TD SYNNEX

Servizi di security

Superare la sfida della compliance con un partner affidabile al tuo fianco

6 Giugno 2025

Webinar

Federico Frosini – Business Development Manager – TD SYNNEX
Andrea Pezzoni – Security Presales Specialist – TD SYNNEX
Michele Sasso – BU Servizi – TD SYNNEX
Pierpaolo Travaglini – BU Servizi – TD SYNNEX

I Servizi sono un’opportunità

$1.7 Miliardi di opportunità

Il mercato dei Servizi crescerà in maniera significativa, con un tasso di 8% YoY fino al 2028

Crescita guidata dalla tecnologia

L’adozione di tecnologie sempre più complesse e verticali, **cloud computing, security e data and AI** alimentano la crescita.

A questi si aggiungono le normative e il tema della compliance

Verso il servizio

I servizi del ciclo di vita del prodotto, i servizi professionali forniti dai partner e la rivendita di servizi pacchettizzati crescono a un tasso del 150-200% rispetto all'hardware

Aumento del budget servizi

I Servizi sono arrivati a rappresentare il 51% del budget IT nel 2024

Sources: TD SYNNEX’s Direction of Technology Ecosystem Report 2022|2023 | Mordor’s IT Services Market Share and Size 2023 | Gartner’s Global IT Spending Forecast

Le sfide degli MSP

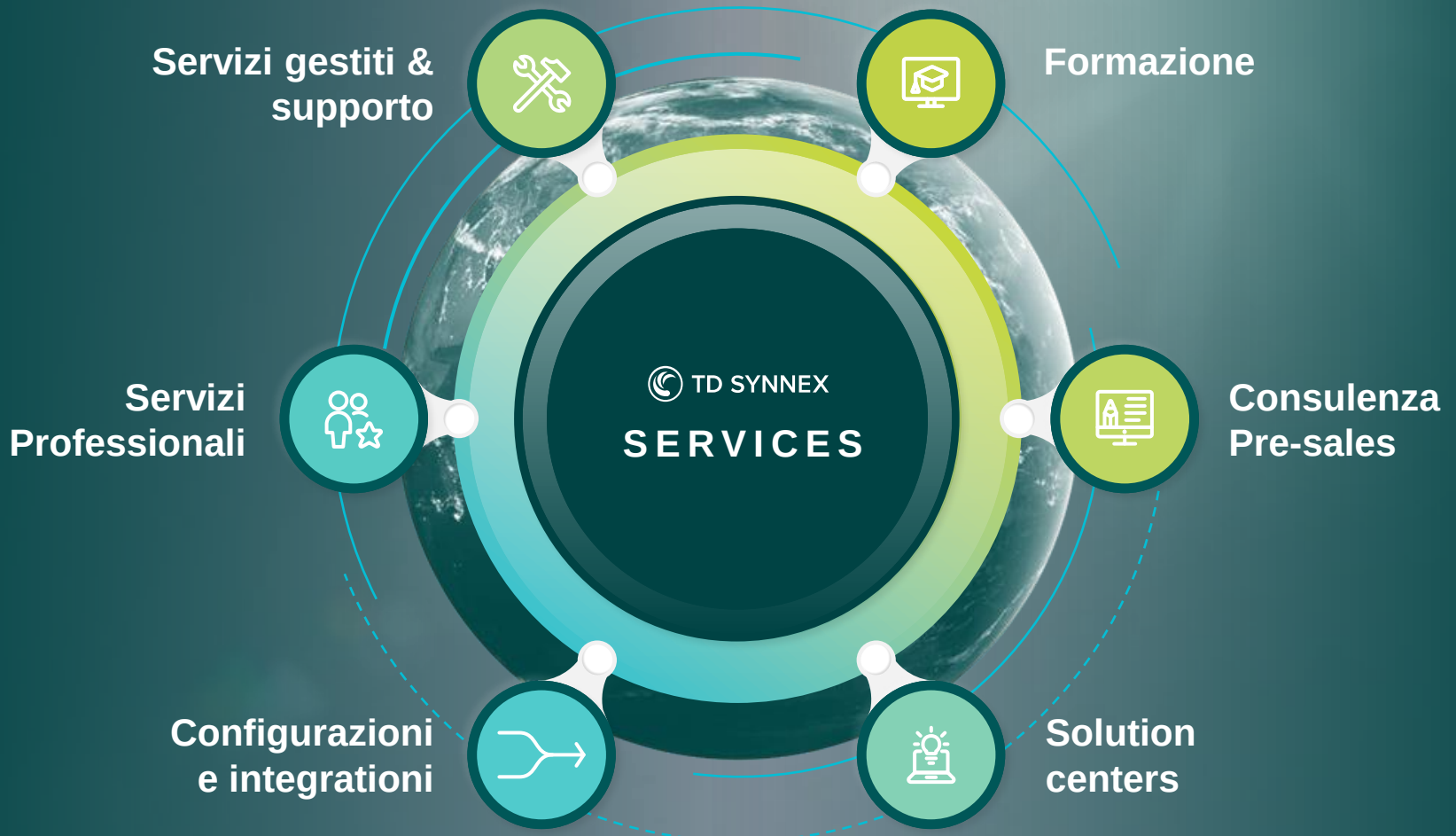
Come posso rimanere aggiornato con un mercato in evoluzione?

