HP Wolf Security

HP WOLF SECURITY

Come semplificare il rispetto di DORA

Ricapitolo requisiti principali

Requisito DORA	Descrizione breve
Gestione del rischio ICT	Framework completo per identificare, valutare e mitigare i rischi legati alle tecnologie dell'informazione e della comunicazione. Include la mappatura degli asset, l'analisi delle minacce e vulnerabilità, e l'implementazione di controlli appropriati.
Governance e strategia	Implementazione di una struttura organizzativa chiara con ruoli e responsabilità definiti per la gestione dei rischi ICT. Include la definizione di politiche, procedure e una strategia complessiva di resilienza digitale approvata dal top management.
Protezione dei dati	Misure tecniche e organizzative per garantire la riservatezza, integrità e disponibilità dei dati. Include controlli di accesso, crittografia, e procedure per la gestione sicura delle informazioni sensibili.
Mitigazione dei rischi	Implementazione di controlli e misure specifiche per ridurre i rischi identificati a un livello accettabile. Include soluzioni tecniche, procedure organizzative e controlli compensativi.
Reportistica degli incidenti	Procedure per la tempestiva identificazione, classificazione e segnalazione degli incidenti ICT significativi alle autorità competenti. Include la documentazione dettagliata degli incidenti e delle azioni intraprese.
Test di resilienza digitale	Esecuzione regolare di test per valutare l'efficacia delle misure di sicurezza implementate. Include test di penetrazione, stress test e simulazioni di scenari di crisi.
Gestione dei fornitori ICT	Monitoraggio e gestione dei rischi legati ai fornitori di servizi ICT terzi. Include la valutazione dei fornitori, contratti con requisiti di sicurezza specifici e monitoraggio continuo delle performance.
Condivisione delle informazioni	Framework per la condivisione di informazioni su minacce e vulnerabilità con altre istituzioni finanziarie e autorità competenti. Include protocolli di comunicazione e procedure per la condivisione sicura delle informazioni.
Formazione del personale	Programmi continui di formazione e sensibilizzazione sulla sicurezza informatica per tutto il personale. Include training specifici per ruolo, aggiornamenti regolari e valutazione dell'efficacia della formazione.
Aggiornamento continuo	Processo per mantenere aggiornati sistemi, software e misure di sicurezza. Include la gestione delle patch, l'aggiornamento delle politiche e l'adeguamento ai nuovi rischi emergenti.
Piani di continuità operativa	Sviluppo e mantenimento di piani dettagliati per garantire la continuità dei servizi critici in caso di incidenti ICT. Include procedure di disaster recovery, backup e ripristino dei sistemi.
Crittografia e protezione dei dati	Implementazione di soluzioni crittografiche robuste per proteggere dati sensibili sia in transito che a riposo. Include gestione delle chiavi crittografiche e procedure per la protezione dei dati durante tutto il loro ciclo di vita.
Monitoraggio continuo	Implementazione di sistemi e procedure per il monitoraggio costante delle minacce, anomalie e performance dei sistemi ICT. Include SIEM, log management e procedure di risposta agli alert.
Resilienza digitale	Capacità complessiva dell'organizzazione di resistere, adattarsi e riprendersi da incidenti ICT. Include aspetti tecnici, organizzativi e procedurali per garantire la continuità delle operazioni critiche.

Può la scelta del vendor HW contribuire all'adeguamento a DORA?

