
Lenovo
Health
Protezione dei dati sanitari ovunque
Un approccio smarter per bloccare le minacce in evoluzione
ThinkShield
Windows 10
Smarter technology for all
Lenovo

La sicurezza IT nel settore sanitario è un obiettivo sempre più complesso

Qualsiasi responsabile aziendale, se interpellato, indicherà le minacce informatiche tra i principali motivi di preoccupazione. Ciò è particolarmente vero nel settore sanitario, che è costantemente quello preso maggiormente di mira dagli hacker.

Le cartelle cliniche dei pazienti sono tra gli asset più preziosi disponibili nel Dark Web perché contengono moltissime informazioni, tra cui data di nascita, dati della carta di credito, codice fiscale, e-mail e indirizzo postale. Una singola cartella può fruttare fino a 780 sterline.[1]

Con una cifra del genere, non c'è da stupirsi che la frequenza degli attacchi ai dati sanitari sia aumentata anno dopo anno.

Nel 2019 è avvenuta la violazione di 41 milioni di cartelle cliniche dei pazienti, una quantità quasi tre volte superiore a quella dell'anno precedente.[2]

IL COSTO SEMPRE PIÙ ALTO DELLE VIOLAZIONI DEI DATI SANITARI

I costi conseguenti alle violazioni dei dati continuano ad aumentare per le organizzazioni sanitarie. In media, le violazioni dei dati costano al settore sanitario 5 milioni di sterline, ovvero il 60% in più rispetto a tutti gli altri settori. Ogni cartella clinica persa o rubata è costata 335 sterline nel 2019 e fino a 318 sterline nel 2018.[3]

MAAS (MALWARE COME SERVIZIO)

L'attuale aumento delle minacce informatiche nel settore sanitario è dovuto alla proliferazione di sofisticati strumenti di hackeraggio. Gli utenti malintenzionati non devono più scrivere codice complesso per sferrare un attacco, ma basta un clic. I siti Web ora offrono il malware come servizio.[4]

Lenovo Windows 10

Un panorama sempre più complesso

Il settore sanitario sta cambiando in modi che rendono più complessa la difesa dalle minacce in evoluzione e in aumento.

L'incremento della mobilità espande la superficie di attacco

Tra le tendenze più evidenti che influiscono sulla sicurezza c'è il notevole aumento della diffusione della tecnologia mobile. Da un recente sondaggio tra i responsabili delle decisioni IT nel settore sanitario è emerso che il 90% sta attualmente implementando o sta pianificando di implementare un programma di mobilità.[5]

Con una maggiore quantità di endpoint e di dati in transito in più reti, la vulnerabilità alle minacce aumenta rapidamente. Come ha sottolineato il National Institute of Standards and Technology (NIST) in una recente pubblicazione, tutte le informazioni sui pazienti che vengono raccolte, archiviate, elaborate o trasmesse tramite dispositivi mobili sono particolarmente vulnerabili agli attacchi.[6]

Eppure, secondo il sondaggio dell'HIMSS sulla sicurezza informatica, meno del 5% degli intervistati ha incluso i dispositivi mobili nei test di penetrazione.[7]

La diffusione sempre maggiore dell'uso dei dispositivi mobili da parte degli operatori sanitari e, in generale, per l'assistenza medica, pone sfide significative per i team IT che operano in questo settore, molti dei quali lavorano a loro volta da remoto.

Normative e conformità

Qualsiasi soluzione tecnologica deve essere valutata con un criterio aggiuntivo prima di poter essere considerata applicabile in ambito sanitario: la soluzione aiuta l'organizzazione a conformarsi ai più alti standard normativi?

Le tecnologie che soddisfano gli standard di sicurezza in altri settori potrebbero non essere conformi agli standard HIPAA per la privacy dei pazienti o alle linee guida per la prescrizione elettronica di sostanze controllate (EPCS).

