Ripensare la sicurezza aziendale partendo dai dispositivi

Le ultime soluzioni e normative in materia di sicurezza degli endpoint

Webinar

Andrea Pezzoni – Security Presales Specialist – TD SYNNEX
Mattia Alushi – Technical Presales Microsoft Devices – TD SYNNEX
Denis Sacchi – Presales & Solution Architect Microsoft – TD SYNNEX

Agenda

11.00 – 11.05 Benvenuto e introduzione

11.05 – 11.10 La fine del supporto di Windows 10: l’importanza degli aggiornamenti

11.10 – 11.15 La sicurezza dell’endpoint

11.15 – 11.20 I vantaggi della sicurezza su Windows 11 Pro

11.20 – 11.30 NIS 2: la normativa europea per la Sicurezza

11.30 – 11.50 Patch Management e utilizzo di Microsoft Intune

11.50 – 12.00 Conclusioni e Q&A

Quattro motivi per passare a nuovi dispositivi

I dispositivi obsoleti aumentano la vulnerabilità

I dispositivi più datati possono essere meno sicuri e, con la fine del supporto per Windows 10 il 14 ottobre 2025, il costo per mantenere la protezione potrebbe arrivare fino a 61 dollari per dispositivo. Rimandare la modernizzazione al domani potrebbe costare caro alla tua azienda già oggi.

Restare competitivi

I nuovi dispositivi con Windows 11 Pro, alimentati dai processori Intel® Core™ Ultra e Intel vPro®, sono progettati per offrire le più recenti funzionalità avanzate dall'IA, migliorando insight ed efficienza.

Controllare i costi

I dispositivi più datati richiedono più tempo per la manutenzione, possono esporre a costosi rischi per la sicurezza e influire negativamente sulla produttività e sulla soddisfazione dei dipendenti.

Il tempo sta per scadere

"Le organizzazioni impiegano fino a 440 giorni per completare la transizione dell'intero parco PC. Con la fine del supporto per Windows 10 il 14 ottobre 2025, il conto alla rovescia è già iniziato.

Il supporto per Windows 10 terminerà il 14 ottobre 2025.[3]

99.7%

Compatibilità delle app con programmi attivi per risolvere i problemi senza costi aggiuntivi. [12]

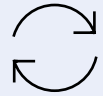
[3]Microsoft, Windows 10 EOS with Windows 11, Windows 365, and ESU, 2023.
[12]Commissioned study delivered by Forrester Consulting "The Total Economic Impact™ of Windows 11 Pro Devices", December 2022. Note, quantified benefits reflect results over three years combined into a single composite organization that generates $1 billion in annual revenue, has 2,000 employees, refreshes hardware on a four-year cycle, and migrates the entirety of its workforce to Windows 11 devices
[22]Microsoft, When to use Windows 10 Extended Security Updates, 2024.

Sistemi di Sicurezza dei dispositivi

La sicurezza è una priorità fondamentale per qualsiasi organizzazione qui vediamo gli strumenti di sicurezza disponibili, suddivisi in due categorie: le funzionalità esistenti su Windows 10 ma migliorate su Windows 11 e le nuove funzionalità.

Sistemi di Sicurezza già presenti su Windows 10 e migliorati

- **Security by default**
- **BitLocker and BitLocker-to-Go**
- **Windows Hello for Business**
- **Multifactor authentication**



Sistemi di Sicurezza nuovi per Windows 11

- **Protezione delle applicazioni—Smart App Control**
- **Rilevamento della presenza**
- **Protezione avanzata contro il phishing**

Smart App Control

Smart App Control è una funzionalità di sicurezza introdotta in Windows 11 che blocca automaticamente le applicazioni non sicure o non attendibili prima che possano essere eseguite sul sistema.

🔐 **Come funziona:**

- Utilizza modelli di **intelligenza artificiale** per decidere se consentire o bloccare l'esecuzione.
- Opera in **modalità attiva o di valutazione.**
- Garantisce un'esperienza **fluida** per l'utente, senza **popup invasivi.**

Rilevamento della presenza

Il rilevamento della presenza è una funzionalità che utilizza sensori integrati nel dispositivo per determinare se l'utente è fisicamente presente davanti al PC.