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

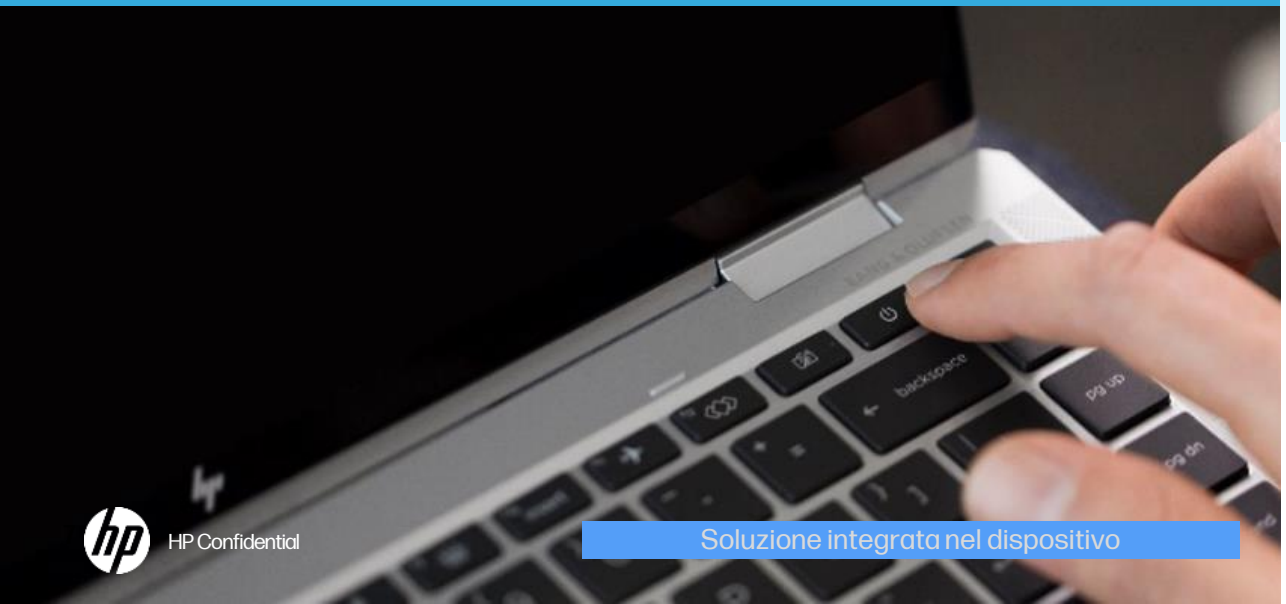
Post-Quantum Security:
Incorpora la crittografia evoluta per proteggere il firmware dagli attacchi informatici quantistici.

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

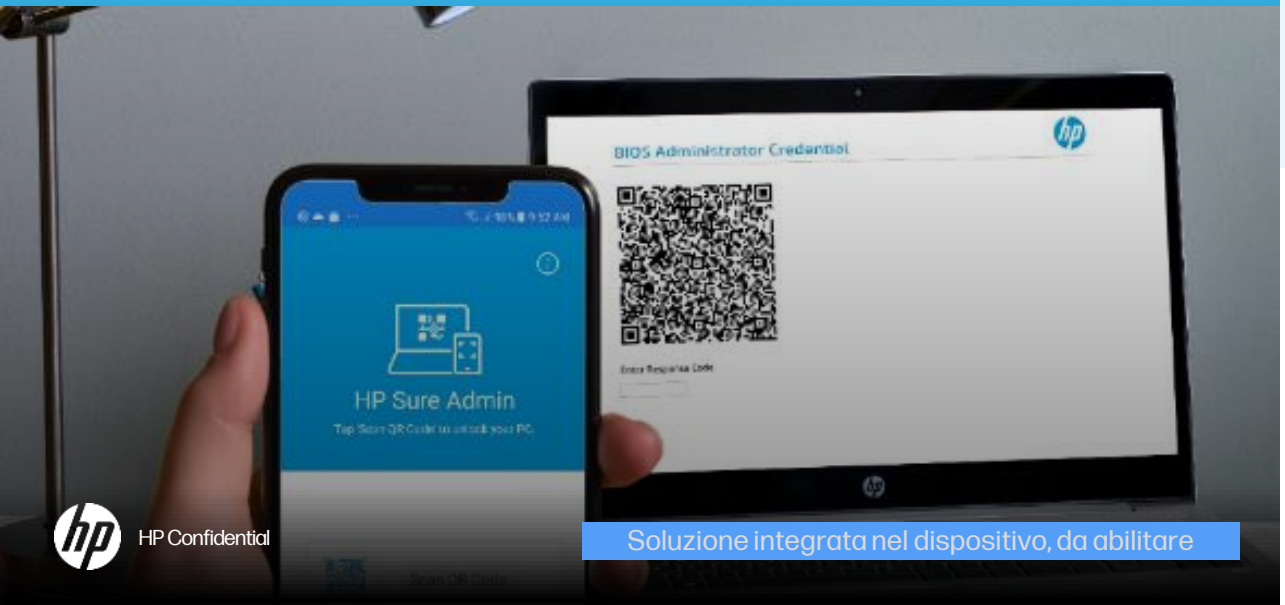
Come contribuisce ad adeguarsi a DORA?

