TD SYNNEX

HW vendor e conformità NIS2

La scelta che fa la differenza… La via di HP

HP WOLF SECURITY

16 Maggio 2025

Webinar

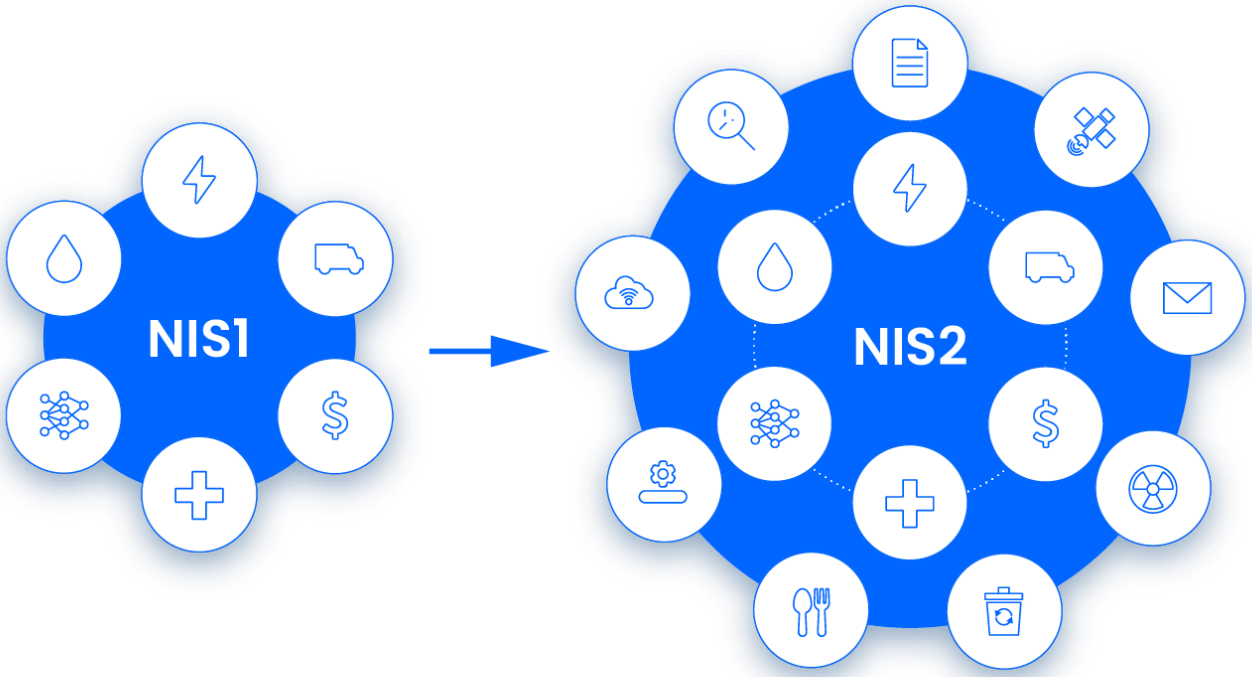
Giampaolo Parravicini - Category manager Digital & Managed Services - HP
Stefano Vacca - Channel Digital Services Business Development Manager - HP
Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

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.

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

Requisiti minimi

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

Può la scelta del vendor HW contribuire alla conformità verso la NIS2?

Più di 20 anni di innovazione nella sicurezza degli endpoint

Contribuiamo agli standard di settore per la sicurezza degli endpoint

Standard stabiliti per TPM, BIOS, resilienza del firmware

HP LABS · TRUSTED COMPUTING GROUP · NIST National Institute of Standards and Technology · ISO

Sicurezza all'avanguardia applicata dall'hardware

Strette partnership per guidare lo stato dell'arte del settore della sicurezza (Intel®, AMD® and Microsoft®)