Sicurezza e convenienza

Nel flusso di lavoro dell'assistenza sanitaria vengono integrate misure di sicurezza sempre maggiori, mentre i medici si impegnano a fornire ai pazienti cure salvavita il più rapidamente possibile. I livelli di sicurezza possono causare interruzioni o ritardi significativi in questi flussi di lavoro e avere un impatto negativo sui risultati riscontrati dai pazienti. I medici sprecano già fino a 45 minuti per turno semplicemente per l'accesso ai sistemi informatici e la disconnessione.8 Di conseguenza, il 41% delle aziende del settore sanitario afferma di aver consapevolmente sacrificato la sicurezza a favore della convenienza o delle prestazioni aziendali.[9]

La sicurezza richiede un approccio incentrato sulle persone

La sicurezza IT nel settore sanitario deve essere perfettamente integrata e onnipresente, ma contemporaneamente adattarsi alle modalità di lavoro degli operatori sanitari. Deve supportarli e fornire loro gli strumenti necessari, proteggendo nel contempo l'organizzazione e i suoi dati.

Sicurezza integrata sin dalla fase di progettazione

Un approccio smarter alla sicurezza IT nel settore sanitario.

ThinkShield è una soluzione personalizzabile che protegge i dati e le tecnologie aziendali importanti con protezione completa end-to-end. Non si tratta di un prodotto autonomo, ma di una combinazione unica di hardware, software, servizi e processi integrati nei dispositivi Lenovo per proteggere le soluzioni IT del settore sanitario attraverso quattro aspetti chiave.

Il concetto di sicurezza integrata sin dalla fase di progettazione inizia con lo sviluppo di requisiti di sicurezza standard per proteggere ogni dispositivo nel panorama delle minacce attuale e in evoluzione.

Questo approccio continua con prassi e politiche efficaci per la protezione della supply chain.

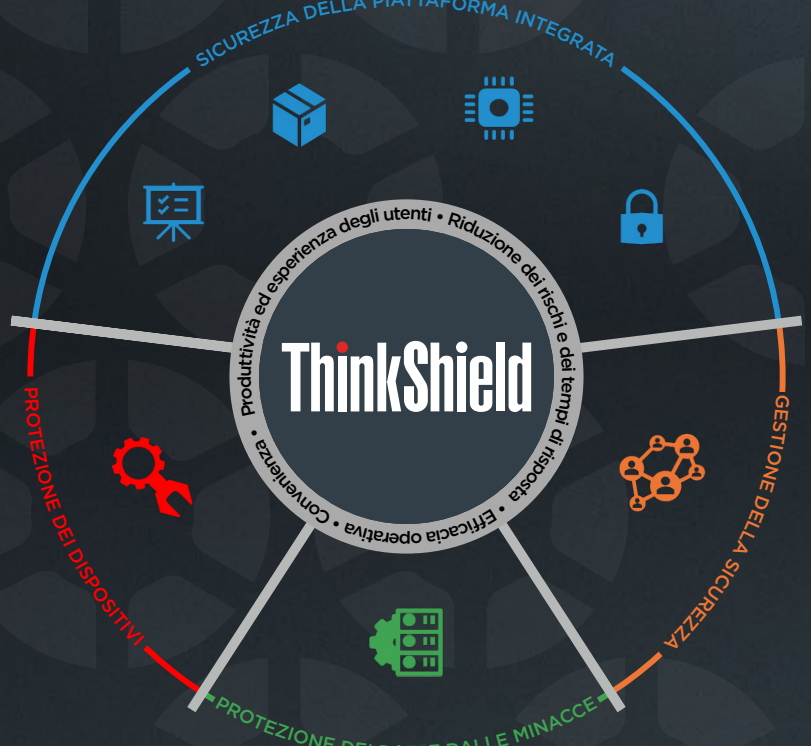
Il nostro programma Trusted Supplier Program prevede un processo di verifica rigoroso per garantire che ogni fornitore di componenti e software Lenovo soddisfi i più alti standard per la sicurezza end-to-end della supply chain. I requisiti per i fornitori includono verifiche di conformità trimestrali, revisioni della protezione degli asset in loco e implementazione del necessario controllo dei processi logistici e di sicurezza delle informazioni.

