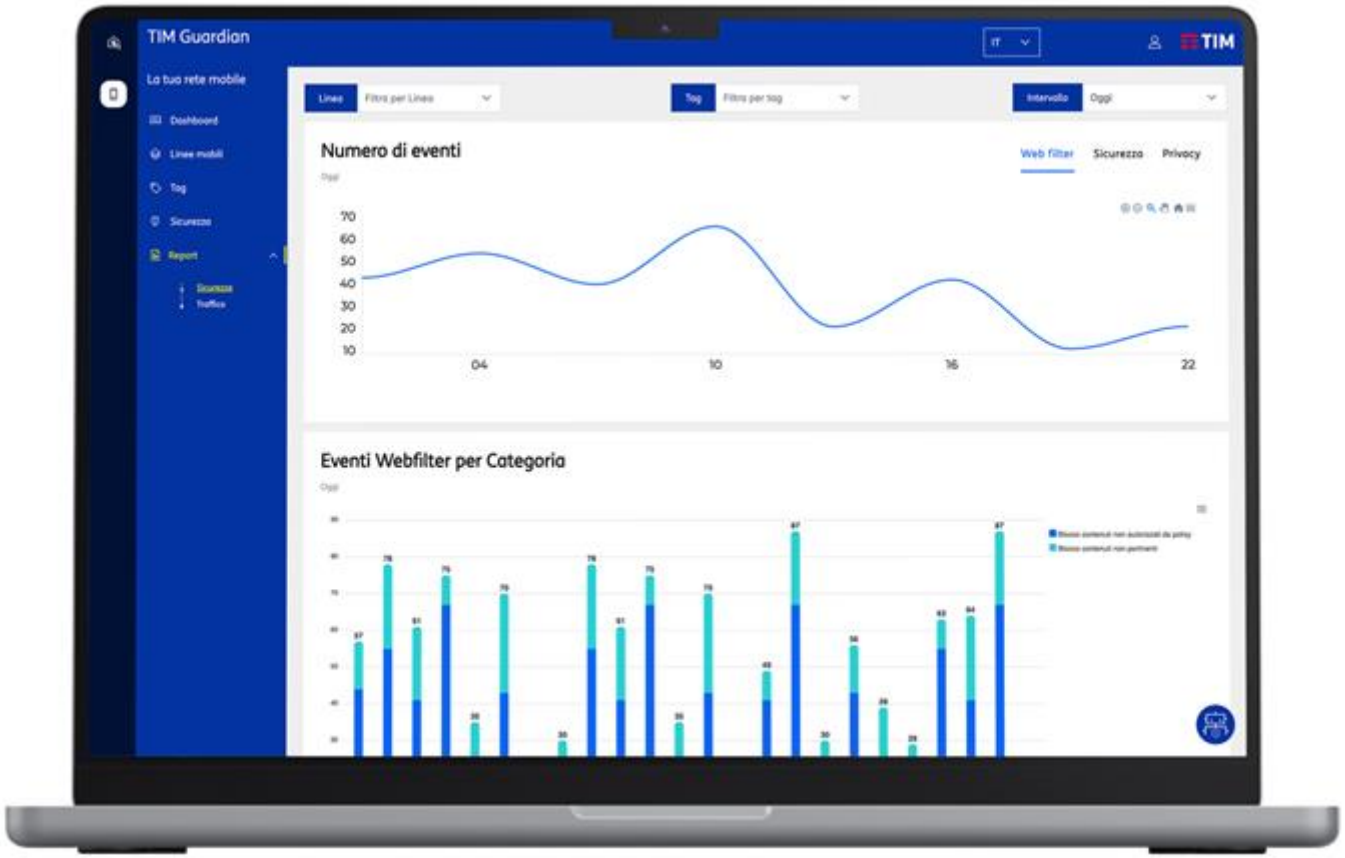
- Monitoraggio della percentuale dei consumi del traffico dati in tempo reale.
- Possibilità di introdurre policy di navigazione in base al profilo, andando ad inibire macro categorie di applicazioni per zone geografiche.



TIM Guardian – Reporting

Sicurezza

La sezione «Sicurezza» consente di avere accesso ai dettagli relativi a tutti gli eventi di sicurezza occorsi sulle linee mobili e fisse censite a sistema, con grafici specifici per tipologia di evento.