Come posso estendere le competenze?

Come posso aumentare l'offerta senza un piano di investimenti iniziale?

TD SYNNEX – Servizi in sintesi

Chiudere il gap tra la complessità e il risultato



Hybrid Cloud / Data & Applications / Networking / Security

Perché i servizi di TD SYNNEX?

Aumentare le skill

Ottenere di più, installare in modo più rapido ed efficace e competere in segmenti di business più ampi senza aumentare il numero di dipendenti a tempo pieno.

Aumentare l’offerta

Migliorare rapidamente le capacità e competenze ottenendo un accesso immediato a servizi, risorse e strumenti per colmare le lacune dei servizi.

Aumentare la profittabilità

Aumentate i margini di profitto al di là delle vendite tradizionali di prodotti, fornendo un ulteriore valore aggiunto ai vostri clienti.

Unica interfaccia

Creare maggiore efficienza in ogni fase del processo del ciclo di vita consolidando i servizi sotto un unico fornitore di servizi fidato, collaudato ed esperto.

I nostri Servizi sono stati studiati per essere totalmente legati al canale

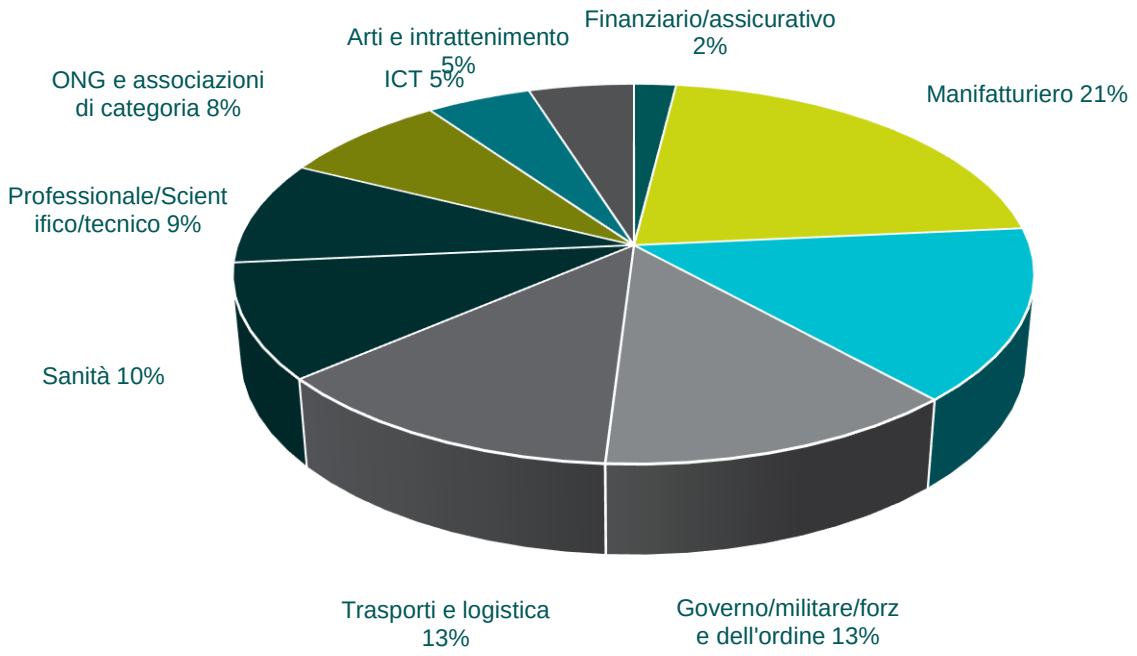
I MegaTrend sel settore

Cybersecurity come driver di crescita:

- nel 2024 si è registrato un aumento del +60% degli attacchi informatici gravi rispetto agli anni precedenti, di cui il 40% degli incidenti totali ha colpito principalmente enti pubblici e sanità.

[Fonte: Rapporto Clusit – Associazione Italiana per la Sicurezza Informatica]

- La Spesa in cybersecurity in Italia è prevista superare i 2 miliardi di euro nel 2025, con una crescita del +12% rispetto all'anno precedente. standard dei grandi Player.