🔐 **Come funziona:**

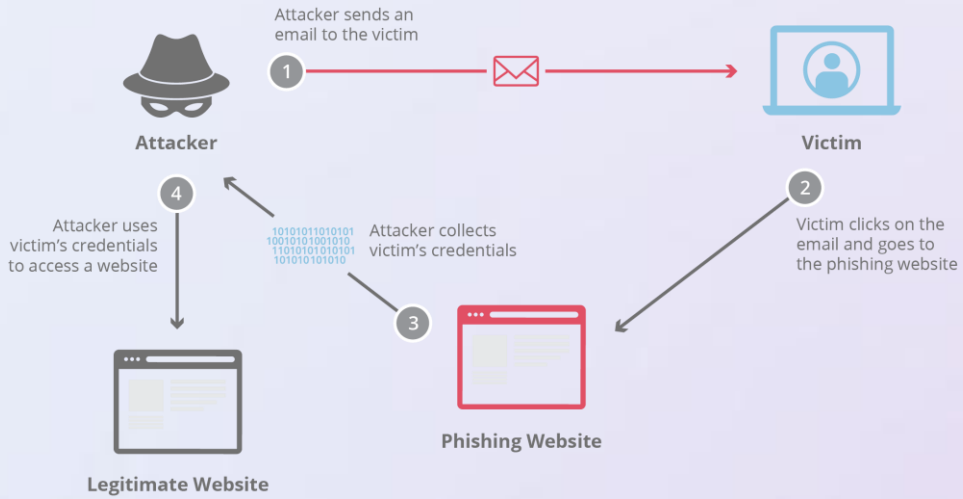
- Se l'utente **si allontana**, il sistema può **bloccare automaticamente lo schermo**.
- Se l'utente **si avvicina**, il PC può **attivare lo schermo o eseguire il login automatico** (se configurato con Windows Hello).
- Utilizza sensori compatibili con **Human Presence Detection (HPD)**.

Protezione avanzata contro il phishing

Una funzionalità di sicurezza avanzata integrata in Windows 11 che protegge gli utenti contro attacchi di phishing in tempo reale.

🔐 **Come funziona:**

- **Microsoft Defender SmartScreen** analizza i siti web visitati e in caso blocca l'accesso.
- **Credential Guard** isola i dati e li rende inaccessibili, protegge le credenziali anche nel caso in cui un attacco riesca a superare i primi livelli di difesa.
- **Intelligenza Artificiale integrata** che rileva e blocca le mail di phishing fermando le minacce in tempo reale.



TD SYNNEX

Come procedere con la valutazione tecnica

Valuta lo stato dei tuoi dispositivi: strumenti a disposizione

1. **PC Health Check**

PC Health Check fornisce un controllo completo dell'idoneità del dispositivo per garantire che soddisfi i requisiti minimi di sistema di Windows 11.

2. **SCCM**

SCCM consente di controllare e gestire lo stato dei dispositivi all'interno di un'organizzazione, assicurandosi che rispettino i requisiti di sicurezza, aggiornamento e configurazione stabiliti dall'amministratore IT.

3. **Intune Endpoint Analytics**

Utilizza il report Intune Endpoint Analytics Windows 11 hardware readiness per avere una visibilità completa sulla preparazione dell'hardware esistente per l'aggiornamento a Windows 11.

Quali sono le caratteristiche fondamentali di un PC con Windows 11?

Device Type	Senza restrizioni
Processore	1 gigahertz (GHz) o superiore con 2 o più core su un processore compatibile a 64 bit o System on a Chip (SoC)
RAM	4 gigabyte (GB)
Memoria di archiviazione	Dispositivo di archiviazione da 64 gigabyte (GB) o più grande. Deve essere disponibile spazio di archiviazione sufficiente per supportare aggiornamenti mensili regolari.
System Firmware	UEFI, compatibile con Secure Boot
TPM	Trusted Platform module (TPM) versione 2.0
Scheda grafica	Compatibile con DirectX 12+ e con driver WDDM 2.0
Display	Schermo ad alta definizione (720p), 9" o più grande, 8 bit per canale colore