- **Gestione del rischio ICT**
  previene e mitiga attacchi al firmware, fondamentali per la sicurezza del sistema
- **Mitigazione dei rischi**
  ripristino automatico riduce l'impatto degli attacchi al BIOS
- **Aggiornamento continuo**
  assicura che il BIOS sia sempre aggiornato all'ultima versione sicura
- **Resilienza digitale**
  il ripristino automatico mantiene il sistema operativo anche dopo attacchi al firmware

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 DORA?

- **Governance e strategia**
  permette una gestione sicura delle configurazioni critiche, fondamentale per la strategia di sicurezza

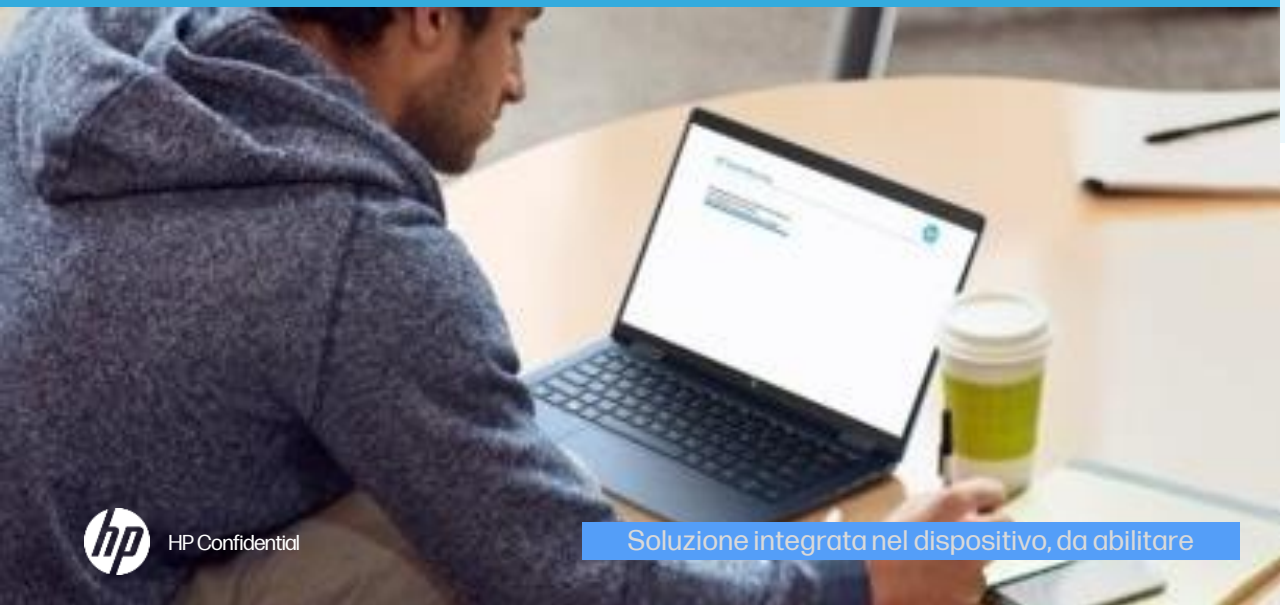
- **Mitigazione dei rischi**
  riduce i rischi associati a configurazioni errate o non autorizzate del BIOS

- **Monitoraggio continuo**
  consente il tracciamento dei cambiamenti nelle impostazioni critiche del sistema

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 DORA?

- **Reportistica degli incidenti**
  riduce l'impatto degli incidenti minimizzando i tempi di inattività, cruciale per la reportistica

