HP Wolf Security

HP WOLF SECURITY

Come semplificare il rispetto di NIS2

Ricapitolo 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

* In base all'art. 24 comma 2 del DECRETO LEGISLATIVO 4 settembre 2024, n. 138

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.

Soluzioni di sicurezza HP

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

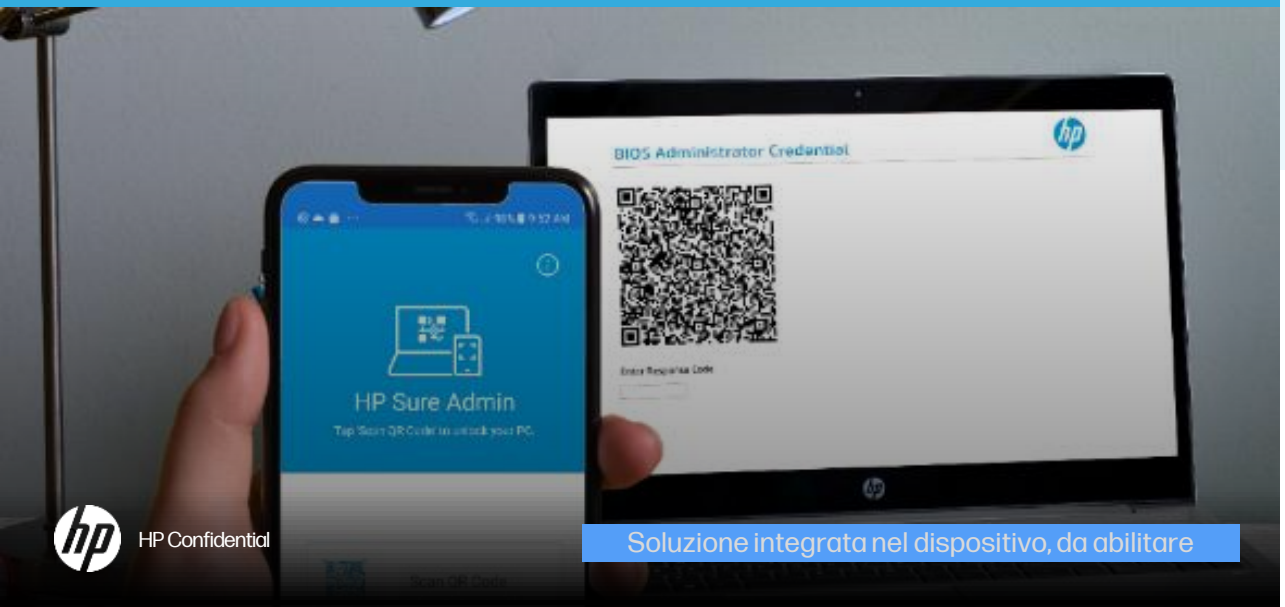
- **d) Sicurezza della catena di approvvigionamento**
  garantisce l'integrità del firmware, proteggendo contro le modifiche non autorizzate nella catena di approvvigionamento

- **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?