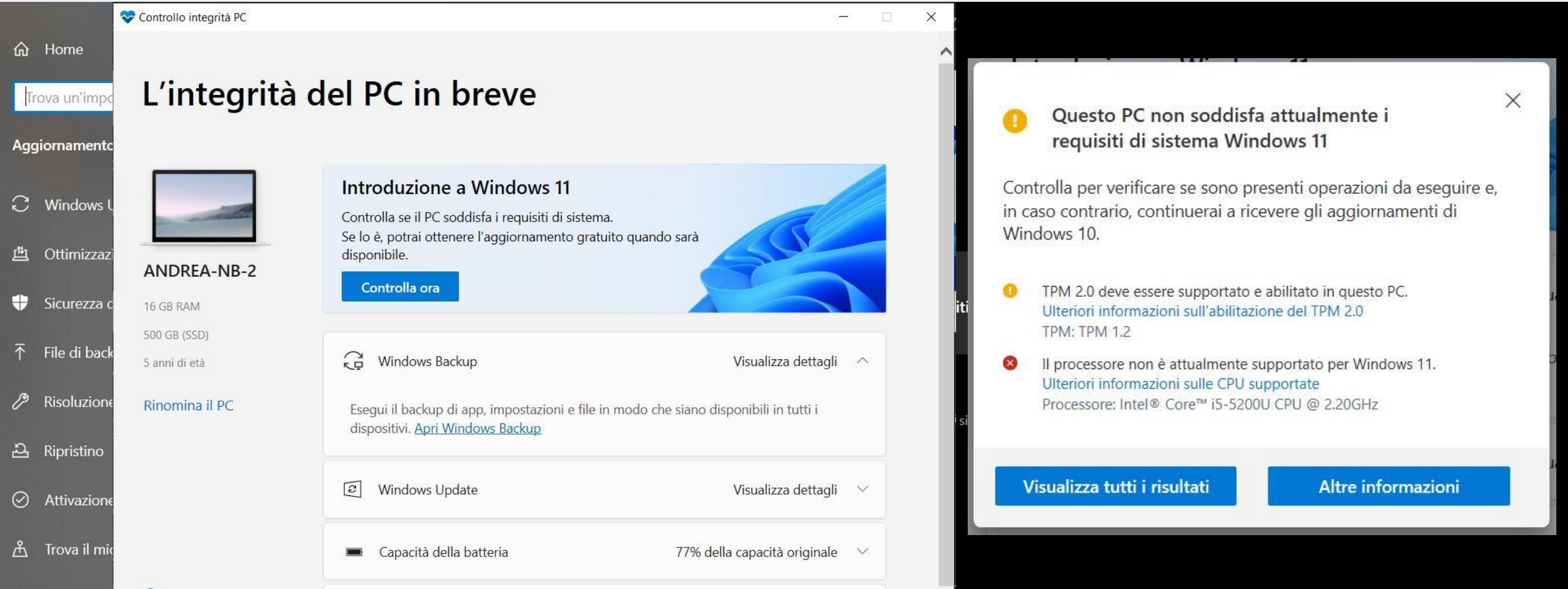
TPM 2.0: Trusted Platform Module

TPM 2.0 è uno standard di sicurezza hardware progettato per fornire funzioni crittografiche sicure, migliorando la protezione dei dispositivi.

TPM 2.0 è un requisito per l'installazione di Windows 11 ed è spesso già integrato nei processori moderni.

- 🔐 **Protezione delle chiavi crittografiche**
- 🧪 **Verifica dell'integrità del sistema operativo**
- 🔒 **Supporto per tecnologie di cifratura come BitLocker**

Controllo integrità



TD SYNNEX

Windows 11 Pro

Windows 11 Pro: Accelera il successo aziendale

IA leader del settore. Potente sicurezza informatica. Progettato per le aziende.

Windows 11 Pro offre:

- Produttività migliorata
- Maggiore sicurezza
- Distribuzione più rapida
- Meno ticket per l'help desk

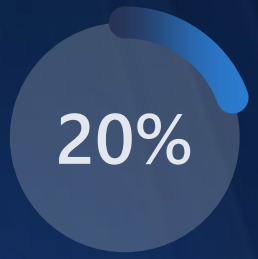
Tutto ciò ha portato **a un ritorno sull'investimento del 250%**[1]

1. Commissioned study delivered by Forrester Consulting "The Total Economic Impact™ of Windows 11 Pro Devices", December 2022. Note, quantified benefits reflect results over three years combined into a single composite organization that generates $1 billion in annual revenue, has 2,000 employees, refreshes hardware on a four-year cycle, and migrates the entirety of its workforce to Windows 11 devices.