Traffico

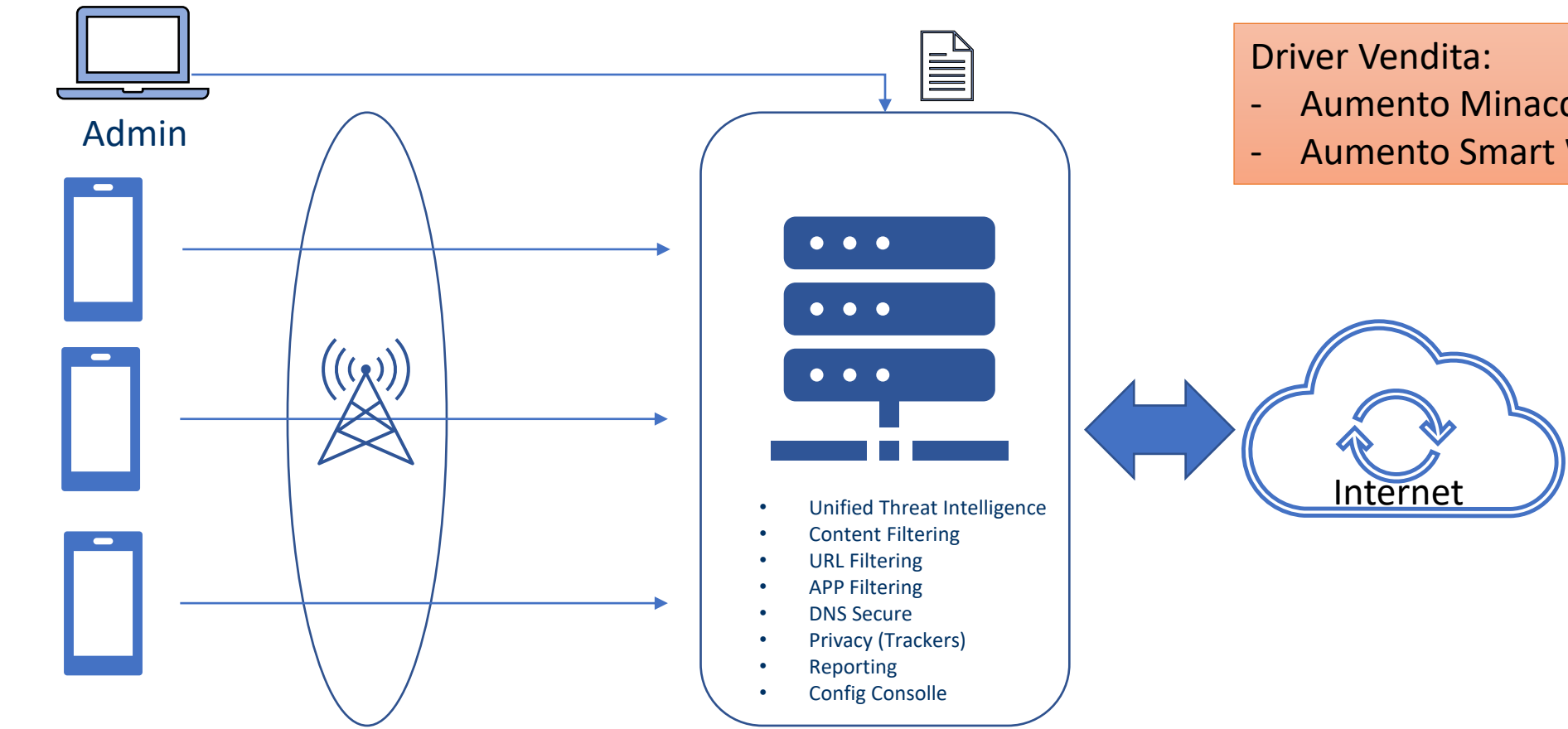
Attraverso la sezione «Traffico», il cliente ha visibilità completa sull'utilizzo dei dati di traffico in near real-time.

- Consumo percentuale dei dati per singola linea mobile in base alle categorie di applicazioni.
- Consumo percentuale dei dati per singola linea mobile in base a zone geografiche specifiche.

Scenari di applicazione della soluzione TIM Guardian

TIM Guardian Mobile

Protezione «in line» su Smartphone aziendali da minacce informatiche e siti malevoli



Driver Vendita:
- Aumento Minacce Cyber
- Aumento Smart Working

Protezione «*in-line*» su tutto il traffico delle proprie le Linee Mobili dalle minacce informatiche.
Consolle per l'amministratore del Cliente con pulsanti di configurazione e Reporting.