ThinkShield fornisce privacy, sicurezza e protezione per l'ambiente IT del settore sanitario.

Sicurezza di Windows

Gestione semplice e flessibile.

Windows 10 Pro semplifica la gestione di identità, dispositivi e applicazioni permettendoti di concentrarti sul business. In un ambiente in rapida evoluzione, il successo aziendale è definito dalla capacità di adattarsi senza rimanere indietro. Connettiti facilmente alle reti aziendali esistenti e ai moderni strumenti per la gestione basata sul cloud. Con un controllo intuitivo sulla tua infrastruttura IT, la tua azienda sarà pronta a tutto.



SICUREZZA DELLA PIATTAFORMA INTEGRATA
Il nostro approccio olistico alla sicurezza inizia con le soluzioni di protezione ThinkShield integrate e di serie nei dispositivi Think® fondamentali per il settore.

PROTEZIONE DEI DISPOSITIVI
Servizi e funzionalità per la sicurezza dell'hardware che aggiungono un ulteriore livello di protezione dei dispositivi.

PROTEZIONE DEI DATI E DALLE MINACCE
Soluzioni di sicurezza che si integrano perfettamente con i dispositivi Lenovo garantendo la protezione di tecnologie aziendali e dati critici.

GESTIONE DELLA SICUREZZA
Soluzioni che forniscono funzionalità per la distribuzione, il monitoraggio e la creazione di report per gli asset IT.

Lenovo Windows 10

Privacy: proteggere i dati dei pazienti e le attività cliniche

L'ambiente sanitario è in continuo movimento e le misure di sicurezza devono restare al passo. Non sempre è facile sapere chi può vedere lo schermo di un dispositivo durante un turno. È per questo che offriamo PrivacyGuard e la protezione dagli sguardi indiscreti.

PrivacyGuard offre un filtro e-privacy integrato che impedisce ad altre persone di guardare da dietro le tue spalle per ottenere informazioni preziose, senza la necessità di filtri per la privacy da acquistare successivamente e che spesso vengono persi o gettati via e devono essere sostituiti. La presenza di un filtro e-privacy preinstallato garantisce maggiore sicurezza e una preoccupazione in meno per il team IT e gli utenti.

La protezione dagli sguardi indiscreti incorpora una tecnologia di rilevamento degli sguardi indesiderati che avvisa l'utente se qualcun altro sta guardando lo schermo e rileva persino il lato dello schermo interessato. La funzione di rilevamento degli sguardi indesiderati consente anche di sfocare automaticamente lo schermo quando l'utente distoglie lo sguardo.

La protezione dagli sguardi indiscreti include la funzionalità integrata di rilevamento della presenza, che blocca il dispositivo per garantire la sicurezza quando l'utente si allontana.

La sicurezza della piattaforma integrata ThinkShield include un otturatore per la webcam a tutela della privacy, che copre sia le webcam normali che quelle a infrarossi. Questo otturatore fisico della webcam offre ai pazienti e agli utenti la tranquillità di sapere che la webcam non è accesa o soggetta a un attacco di un hacker.

L'approccio di ThinkShield alla privacy si estende fino alla fine del ciclo di vita di un dispositivo, con più opzioni per lo smaltimento sicuro in modo da proteggere la privacy dei pazienti.

La funzione Secure Wipe, per la cancellazione sicura del BIOS, elimina in modo affidabile tutti i dati da un'unità senza la necessità di strumenti esterni.

Il servizio Keep Your Drive consente ai clienti di conservare l'unità disco fisso di un dispositivo in caso di guasto, eliminando la necessità di monitorare le unità in transito.