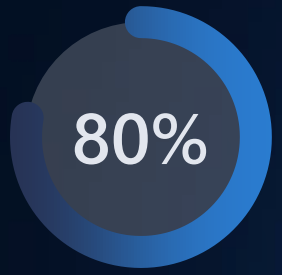
TD SYNNEX

Windows 11 Pro offre migliori opportunità

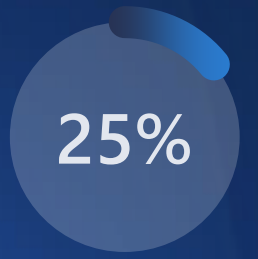
Riduzione degli incidenti di sicurezza



Aumento della produttività dei team di sicurezza e IT



Riduzione delle richieste di supporto al help desk



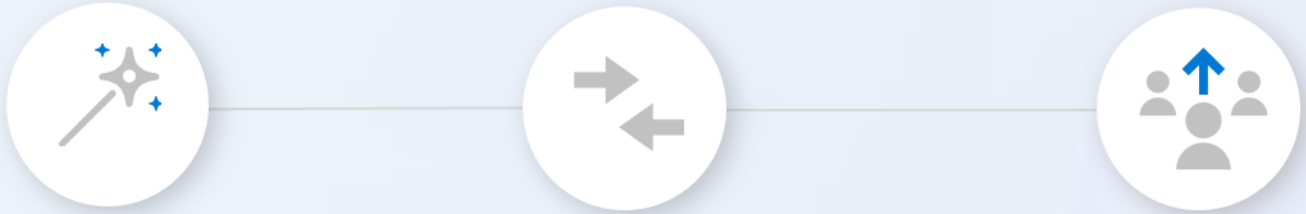
Riduzione dei tempi e dei costi di distribuzione con i dispositivi Windows 11 Pro

Aumento della produttività degli utenti finali

Riduzione dei costi per il supporto della tecnologia

Windows Autopilot

Autopilot consente la configurazione automatica dei dispositivi Windows. Personalizzando i dispositivi, direttamente al primo avvio, senza interventi manuali da parte dell'IT.



Semplifica la distribuzione dei dispositivi

Monitora e gestisci facilmente i dispositivi

Migliora la soddisfazione dei dipendenti

- Zero IT touchpoints
- Configurazione da qualsiasi posizione
- Riconversione dei dispositivi

Windows Autopilot può ridurre i costi relativi alle immagini

Monitor & manage

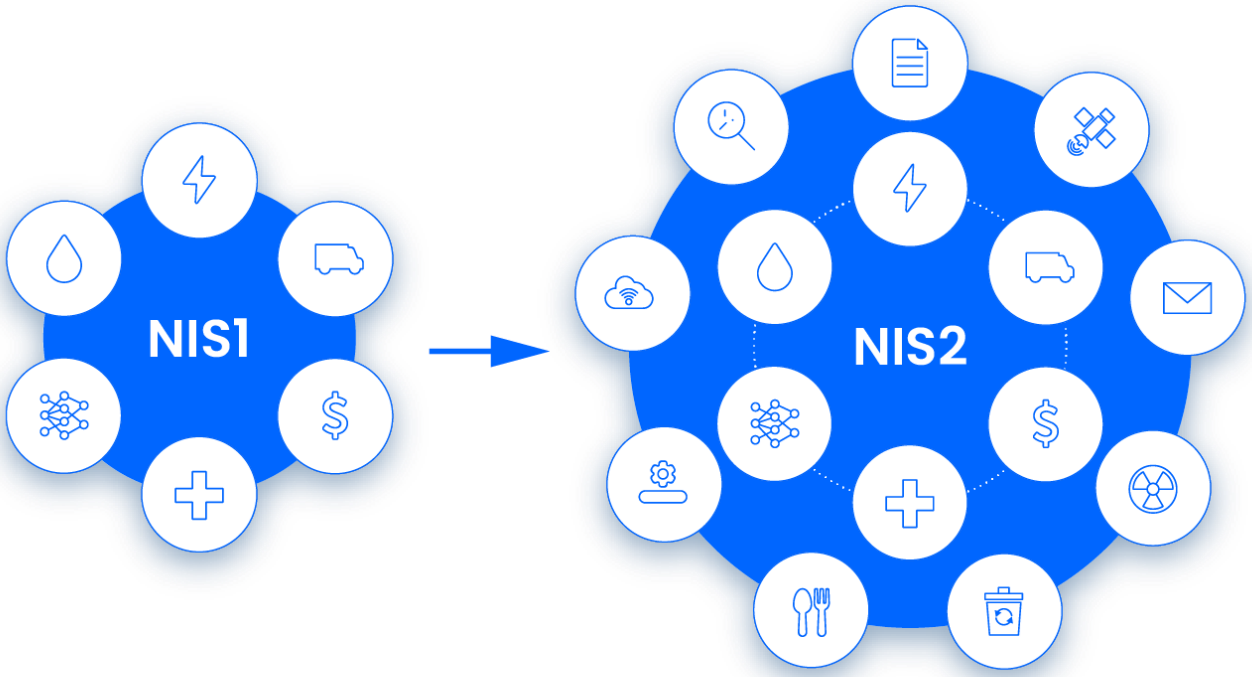
- Riparazione rapida dei dispositivi
- Reimpostazione da remoto semplificata
- Ottimizzato per Microsoft 365

