CASO STUDIO

Cyber Security · Gestione Unificata · EDR · Vulnerability Management · Monitoraggio h24

Tarros S.p.A.

Sicurezza informatica proattiva, centralizzata e finalmente sotto controllo

Tre strumenti di sicurezza scollegati, visibilità frammentata sugli asset aziendali e risposta alle minacce difficile da coordinare. Omnia ha ridisegnato la gestione della cybersecurity con un sistema unificato, monitorato h24 e pensato per proteggere la continuità operativa di una realtà logistica complessa.

-40%	**Zero**	**1**	**h24**
Tempi gestione	Violazioni dati	Pannello unico	Monitoraggio
100%	**EDR**	**VM**	**167**
Asset coperti	Protezione endpoint	Vulnerability mgmt	Dipendenti 2024

Il valore del progetto

Una cybersecurity più semplice da governare: meno console, meno attività manuali, più visibilità e una difesa proattiva allineata alla complessità operativa di Tarros.

OMNIA S.R.L
Via Salvatorelli, 49 Pistoia 51100 PT
P.IVA 01875190470

Email: contratti@omnia.srl
Pec: pec@pec.omnia.srl

www.omnia.srl
Tel. +39 0573 1936474

Registro imprese: PT-186939
Capitale Sociale: 12.000€

1. Il cliente: chi è Tarros S.p.A.

Tarros S.p.A. è una realtà ligure con sede a La Spezia, attiva nel settore del trasporto marittimo e per vie d'acqua interne. Il profilo aziendale evidenzia una struttura importante, con presenza anche su Genova e Napoli e un perimetro operativo legato a logistica, spedizioni e trasporto marittimo.

Il report aziendale indica per il 2024 un fatturato di 130,58 milioni di euro, 167 dipendenti e un capitale sociale di 1,05 milioni di euro. Per un'azienda di queste dimensioni, la continuità operativa e la protezione dei dati sono elementi centrali: un incidente di sicurezza può generare impatti immediati sulla catena logistica.

Cosa fa Tarros

- Trasporto marittimo, logistica e gestione di flussi operativi complessi.
- Presenza operativa distribuita, con sedi secondarie a Genova e Napoli.
- Processi che richiedono continuità, coordinamento e disponibilità dei sistemi IT.
- Un'organizzazione in cui la sicurezza informatica deve proteggere asset, dati e operatività quotidiana.

Perché la sicurezza è strategica

Nel mondo logistico la tecnologia non supporta soltanto l'ufficio: collega processi, persone, dati e flussi operativi. La protezione deve quindi essere continua, visibile e coordinata.

2. Scheda progetto

Cliente	Tarros S.p.A.
Sede	La Spezia (SP), Liguria
Settore	Spedizioni, logistica e trasporto marittimo - ATECO 50.00.00
Numeri	130,58 Mln euro fatturato 2024 · 167 dipendenti · 2 sedi secondarie
Esigenza	Unificare strumenti di sicurezza scollegati e rendere la difesa proattiva
Soluzione	Sistema unificato antivirus + EDR + vulnerability management con monitoraggio h24
Risultato	-40% tempi di gestione · zero violazioni · pieno controllo sugli asset
Servizi Omnia	Cyber Security · EDR · Vulnerability Management · Monitoraggio h24 · MSP ISO 27001

La richiesta iniziale

Passare da una sicurezza frammentata, distribuita su più strumenti, a un modello centralizzato e proattivo, in grado di dare visibilità immediata e ridurre i tempi di gestione.

3. La situazione iniziale

Tre strumenti. Zero integrazione. Troppo poco controllo.

Tarros gestiva la sicurezza informatica con strumenti separati: antivirus, EDR e vulnerability management lavoravano su console diverse, senza una vista unica e coordinata. La sicurezza era presente, ma difficile da leggere, interpretare e governare in modo rapido.

- Tre strumenti scollegati: console diverse, logiche diverse e maggiore complessità di gestione.
- Visibilità frammentata: per capire lo stato reale degli asset era necessario incrociare manualmente informazioni diverse.
- Risposta lenta alle minacce: identificare, valutare e intervenire richiedeva tempo prezioso.
- Gestione reattiva: il modello era più orientato a rispondere agli eventi che a prevenirli.
- Complessità aziendale elevata: asset distribuiti e processi logistici critici richiedevano un presidio più strutturato.

4. Gli obiettivi

Da sicurezza frammentata a difesa proattiva e coordinata.

- Unificare antivirus, EDR e vulnerabilità in un unico pannello di controllo.
- Passare da un modello reattivo a un presidio proattivo e continuo.
- Aumentare la visibilità sullo stato di sicurezza di asset, dispositivi e risorse.
- Ridurre i tempi necessari per identificare, valutare e rispondere agli eventi.
- Proteggere la continuità operativa in un contesto logistico complesso e distribuito.

5. La soluzione Omnia

Un sistema di sicurezza unificato, proattivo e sempre attivo.