THINKPAD® T14I HEALTHCARE EDITION
Tutte queste funzionalità di ThinkShield sono disponibili con ThinkPad T14i Healthcare Edition, un notebook professionale che offre agli operatori sanitari le prestazioni che hanno decretato il successo globale della famiglia ThinkPad®, con funzionalità e opzioni progettate specificamente per soddisfare le esigenze degli ambienti sanitari.

Lenovo Windows 10

Sicurezza: proteggere i pazienti riducendo i vettori di trasmissione

Oggi più che mai è fondamentale seguire i protocolli di prevenzione delle infezioni. Un volume di documentazione in continua crescita mostra che il tasso di contaminazione batterica dei dispositivi mobili degli operatori sanitari varia dal 40% a quasi il 100%, ma nonostante questo addirittura il 90% degli operatori a contatto con i pazienti non pulisce mai i propri telefoni cellulari.[10]

Ma ci sono anche alcune buone notizie. Non ci vuole molto per ridurre tutta questa contaminazione. Da uno studio è risultata una riduzione della contaminazione dal 36% al 100% entro cinque minuti dal semplice utilizzo di una salviettina umidificata antibatterica.[11] Secondo un altro studio, la contaminazione batterica viene dimezzata con 15 secondi di frizione con alcol isopropilico al 70%.[12]

Uno studio condotto presso un ospedale ha mostrato la presenza di agenti patogeni sull'80% dei telefoni cellulari e sull'81% delle mani dei medici che hanno maneggiato quei telefoni.[13]

Lenovo prende molto sul serio la salute e la sicurezza dei suoi utenti e dei loro pazienti. È per questo che i nostri dispositivi per il settore sanitario hanno funzioni appositamente progettate che includono:

- Un trattamento antibatterico della superficie conforme a ISO 22196
- Test approfonditi in base gli standard CDC per la resistenza a una pulizia profonda durante la giornata, con prodotti rinomati come salviettine Virox Accel, salviettine germicide PDI e Meliseptol B. Braun
- Durata per oltre 10.000 cicli di pulizia durante la vita del dispositivo
- Applicazione software Lenovo Quick Clean che sospende l'input dell'utente in modo da consentire l'esecuzione rapida dei cicli di pulizia senza spegnere il dispositivo
- Timer di Lenovo Quick Clean che può essere personalizzato per garantire un tempo di contatto adeguato per operazioni di pulizia e disinfezione corrette
- Test di conformità alle specifiche militari per garantire resistenza a umidità, basse/alte temperature, polvere, vibrazioni e muffa

Le infezioni ospedaliere colpiscono un paziente ricoverato su 25 negli Stati Uniti, con conseguente perdita di decine di migliaia di vite e costi di miliardi di dollari per il sistema sanitario. Le prassi di prevenzione delle infezioni come quelle descritte possono tuttavia ridurre le infezioni ospedaliere fino al 70%.[14]

Lenovo Windows 10

Sicurezza: autenticazione e dati

Limitare l'accesso ai dati sanitari solo agli utenti autorizzati è una prassi di sicurezza importante nell'ambiente sanitario. ThinkShield offre diversi modi per verificare l'identità di un utente, tra cui funzionalità di autenticazione a più fattori senza intoppi.

SICUREZZA DELLA RETE
In base all'indirizzo IP del dispositivo

SICUREZZA GPS
In base alla geolocalizzazione

RICONOSCIMENTO FACCIALE
Webcam a infrarossi con supporto per Windows Hello

BLUETOOTH
Per l'autenticazione di prossimità basata sul telefono

PASSWORD E PIN
PIN di protezione Intel Authenticate, PIN di Windows 10 digitato e PIN visivi

LETTORE DI IMPRONTE DIGITALI MATCH ON CHIP
Con algoritmi anti-spoofing Quantum Matcher

CONFORMITÀ A FIPS 201
Conformità ai requisiti EPCS

NFC
Accesso touch sicuro con tecnologia NFC compatibile con tutti i principali provider di servizi Single Sign-On, incluso Imprivata®

La presenza di tutte queste funzionalità integrate significa che i dispositivi protetti da ThinkShield rispettano perfettamente i protocolli di sicurezza esistenti senza necessità di hardware aggiuntivo.