Con Windows Autopilot, configurare e predisporre i dispositivi per i nuovi dipendenti è un processo rapido e semplice.

Employee satisfaction

- Self-service setup
- Accesso rapido alle app personalizzate
- Tecnologia all'avanguardia

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 – Al via la fase 2

Dal 12 Aprile 2025, ACN ha iniziato a notificare a mezzo PEC i soggetti coinvolti nel perimetro della normativa.
Dal 15 Aprile 2025 è disponibile il framework dei requisiti e misure preventive a cui le aziende soggette devono provvedere.

Entro Maggio i soggetti dovranno trasmettere un set informativo obbligatorio tramite il portale di ACN che comprende:
Indirizzamenti IP, Paesi UE a cui si offrono servizi, i contatti dei responsabili della sicurezza.

Requisiti minimi

Requisito	Descrizione
Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete	Implica la definizione e implementazione di strategie per identificare, valutare e mitigare i rischi di sicurezza informatica
Gestione degli incidenti	Richiede procedure e strumenti per rilevare, rispondere e notificare gli incidenti di sicurezza
Continuità operativa	Comprende la gestione dei backup, il disaster recovery e la gestione delle crisi per garantire la continuità del business
Sicurezza della catena di approvvigionamento	Riguarda la gestione dei rischi di sicurezza legati ai fornitori e ai servizi esterni
Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi	Include la gestione delle vulnerabilità e l'implementazione di pratiche di sviluppo sicuro
Valutazione dell'efficacia delle misure di gestione dei rischi	Richiede politiche e procedure per misurare e migliorare l'efficacia delle misure di sicurezza implementate
Pratiche di igiene di base e formazione in sicurezza informatica	Comprende l'educazione degli utenti sulle best practice di sicurezza e la formazione continua
Politiche sull'uso della crittografia e cifratura	Richiede l'implementazione di misure crittografiche per proteggere i dati sensibili
Sicurezza del personale e controllo degli accessi	Riguarda la gestione delle identità, degli accessi e dei beni aziendali
Autenticazione multi-fattore e comunicazioni sicure	Implica l'implementazione di metodi di autenticazione avanzati e la protezione delle comunicazioni

TD SYNNEX

Microsoft

Patch Management e utilizzo di Microsoft Intune

Denis Sacchi – Presales & Solution Architect Microsoft – TD SYNNEX

TD SYNNEX

“More people are killed every year by pigs than by sharks, which shows you how good we are at evaluating risk”

Bruce Schneier

TD SYNNEX

Q&A

Scarica subito la guida per il passaggio a Windows 11!

30 MAGGIO: Acronis – La seconda fase del NIS2 e come farsi trovare pronti

06 GIUGNO: I servizi di TD SYNNEX per la compliance

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

TEAM SECURITY: security.it@tdsynnex.com
SPEAKER: andrea.pezzoni@tdsynnex.com
denis.sacchi@tdsynnex.com
mattia.alushi@tdsynnex.com

Microsoft