Approfondimento NIS2

Normativa NIS2
Recepita in italia nel 2024, prevede obblighi sulla gestione del rischio in CyberSecurity e l'istituzione di Policies molto rigide in tema di rilevamento, identificazione e comunicazione degli *incident*
Le scadenze per l'adeguamento sono:

- Entro il 31 luglio 2025: avviata la fase 2, con obblighi di comunicazione soggetti incaricati del punto di contatto
- Entro il 1° gennaio 2026: Adeguarsi agli obblighi gestiOne incidenti e aggiornamento informazioni c/o ACN.
- Entro 31 ottobre 2026: Adeguarsi agli obblighi sugli organi di amministrazione e direttivi per la gestione dei rischi.

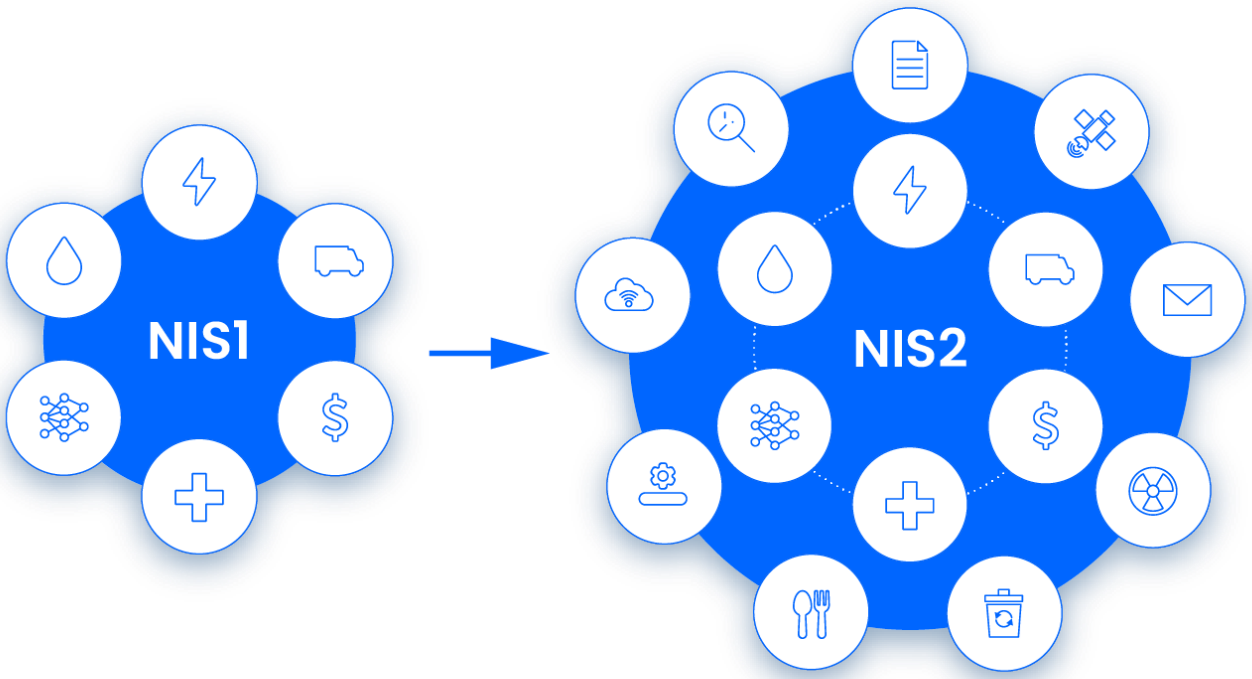
Le sanzioni per la non conformità possono raggiungere fino al 2% del fatturato annuo per le entità essenziali, e fino all'1,4% del fatturato annuo per le entità importanti

Identificazione dei soggetti interessati

Entità Essenziali	Entità Importanti
Energia	Poste
Trasporti	Gestione dei rifiuti
Finanza (DORA)	Industria chimica
Pubblica Amministrazione	Ricerca
Salute	Alimentare
Aerospaziale	Manifattura per entità Essenziali
Distribuzione e gestione acque	Provider digitali
Infrastrutture digitali	
Fatturato >50M €	Fatturato >10M €
Dipendenti >250	Dipendenti >50

Un'entità può comunque essere considerata "essenziale" o "importante" anche se non soddisfa i criteri di fatturato e numero dipendenti

A chi si rivolge



Energy Essential Entity	**Health** Essential Entity	**Transport** Essential Entity	**Finance** Essential Entity	**Water Supply** Essential Entity
Digital Infrastructure Essential Entity	**Public Administration** Essential Entity	**Digital Providers** Important Entity	**Postal Services** Important Entity	**Waste Management** Important Entity
Space Essential Entity	**Foods** Important Entity	**Manufacturing** Important Entity	**Chemicals** Important Entity	**Research** Important Entity

NIS2… Fase 2?