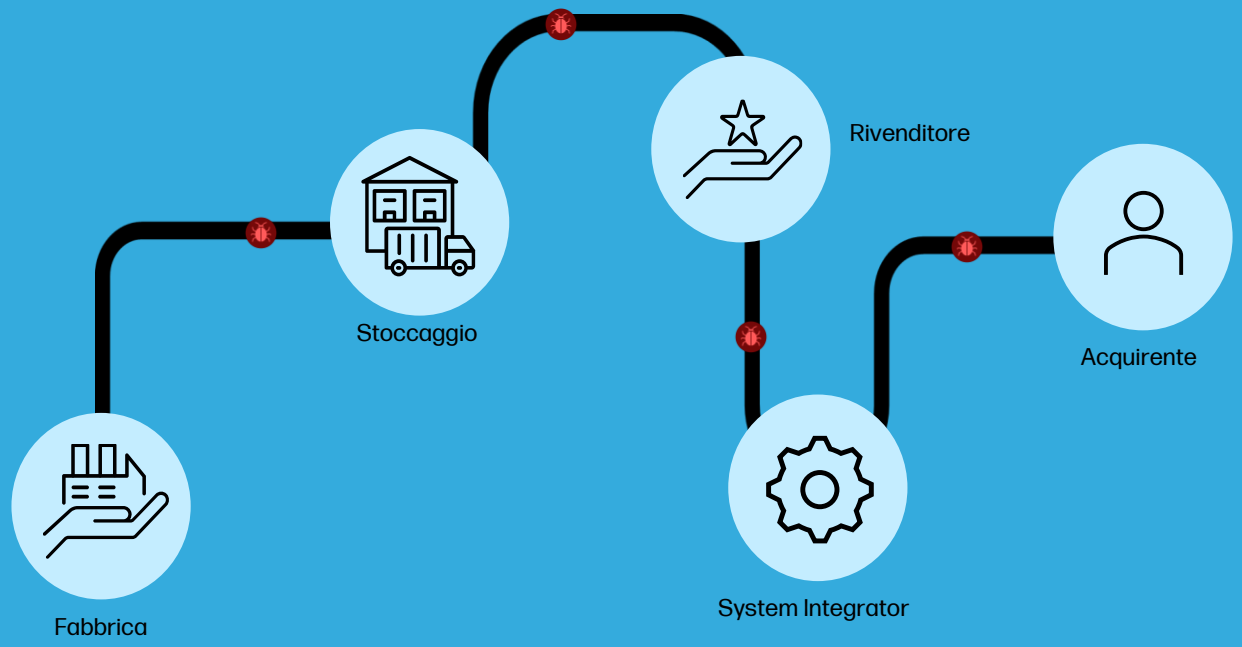
- **Test di resilienza digitale**
  dimostra la capacità di recupero rapido, componente chiave della resilienza

- **Piani di continuità operativa**
  supporta il ripristino rapido, essenziale per i piani di continuità

- **Resilienza digitale**
  permette un recupero veloce da incidenti, fondamentale per la resilienza complessiva

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 DORA?

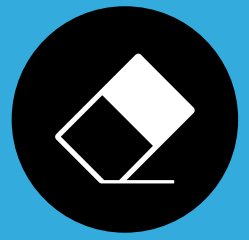
- **Gestione del rischio ICT**
  verifica l’integrità del sistema a livello hardware e firmware, fondamentale per la sicurezza di base
- **Mitigazione dei rischi**
  rileva manomissioni hardware e firmware, mitigando rischi di supply chain
- **Monitoraggio continuo**
  offre la possibilità di verifica costante dell'integrità del sistema
- **Resilienza digitale**
  assicura l'affidabilità del sistema a livello hardware, base per la resilienza complessiva

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 DORA?

- **Gestione del rischio ICT**
  gestisce i rischi associati ai dispositivi mobili, componente critico dell'infrastruttura IT moderna
- **Protezione dei dati**
  offre cancellazione remota dei dati, cruciale per proteggere le informazioni sui dispositivi persi o rubati
- **Mitigazione dei rischi**
  fornisce strumenti per gestire efficacemente i rischi dei dispositivi persi o rubati
- **Reportistica degli incidenti**
  permette il tracciamento dei dispositivi, fondamentale per la reportistica in caso di perdita
- **Piani di continuità operativa**
  supporta la gestione degli incidenti relativi ai dispositivi mobili, cruciale per la continuità operativa

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 DORA?

- **Gestione del rischio ICT**
  isola le minacce esterne, riducendo significativamente il rischio di infezioni da malware

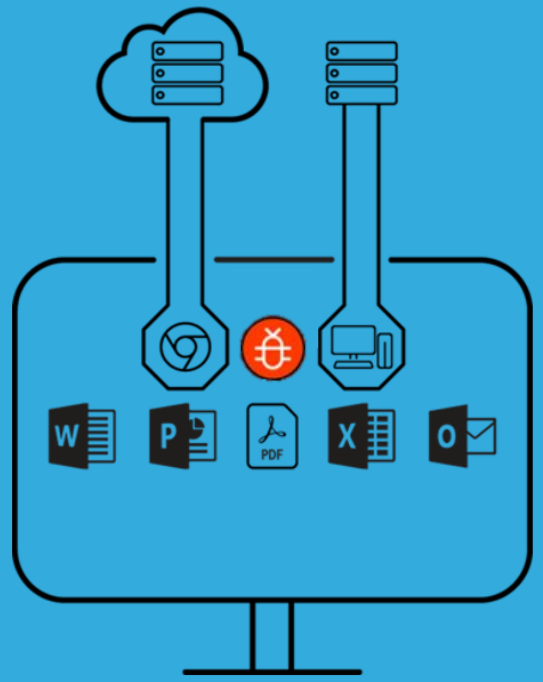
- **Protezione dei dati**
  previene l'accesso non autorizzato ai dati isolando preventivamente i contenuti provenienti da fonti potenzialmente inaffidabili