Miglioramenti rafforzati in ambito di sicurezza con Bromium

HP | Bromium

Protezione univoca via hardware

HP Endpoint Security Controller (ESC): concepito differentemente all'origine

100+ milioni di dispositivi spediti

Nessuna violazione del firmware segnalata

Priorità sulla CPU

Sempre attivo, anche quando il PC è spento

Fisicamente isolato

Monitoraggio continuo

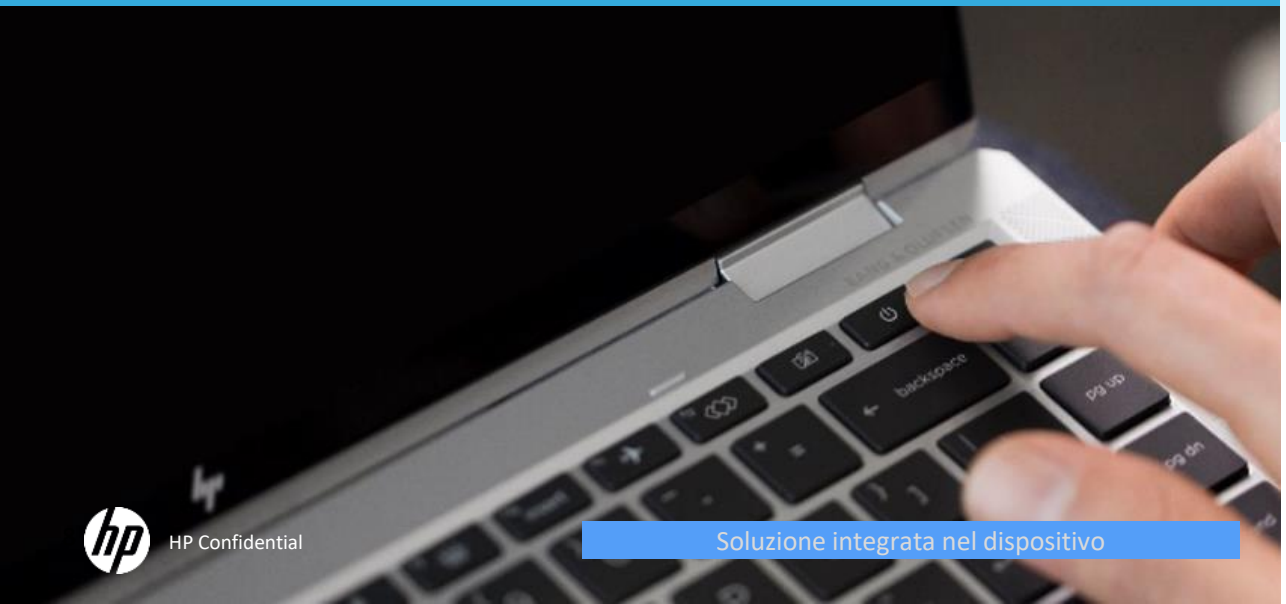
Conforme a NIST e certificato ANSSI

Post-Quantum Security:
Incorpora la crittografia evoluta per proteggere il firmware dagli attacchi informatici quantistici.

Resilienza del BIOS

con HP Sure Start

Protezione persistente del firmware



Soluzione integrata nel dispositivo

Requisito: resilienza del firmware

- L'integrità del codice BIOS è essenziale per la sicurezza del PC
- La protezione del BIOS deve essere automatica, affidabile e non richiedere un sovraccarico IT significativo

Soluzione: HP Sure Start

- Verifica che il codice del BIOS non sia stato danneggiato
- Ripristina automaticamente una copia convalidata del firmware se viene rilevato un BIOS danneggiato
- Utilizza il chip HP eSC per fornire la massima protezione

Vantaggio: resilienza del livello BIOS

- Riduce i rischi bloccando gli attacchi al firmware
- Aumenta la disponibilità con la sicurezza basata su hardware
- Riduce il sovraccarico IT: Attivato per impostazione predefinita; Nessuna gestione richiesta

Come contribuisce ad adeguarsi a NIS2?

- **a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete**
  verifica l'integrità dell'hardware e del firmware, fornendo una base sicura per l'analisi dei rischi a livello di sistema