1. **GOVERNANCE**

   Composizione degli organi di amministrazione e direzione:

2. **IT INFRASTRUCTURE**

   Indirizzi IP pubblici e statici in uso / Elenco degli IP assegnati all'organizzazione

   Nomi di dominio utilizzati o registrati

3. **CERTIFICAZIONE**

   Accordi volontari di condivisione info sulla cybersicurezza (CERT, CSIRT, condivisione IOC, ecc.)

4. **PUNTO DI CONTATTO**

   Verifica Punto di Contatto e presenza di eventuale sostituto

Servizio NIS2 Compliance

COSA OFFRIAMO?

Un **pacchetto** pensato per l'adeguamento alla Direttiva Europea, per garantire conformità legale ed operativa delle aziende

GAP ANALYSIS NORMATIVA

Verificare le procedure organizzative interne per la gestione di potenziali rischi di cybersicurezza, intervenire con azioni formative al Board direttivo, indicare il set documentale idoneo a dimostrare di possedere un modello nella gestione dei rischi.

GAP ANALYSIS TECNOLOGICA

Identificare e mappare l'infrastruttura IT, OT, ICS/SCADA, effettuare Vulnerability assessment (VA) su sistemi, apparati di rete, endpoint, server, firewall,, al fine di elaborare un piano tecnico per la conformità e remediation

Servizio NIS2 Compliance

GAP ANALYSIS NORMATIVA

MACRO FASI:

1.	**GOVERNANCE CYBERSECURITY :**	Organigramma, deleghe di funzioni risultanti dallo statuto o da atti notarili
2.	**PROCEDURE CYBERSECURITY :**	Procedure formalizzate e prassi operative interne
3.	**CONTROLLO DELLA SUPPLY CHAIN:**	Mappatura Fornitori, criteri selezione, clausole e tutele contrattuali
4.	**FORMAZIONE AL BOARD DIRETTIVO:**	Trasferire gli elementi conoscitivi obbligatori della norma NIS 2
5.	**NIS 2 COMPLIANCE PROGRAM:**	Predisposizione di un piano di Remediation

Tempo totale stimato: 30- 35 giorni

Servizio NIS2 Compliance

GAP ANALYSIS NORMATIVA

- Fase 1, 2, 3: RIUNIONE DI PROGRAMMAZIONE – 5/7 giorni
- Fase 1, 2, 3:: INTERVISTE E RACCOLTA DOCUMENTALE – 12/15 giorni
- Fase 4: FORMAZIONE AL BOARD – 1/3 giorni
- Fase 5: PRESENTAZIONE NIS2 COMPLIANCE PROGRAM – 10 giorni

Tempo totale stimato: 30- 35 giorni

Servizio NIS2 Compliance

GAP ANALYSIS TECNOLOGICA

MACRO FASI:

1. **ASSESSMENT STRUTTURALE:** Inventario di asset e Mappatura architetturale (rete, segmentazioni, flussi dati)
2. **DEPLOY STRUMENTI :** Installazione/configurazione agent e/o scanner, raccolta log da remoto
3. **NIS 2 & CONTROLLI SICUREZZA:** Identificazione dei controlli implementati e Vulnerability Assessment
4. **GAP REMEDIATION PLANNING:** Elaborazione Piano di remediation, roadmap tecnica dettagliata
5. **DEBRIEFING E HANDOVER:** Condivisione delle buone pratiche e consegna piano di remediation

Servizio NIS2 Compliance

GAP ANALYSIS TECNOLOGICA

- Fase 1: **ASSESSMENT STRUTTURALE** – 3/4 giorni
- Fase 2: **DEPLOY STRUMENTI AUTOMATIZZATI** – 1/2 giorni
- Fase 3: **NIS 2 & CONTROLLI DI SICUREZZA** – 4/5 giorni
- Fase 4: **GAP REMEDIATION PLAN** – 4/5 giorni
- Fase 5: **DEBRIEFING E HANDOVER** – 1/2 giorno

Tempo totale stimato: 18-21 giorni

TD SYNNEX

“The most effective way to do it, is to do it.”

Amelia Earhart

Q&A

13 GIUGNO: Affidare le chiavi della sicurezza ad un partner fidato

20 GIUGNO: Sonicwall CSE – ZTNA fatto semplice

27 GIUGNO: Nella mente di un hacker – Un attacco Bruteforce

https://events.tdsynnex.it/cyber-unit-missione-protezione/

TEAM SECURITY: security.it@tdsynnex.com
TEAM SERVIZI: serviziprofessionali-ita@tdsynnex.com