- **Mitigazione dei rischi**
  contiene le minacce in ambienti isolati, impedendo la loro diffusione nel sistema

- **Aggiornamento continuo**
  la sua natura containerizzata protegge contro nuove minacce senza necessità di aggiornamenti continui

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

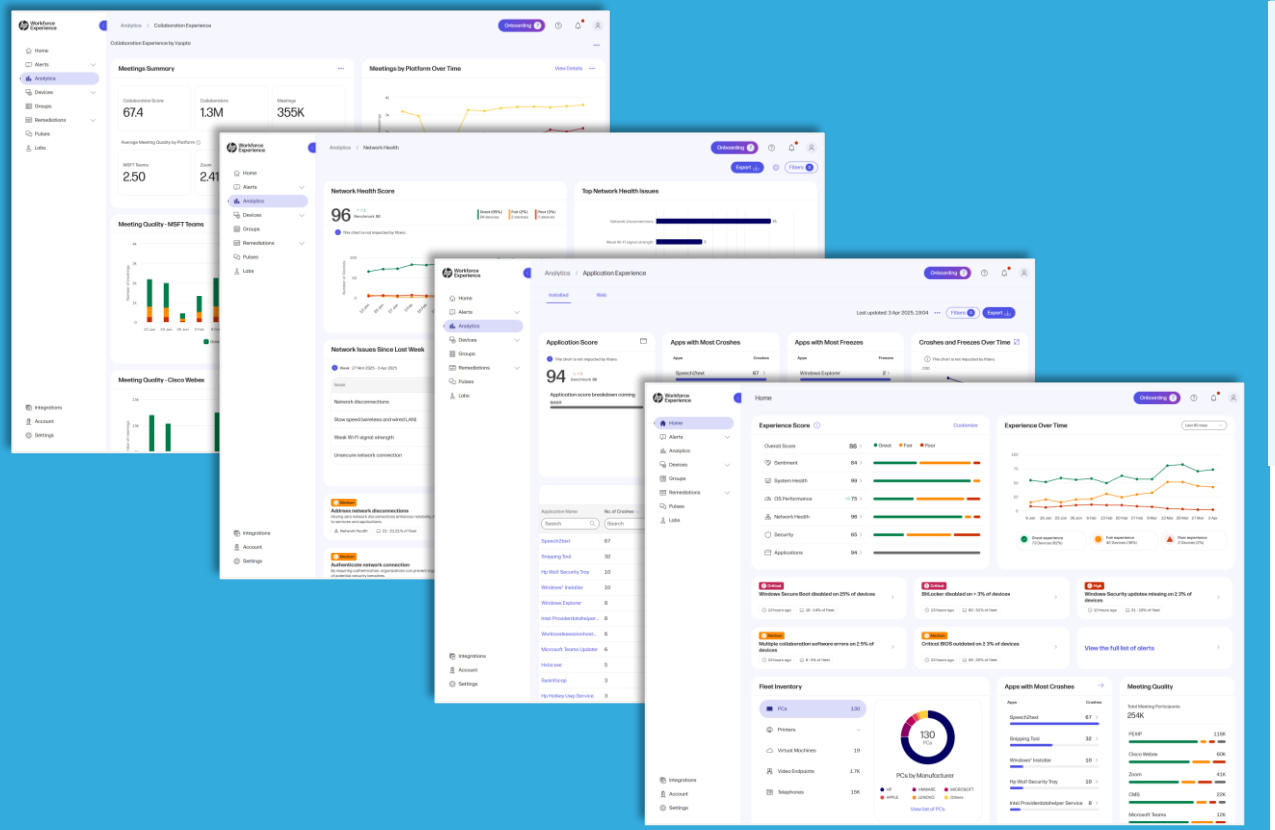
Soluzione software indipendente dall'hardware

Come contribuisce ad adeguarsi a DORA?