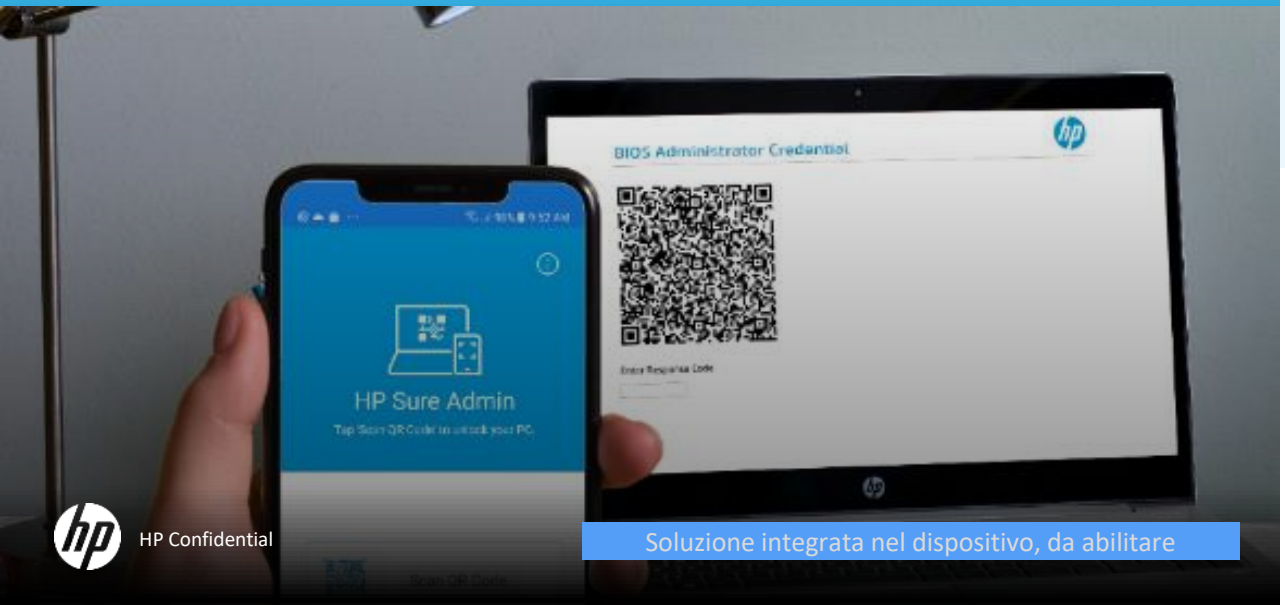
- **d) Sicurezza della catena di approvvigionamento**
  garantisce l'integrità del firmware, proteggendo contro le modifiche non autorizzate nella catena di approvvigionamento

- **e) Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi**
  verifica l'integrità del sistema all'avvio, garantendo una base sicura per lo sviluppo e la manutenzione

Gestione del BIOS scalabile e sicura

con HP Sure Admin

Proteggi le impostazioni del BIOS con un basso impatto operativo



Requisito: Sicurezza della configurazione

- La sicurezza della configurazione del BIOS è fondamentale per gestire il rischio
- Le password del BIOS sono molto difficili da gestire su larga scala
- Quindi o l'organizzazione è a rischio o c'è un impatto operativo significativo

Soluzione: HP Sure Admin

- Sostituisce le password del BIOS con chiavi crittografiche
- Supporta l'amministrazione locale e remota
- App per smartphone per l'accesso al BIOS dell'utente finale

Vantaggio: sicurezza scalabile del BIOS

- Riduce notevolmente il rischio di compromissione della configurazione del BIOS
- Scalabilità fino a migliaia di PC con un basso sovraccarico amministrativo

Come contribuisce ad adeguarsi a NIS2?

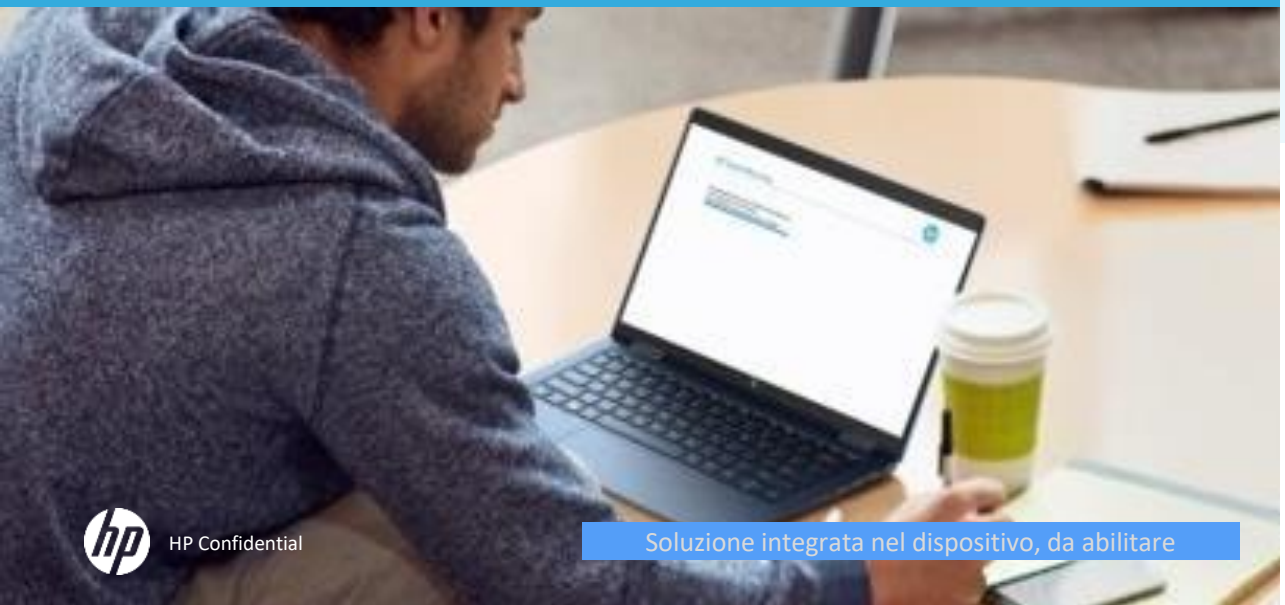
- **i) Sicurezza del personale e controllo degli accessi**
  fornisce accesso privilegiato sicuro alle impostazioni del BIOS, controllando rigorosamente le azioni degli amministratori