Omnia ha progettato e implementato una gestione centralizzata della cybersecurity, riunendo gli strumenti esistenti in una piattaforma unica e aggiungendo un presidio continuativo. Il progetto ha trasformato la sicurezza da attività di emergenza a controllo costante e misurabile.

5.1 Assessment e mappatura degli asset

Analisi del parco macchine, degli strumenti esistenti e delle lacune operative, per costruire una soluzione aderente alla complessità reale di Tarros.

5.2 Centralizzazione in un unico pannello

Integrazione di antivirus, EDR e vulnerability management in una sola console, con visibilità immediata sullo stato di protezione degli asset aziendali.

5.3 Monitoraggio proattivo h24

Attivazione di un presidio continuo con alert in tempo reale, rilevamento automatico delle anomalie e risposta rapida prima che le minacce diventino incidenti.

5.4 Gestione continuativa degli aggiornamenti

Omnia segue aggiornamenti, verifica della postura di sicurezza e attività operative ricorrenti, liberando il team interno da attività manuali e ripetitive.

Elemento	Cosa è stato fatto
Antivirus	Protezione centralizzata degli endpoint e aggiornamenti continui.
EDR	Rilevamento comportamentale e supporto alla risposta rapida.
Vulnerability management	Scansioni, prioritizzazione e gestione delle vulnerabilità.
Monitoraggio h24	Alert in tempo reale e presidio proattivo Omnia.

5.5 Le fasi del progetto

Il percorso è stato impostato per ridurre la complessità senza interrompere l'operatività: prima la fotografia dell'esistente, poi la centralizzazione degli strumenti e infine il presidio continuativo.

- Analisi e progettazione: mappatura degli asset, delle console e dei flussi di gestione esistenti.
- Integrazione degli strumenti: antivirus, EDR e vulnerability management ricondotti a un'unica vista.
- Attivazione del monitoraggio: presidio h24, alerting e controllo proattivo degli eventi.
- Governance continuativa: aggiornamenti, verifica degli asset e gestione delle attività ricorrenti.

Il valore del pannello unico

La centralizzazione riduce il tempo speso a passare da un sistema all'altro: ogni asset, evento e criticità può essere valutato da una vista coordinata.

Security dashboard - visione operativa

Modulo	Stato / valore per Tarros
Antivirus centralizzato	Protezione endpoint e aggiornamento automatico.
EDR	Rilevamento comportamentale e risposta agli eventi.
Vulnerability management	Scansione continua, priorità e remediation.
Monitoraggio h24	Alert in tempo reale e presidio Omnia.
Asset coperti	Visibilità completa e aggiornata sul parco macchine.

6. I risultati ottenuti

Meno complessità. Più controllo. Zero violazioni.

Il progetto ha trasformato la gestione della sicurezza IT su tre livelli: operativo, organizzativo e di controllo. La sicurezza non è più distribuita su strumenti scollegati, ma governata da un sistema unico e proattivo.

-40%	Zero	1	h24
Tempi gestione	Violazioni dati	Pannello unico	Difesa proattiva

- Riduzione dei tempi di gestione: meno passaggi manuali tra console diverse.
- Zero violazioni dei dati dall'attivazione del sistema unificato.
- Visione immediata e completa su antivirus, EDR e vulnerabilità.
- Passaggio da gestione reattiva a difesa proattiva h24.
- Controllo aggiornato degli asset aziendali e delle criticità aperte.
- Team IT più libero dalle attività operative ripetitive.

7. La testimonianza

"Ora abbiamo tutto sotto controllo, in un'unica interfaccia. La sicurezza è diventata proattiva, semplice da gestire e finalmente all'altezza della complessità aziendale."

Mauro Solinas - Corporate External Relations and Brand Director, Tarros S.p.A.

8. Perché Omnia

Omnia S.r.l. è un Managed Service Provider e WISP toscano specializzato in cybersecurity, connettività, comunicazione unificata e infrastrutture IT. L'approccio parte sempre dall'operatività del cliente: meno complessità, più controllo e continuità nel tempo.

- Metodo: assessment reale prima della proposta tecnica.
- Centralizzazione: meno console e più visibilità per chi gestisce la sicurezza.
- Presidio: monitoraggio h24 e risposta rapida agli eventi.
- Continuità: cybersecurity progettata per proteggere processi critici e business operativo.
- Competenza: un partner MSP certificato ISO 27001, vicino e continuativo.

Il messaggio del progetto

Quando l'azienda cresce e gli asset diventano distribuiti, la sicurezza non può restare frammentata. Serve una governance unica, leggibile e sempre attiva.

Come gestisce la sicurezza la tua azienda?

Parliamo della postura di sicurezza IT della tua organizzazione. Nessun impegno: un confronto concreto per capire dove ci sono lacune e cosa si può fare.

Omnia S.r.l. · Via L. Salvatorelli 49, 51100 Pistoia (PT) · +39 0573 1936474 · www.omnia.srl

MSP / WISP certificato ISO 9001 · ISO 14001 · ISO 27001