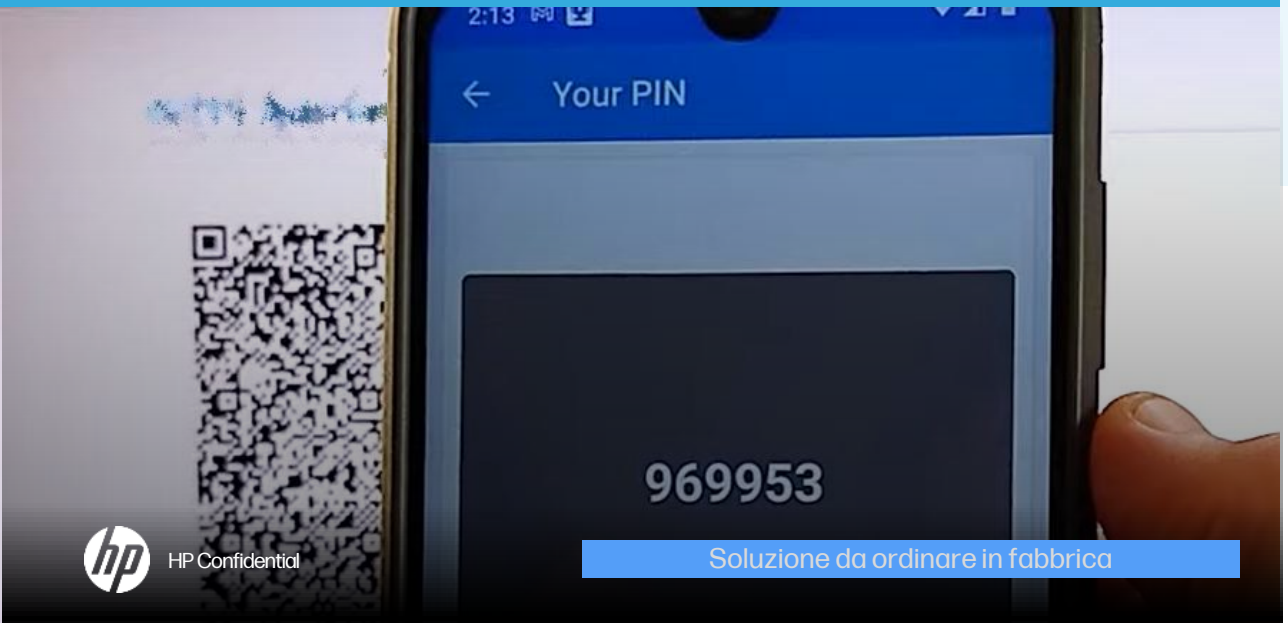
- **i) Sicurezza del personale e controllo degli accessi**
  fornisce accesso privilegiato sicuro alle impostazioni del BIOS, controllando rigorosamente le azioni degli amministratori

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

Blocco del PC al livello di firmware

con HP Firmware Lock

Garantisci l'accesso ai sistemi solo agli autorizzati



Requisito: Protezione dell'accesso al PC

- La sicurezza pre-boot è fondamentale per proteggere l'accesso al PC
- La protezione deve essere integrata a livello firmware/hardware e non solo software
- È necessario un meccanismo di autenticazione affidabile e senza password

Soluzione: HP Firmware Lock

- Richiede autenticazione pre-boot prima di avviare il sistema operativo
- Utilizza tecnologia HP Sure Admin per l'autenticazione passwordless
- Si integra con il sistema di gestione delle chiavi HP Sure Admin KMS per Azure

Vantaggio: Protezione avanzata degli endpoint

- Previene accessi non autorizzati bloccando l'avvio del sistema
- Offre protezione hardware/firmware contro i bypass a livello OS

Come contribuisce ad adeguarsi a NIS2?

- **d) Sicurezza della catena di approvvigionamento**
  Protegge l'integrità dei dispositivi durante il trasporto implementando un blocco a livello firmware che può essere rimosso solo da personale autorizzato nella sede di destinazione, prevenendo manomissioni.

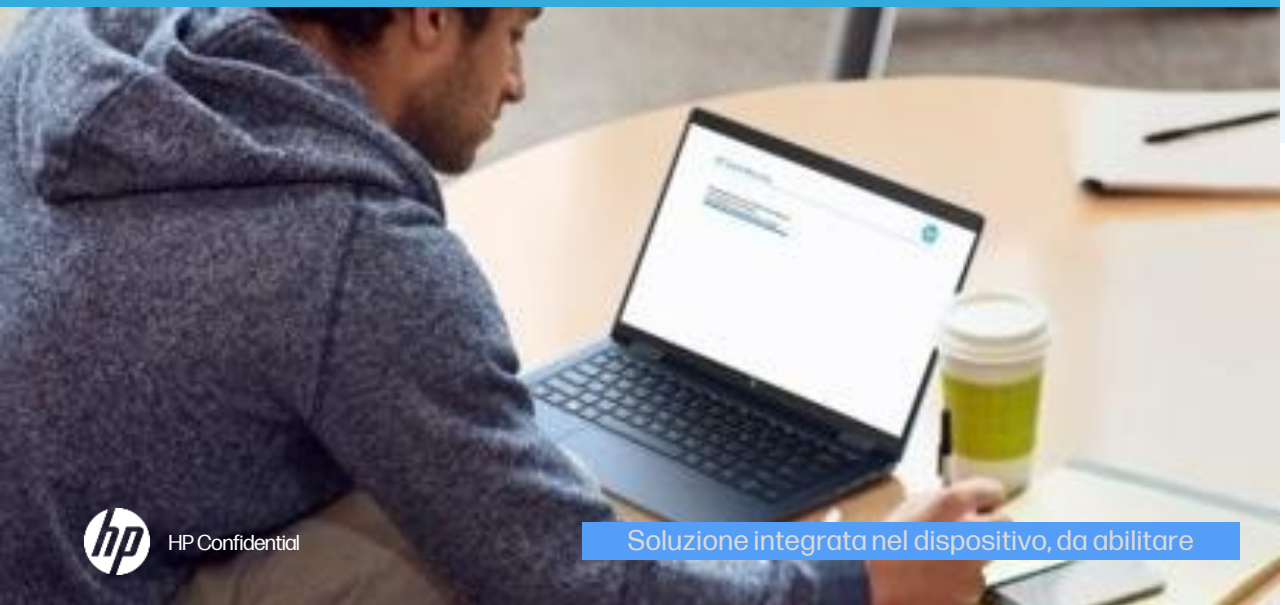
- **i) Sicurezza del personale e controllo degli accessi**
  Offre un sistema granulare di controllo accessi integrato con Azure AD, permettendo di gestire le autorizzazioni a livello di gruppo e garantendo che solo gli utenti autorizzati possano sbloccare i dispositivi.