- **l) Autenticazione multi-fattore e comunicazioni sicure**
  fornisce comunicazioni sicure per gli amministratori, proteggendo le interazioni più sensibili grazie all'uso della MFA

Ripristina sempre e ovunque su larga scala

con HP Sure Recover[15]

Ripristino sicuro del sistema operativo Windows



Requisito: resilienza di Windows

- Ripristino affidabile di Windows, anche da attacchi che sconfiggono gli strumenti di ripristino del sistema operativo convenzionali
- Disaster Recovery: continuità aziendale rapida e su larga scala

Soluzione: HP Sure Recover

- Ripristina rapidamente il sistema operativo Windows e le app
- Supporta immagini generiche e personalizzate
- Ripristino automatico dal cloud o dall'archiviazione locale sicura
- HP Security Controller garantisce un ripristino affidabile

Vantaggio: Continuità lavorativa del lavoro ibrido

- Supporta casi d'uso sia in caso di incidente che di ripristino di emergenza
- Continuità aziendale, anche se sotto attacco sofisticato
- Opzioni di implementazione flessibili per un basso sovraccarico operativo

Soluzione integrata nel dispositivo, da abilitare

Come contribuisce ad adeguarsi a NIS2?

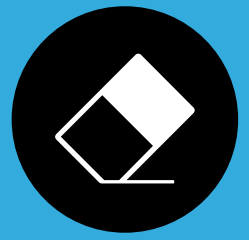
- **c) Continuità operativa**
  permette il ripristino sicuro del sistema a uno stato noto e affidabile, cruciale per la continuità operativa

Gestisci e proteggi i PC portatili

con HP Protect & Trace

TROVA

BLOCCA



CANCELLA

Requisito: Gestione e Protezione dei Dispositivi

- Localizzare e proteggere i dispositivi in caso di furto o smarrimento
- Gestire remotamente la sicurezza dei dati sui dispositivi
- Semplificare il recupero e la protezione dei dispositivi persi

Soluzione: HP Protect & Trace

- Fornisce tracciamento GPS e geolocalizzazione dei dispositivi
- Permette il blocco remoto e la cancellazione dei dati
- Offre un portale di gestione centralizzato per il monitoraggio
- Funziona anche con dispositivo spento o Sistema Operativo corrotto

Beneficio: Sicurezza dei Dati e Gestione degli Asset

- Riduce il rischio di perdita di dati sensibili
- Aumenta le possibilità di recupero dei dispositivi smarriti
- Semplifica la gestione della sicurezza per i team IT
- Migliora la conformità con le normative sulla protezione dei dati

Soluzione da ordinare in fabbrica

Come contribuisce ad adeguarsi a NIS2?

- **c) Continuità operativa**
  aiuta a localizzare e proteggere i dispositivi smarriti o rubati, salvaguardando i dati critici per la continuità aziendale

- **i) Sicurezza del personale e controllo degli accessi**
  gestisce la sicurezza anche attraverso il controllo dell'accesso ai dispositivi, proteggendo i beni aziendali fisici e digitali