- **Gestione del rischio ICT**
  isola le sessioni ad applicazioni critiche, riducendo il rischio di compromissione
- **Protezione dei dati**
  crea un ambiente sicuro per l'elaborazione di dati sensibili
- **Mitigazione dei rischi**
  riduce la superficie di attacco isolando le sessioni ad applicazioni critiche
- **Crittografia e protezione dei dati**
  fornisce un ambiente protetto per operazioni sensibili
- **Resilienza digitale**
  mantiene le operazioni critiche sicure anche in caso di compromissione del sistema principale

Monitora e governa i tuoi dispositivi

con HP Workforce Experience Platform (WXP)



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 WXP

- 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 DORA?

- **Gestione del rischio ICT**
  offre monitoraggio continuo e analisi predittiva per identificare rischi potenziali
- **Governance e strategia**
  fornisce dati dettagliati per decisioni informate sulla sicurezza IT
- **Mitigazione dei rischi**
  identifica proattivamente problemi potenziali prima che diventino critici
- **Reportistica degli incidenti**
  raccoglie dati dettagliati utili per l'analisi post-incidente
- **Test di resilienza digitale**
  fornisce metriche per valutare la resilienza del sistema
- **Monitoraggio continuo**
  offre analisi in tempo reale dello stato di sicurezza degli asset IT

Riepilogo mappatura

Requisito DORA	Soluzioni HP che contribuiscono a rispettarlo
Gestione del rischio ICT	**Sure Start** (protezione BIOS), **Sure Click** (isolamento minacce web), **Sure Access** (isolamento app critiche), **Platform Certificate** (verifica integrità hardware), **Workforce Experience Platform** (monitoraggio asset), **Protect & Trace** (sicurezza dispositivi mobili)
Governance e strategia	**Sure Admin** (gestione sicura configurazioni), **Workforce Experience Platform** (visibilità asset IT), **Protect & Trace** (gestione dispositivi), **Platform Certificate** (verifica integrità sistemi)
Protezione dei dati	**Sure Access** (ambiente isolato per dati sensibili), **Sure Click** (protezione da attacchi), **Protect & Trace** (cancellazione remota dati)
Mitigazione dei rischi	**Sure Start** (ripristino automatico BIOS), **Sure Click** (contenimento minacce), **Sure Access** (riduzione superficie attacco), **Platform Certificate** (rilevamento manomissioni), **Workforce Experience Platform** (identificazione vulnerabilità), **Protect & Trace** (gestione rischi mobilità)
Reportistica degli incidenti	**Sure Recover** (minimizzazione downtime), **Workforce Experience Platform** (dati per analisi), **Protect & Trace** (tracciamento dispositivi), **Platform Certificate** (segnalazione anomalie)
Test di resilienza digitale	**Sure Recover** (test recupero), **Workforce Experience Platform** (valutazione resilienza), **Platform Certificate** (verifica integrità)
Gestione dei fornitori ICT	**Workforce Experience Platform** (monitoraggio asset fornitori), **Protect & Trace** (gestione dispositivi forniti), **Platform Certificate** (verifica componenti supply chain)
Condivisione delle informazioni	**Workforce Experience Platform** (dati aggregati minacce), **Protect & Trace** (informazioni sicurezza mobile), **Platform Certificate** (dati integrità sistema)
Formazione del personale	**Workforce Experience Platform** (identificazione necessità formative), **Protect & Trace** (formazione sicurezza mobile)
Aggiornamento continuo	**Sure Start** (aggiornamento BIOS), **Sure Click** (protezione nuove minacce), **Workforce Experience Platform** (monitoraggio aggiornamenti), **Platform Certificate** (verifica integrità aggiornamenti)
Piani di continuità operativa	**Sure Recover** (ripristino rapido), **Workforce Experience Platform** (pianificazione preventiva), **Protect & Trace** (continuità mobile), **Platform Certificate** (verifica integrità ripristino)
Crittografia e protezione dei dati	**Sure Access** (ambiente protetto)
Monitoraggio continuo	**Sure Admin** (monitoraggio accessi), **Workforce Experience Platform** (monitoraggio asset), **Protect & Trace** (monitoraggio dispositivi), **Platform Certificate** (monitoraggio integrità)
Resilienza digitale	**Sure Start** (recupero BIOS), **Sure Access** (isolamento operazioni), **Sure Recover** (ripristino sistema), **Platform Certificate** (affidabilità hardware), **Workforce Experience Platform** (ottimizzazione asset), **Protect & Trace** (resilienza mobile)


HP WOLF SECURITY
GRAZIE