- **l) Autenticazione multi-fattore e comunicazioni sicure**
  Implementa autenticazione multi-fattore combinando il possesso del dispositivo fisico con l'autorizzazione digitale tramite Sure Admin e assicura comunicazioni sicure con Azure AD per la distribuzione dei PIN.

Ripristina sempre e ovunque su larga scala

con HP Sure Recover[15]

Ripristino sicuro del sistema operativo Windows



Soluzione integrata nel dispositivo, da abilitare

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

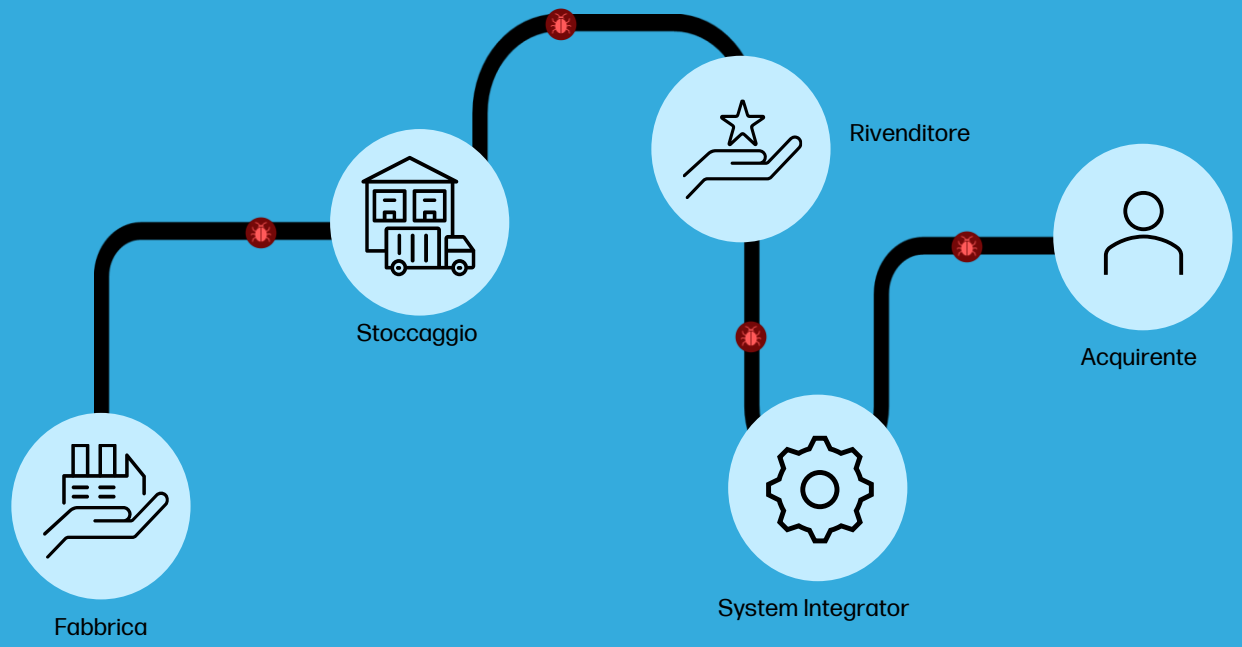
- Supporta casi d'uso sia in caso di incidente che di ripristino di emergenza
- Continuità aziendale, anche se sotto attacco sofisticato
- Opzioni di implementazione flessibili per un basso sovraccarico operativo