Mappatura requisiti <> Soluzioni HP 1/2

Requisito	Soluzioni HP
a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete	**Sure Start** (verifica l'integrità dell'hardware e del firmware, fornendo una base sicura per l'analisi dei rischi a livello di sistema); **Sure Click** (isola le minacce in contenitori virtuali, permettendo un'analisi sicura del comportamento delle minacce); **Workforce Experience Platform** (monitora e analizza la salute dei dispositivi, fornendo dati cruciali per l'analisi dei rischi e la sicurezza della rete)
b) Gestione degli incidenti	**Sure Click** (isola e contiene le minacce, facilitando la gestione degli incidenti senza compromettere l'intero sistema); **Sure Access** (controlla l'accesso alle risorse critiche, aiutando a prevenire e limitare l'impatto degli incidenti); **Workforce Experience Platform** (fornisce avvisi e analisi degli incidenti in tempo reale, accelerando la risposta e la notifica)
c) Continuità operativa	**Sure Recover** (permette il ripristino sicuro del sistema a uno stato noto e affidabile, cruciale per la continuità operativa); **Protect & Trace** (aiuta a localizzare e proteggere i dispositivi smarriti o rubati, salvaguardando i dati critici per la continuità aziendale)
d) Sicurezza della catena di approvvigionamento	**Platform Certificates** (verifica l'autenticità dell'hardware, assicurando che i componenti provengano da fonti affidabili); **Sure Start** (garantisce l'integrità del firmware, proteggendo contro le modifiche non autorizzate nella catena di approvvigionamento); **Firmware Lock** (Protegge i dispositivi durante il trasporto tra sedi attraverso blocco firmware con sblocco autorizzato)
e) Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi	**Sure Start** (verifica l'integrità del sistema all'avvio, garantendo una base sicura per lo sviluppo e la manutenzione); **Sure Click** (protegge durante la navigazione e l'uso di applicazioni, riducendo i rischi durante le fasi di sviluppo e test); **Workforce Experience Platform** (monitora e segnala le vulnerabilità, supportando la manutenzione proattiva dei sistemi)

Mappatura requisiti <> Soluzioni HP 2/2

Requisito	Soluzioni HP
f) Valutazione dell'efficacia delle misure di gestione dei rischi	**Workforce Experience Platform** (fornisce analisi e report dettagliati sulle prestazioni di sicurezza, permettendo una valutazione continua dell'efficacia); **Sure Click** (offre visibilità sulle minacce bloccate, consentendo di valutare l'efficacia delle misure di protezione)
g) Pratiche di igiene di base e formazione in sicurezza informatica	**Sure Click** (educa gli utenti sulle minacce attraverso l'isolamento, fornendo esperienze pratiche di sicurezza); **Workforce Experience Platform** (fornisce informazioni per la formazione basata sui rischi rilevati, personalizzando l'educazione alla sicurezza)
h) Politiche sull'uso della crittografia e cifratura	**Sure Access** (utilizza crittografia avanzata per l'accesso remoto sicuro, proteggendo i dati in transito); **Platform Certificates** (utilizza firme digitali per l'autenticazione dell'hardware, implementando la crittografia per la verifica a livello di componente)
i) Sicurezza del personale e controllo degli accessi	**Sure Admin** (fornisce accesso privilegiato sicuro alle impostazioni del BIOS, controllando rigorosamente le azioni degli amministratori); **Sure Access** (gestisce l'accesso remoto e le identità, implementando un controllo granulare degli accessi); **Protect & Trace** (gestisce la sicurezza anche attraverso il controllo dell'accesso ai dispositivi, proteggendo i beni aziendali fisici e digitali); **Firmware Lock** (Implementa controllo accessi granulare basato su gruppi Azure AD e App companion)
l) Autenticazione multi-fattore e comunicazioni sicure	**Sure Access** (supporta l'autenticazione multi-fattore, aumentando la sicurezza dell'accesso alle risorse critiche); **Sure Admin** (fornisce comunicazioni sicure per gli amministratori, proteggendo le interazioni più sensibili grazie all'uso della MFA); **Sure Click** (protegge le comunicazioni web, isolando le minacce potenziali in contenitori virtuali); **Firware Lock** (Richiede più fattori per lo sblocco del PC)

https://www.acn.gov.it/portale/w/nis-avviata-la-seconda-fase
https://piattaformaitalia.pwc.it/articles/direttiva-nis-2-al-via-con-la-seconda-fase-operativa/
https://nis2directive.eu/
https://www.SoluzioniHP.it
https://www.cybersecurityframework.it/

TD SYNNEX

“Given a choice between dancing pigs and security, users will pick dancing pigs every time.”

Edward Felten

Q&A

PROSSIMI APPUNTAMENTI

23 MAGGIO: Microsoft e la sicurezza del dispositivo e il patch management
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

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

TEAM SECURITY: security.it@tdsynnex.com

SPEAKER: andrea.pezzoni@tdsynnex.com stefano.vacca@hp.com