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

Convalida l'integrità del PC

con HP Platform Certificae



Requisito: Integrità della Catena di Approvvigionamento

- Verificare l'autenticità e l'integrità dei PC e dei componenti
- Protezione contro manomissioni durante il trasporto
- Processo di verifica scalabile e automatizzato

Soluzione: HP Platform Certificate

- Crea un certificato crittografico della configurazione di fabbrica
- Fornisce un'API per il download sicuro dei certificati
- Permette la verifica dell'integrità del PC prima della distribuzione

Beneficio: Sicurezza della Catena di Approvvigionamento

- Riduce i rischi identificando modifiche non autorizzate
- Aumenta la fiducia nella distribuzione di PC remoti
- Si integra facilmente nei processi IT esistenti
- Allineato con gli standard di sicurezza del settore (TCG, NIST)

Soluzione da ordinare in fabbrica

Come contribuisce ad adeguarsi a NIS2?

- **d) Sicurezza della catena di approvvigionamento**
  verifica l'autenticità dell'hardware, assicurando che i componenti provengano da fonti affidabili

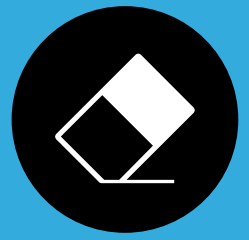
- **h) Politiche sull'uso della crittografia e cifratura**
  utilizza firme digitali per l'autenticazione dell'hardware, implementando la crittografia per la verifica a livello di componente

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

Il “Click incauto" capita a tutti

HP Sure Click

Incluso con Wolf Pro Security e Sure Click Enterprise

Soluzione software indipendente dall’hardware

Requisito: Difesa sul Social Engineering

- Gli attori delle minacce utilizzano l'ingegneria sociale per indurre il personale a facilitare i loro attacchi
- Phishing e Ransomware sono minacce costanti
- I prodotti di sicurezza convenzionali non riescono a bloccare in modo affidabile tali attacchi

Soluzione: HP Sure Click

- Contrasta gli attacchi che sfruttano il comportamento degli utenti
- Utilizza la micro-virtualizzazione applicata dall'hardware per contenere le minacce
- Fornisce un'intelligence completa sulle minacce
- Nessuna modifica ai flussi di lavoro degli utenti

Vantaggio: protezione intrinseca

- Elimina il rischio dai tipi di attacco più comuni
- La console fornisce informazioni utili al team di sicurezza
- Riduce il rumore operativo dovuto ai falsi positivi
- Gli utenti "lavorano senza preoccupazioni"

Come contribuisce ad adeguarsi a NIS2?

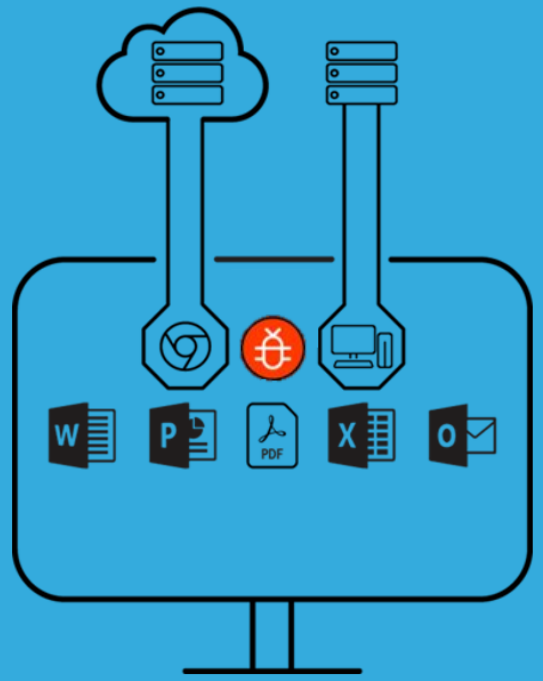
- **a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete**
  isola le minacce in contenitori virtuali, permettendo un'analisi sicura del comportamento delle minacce
- **b) Gestione degli incidenti**
  isola e contiene le minacce, facilitando la gestione degli incidenti senza compromettere l'intero sistema
- **e) Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi**
  protegge durante la navigazione e l'uso di applicazioni, riducendo i rischi durante le fasi di sviluppo e test
- **f) Valutazione dell'efficacia delle misure di gestione dei rischi**
  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
  educa gli utenti sulle minacce attraverso l'isolamento, fornendo esperienze pratiche di sicurezza

  l) Autenticazione multi-fattore e comunicazioni sicure
  protegge le comunicazioni web, isolando le minacce potenziali in contenitori virtuali

Risolvi la sfida della sicurezza degli utenti privilegiati

con HP Sure Access Enterprise



Protegge le risorse critiche, anche se il PC è compromesso

Requisito: Proteggere le attività con privilegi

- Gli utenti con elevati privilegi (amministratori IT, supporto tecnico di terze parti) accedono in remoto a sistemi di alto valore strategico
- Gli utenti privilegiati richiedono controlli di sicurezza aggiuntivi per mitigare l'aumento del rischio

Soluzione: isolamento dell'attività con privilegi

- Ogni sessione di accesso remoto con privilegi nel PC dell'utente è isolata
- Protegge le applicazioni e i dati di alto valore anche se l'endpoint è compromesso
- Isolamento rinforzato dall'hardware per la massima sicurezza

Vantaggio: riduzione efficiente del rischio

- Proteggi i dati e le applicazioni più sensibili
- Le connessioni isolate consentono agli utenti con privilegi di utilizzare in modo sicuro un singolo PC per tutte le attività
- Soddisfa in modo efficiente i requisiti di conformità e controllo degli audit

Come contribuisce ad adeguarsi a NIS2?

- **b) Gestione degli incidenti**
  controlla l'accesso alle risorse critiche, aiutando a prevenire e limitare l'impatto degli incidenti

- **h) Politiche sull'uso della crittografia e cifratura**
  utilizza crittografia avanzata per l'accesso remoto sicuro, proteggendo i dati in transito

- **i) Sicurezza del personale e controllo degli accessi**
  gestisce l'accesso remoto e le identità, implementando un controllo granulare degli accessi

- **l) Autenticazione multi-fattore e comunicazioni sicure**
  supporta l'autenticazione multi-fattore, aumentando la sicurezza dell'accesso alle risorse critiche

Monitora e governa i tuoi dispositivi

con HP Proactive Insights

Requisito: Ottimizzazione della Gestione del Parco Dispositivi

- Monitoraggio proattivo dello stato dei dispositivi
- Identificazione precoce di problemi hardware e software
- Miglioramento dell'esperienza utente e della produttività

Soluzione: HP Proactive Insights

- Fornisce analisi avanzate basate su AI per il monitoraggio dei dispositivi
- Offre dashboard intuitive per la visualizzazione dello stato del parco IT
- Genera avvisi automatici per problemi imminenti o prestazioni degradate

Beneficio: Gestione IT Intelligente e Preventiva

- Riduce i tempi di inattività anticipando e prevenendo i problemi
- Ottimizza le prestazioni dei dispositivi e la soddisfazione degli utenti
- Semplifica la pianificazione degli interventi di manutenzione
- Fornisce insights actionable per decisioni IT basate sui dati

Soluzione software indipendente dall'hardware

Come contribuisce ad adeguarsi a NIS2?

- **a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete**
  monitora e analizza la salute dei dispositivi, fornendo dati cruciali per l'analisi dei rischi e la sicurezza della rete
- **b) Gestione degli incidenti**
  fornisce avvisi e analisi degli incidenti in tempo reale, accelerando la risposta e la notifica
- **e) Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi**
  monitora e segnala le vulnerabilità, supportando la manutenzione proattiva dei sistemi
- **f) Valutazione dell'efficacia delle misure di gestione dei rischi**
  fornisce analisi e report dettagliati sulle prestazioni di sicurezza, permettendo una valutazione continua dell'efficacia
- **g) Pratiche di igiene di base e formazione in sicurezza informatica**
  fornisce informazioni per la formazione basata sui rischi rilevati, personalizzando l'educazione alla sicurezza

Vista d'insieme

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); **Proactive Insights** (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); **Proactive Insights** (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); **Proactive Insights** (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	**Proactive Insights** (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); **Proactive Insights** (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)


HP WOLF SECURITY
Maggiori informazioni su
www.SoluzioniHP.it