Lenovo Windows 10

ACCESSO SINGLE SIGN-ON PER RISPARMIARE TEMPO

Da uno studio recente è emerso che l'accesso SSO ha aiutato un ospedale a ridurre il tempo medio di accesso dei medici da 29,3 a 8,9 secondi, con una diminuzione del 69%. Nel corso di una settimana, presso una struttura, il tempo totale risparmiato è stato di 49,7 ore o circa quattro turni di 12 ore.[15]

Sicurezza: protezione degli endpoint in tempo reale

ThinkShield include funzionalità progettate specificamente per la protezione degli endpoint in tempo reale all'interno e all'esterno di una struttura sanitaria.

SentinelOne: protezione autonoma degli endpoint
SentinelOne offre protezione antivirus all'avanguardia basata su intelligenza artificiale comportamentale brevettata. Questo tipo di rilevamento delle minacce autonomo e avanzato sostituisce completamente una soluzione antivirus e include la tecnologia EDR (Endpoint Detection and Response) attiva per le tipologie di malware note e sconosciute, che consente la riparazione automatica e istantanea dei dispositivi in caso di modalità di attacco su larga scala.

WinMagic: crittografia dell'unità
Crittografia su larga scala con numerose possibilità di configurazione per l'ambiente aziendale, per proteggere le informazioni sensibili archiviate nei dispositivi. Gestisci la crittografia sui dispositivi in tutte le piattaforme da una posizione centrale, usando SecureDoc FDE, FileVault2, BitLocker, dm-crypt e SED (Self-Encrypting Drive). Monitora facilmente la crittografia e gestisci le chiavi per dispositivi SecureDoc e per applicazioni, piattaforme ed entità di terze parti attraverso un'unica console.

Absolute®: visibilità e controllo sugli endpoint
Incorporato direttamente nel firmware dei dispositivi Lenovo, Absolute è uno strumento per la visibilità e il controllo sugli endpoint che consente una gestione persistente della sicurezza. Automatizza il controllo dell'integrità degli endpoint con il supporto di capacità di riparazione automatica. Il controllo sulle correzioni in tempo reale consente l'analisi remota delle minacce potenziali e suggerisce le azioni da intraprendere qualora si verifichi un problema di sicurezza.

Lenovo WiFi Security: protezione dei dati all'interno e all'esterno degli istituti
Lenovo WiFi Security rileva automaticamente le attività sospette e protegge i dispositivi dagli attacchi attraverso una rete Wi-Fi. Quando un utente è fuori sede, l'agente locale controlla i dettagli del punto di accesso in cerca di eventuali comportamenti di vulnerabilità, esegue un'analisi del rischio locale e avvisa gli utenti in caso di comportamenti sospetti nel punto di accesso.

LENOVO VIRTUAL ROUNDING

Scopri come la soluzione Lenovo Virtual Rounding offre comunicazioni faccia a faccia sicure nell'ambiente sanitario, contribuendo nel contempo a ridurre la diffusione di infezioni ospedaliere.

Equilibrio tra protezione e produttività

La protezione dei dati dei pazienti dalle minacce esterne e dall'esposizione interna è una sfida continua. Allo stesso tempo, le misure di sicurezza devono supportare i flussi di lavoro dinamici caratteristici dell'attuale ambiente sanitario e consentire l'accesso tempestivo ai dati critici dei pazienti quando è necessario.

I dispositivi Lenovo per il settore sanitario protetti da ThinkShield aiutano a raggiungere un equilibrio con potenti funzionalità progettate per offrire privacy, protezione e sicurezza nel moderno ambiente sanitario.

Visita **techtoday.lenovo.com/it/it/solutions/healthcare** per maggiori informazioni.

Lenovo Windows 10

Diventa smarter con Lenovo Health

Windows 10

Contatta Lenovo Health. Siamo esperti nell'abbattere le barriere e nel costruire soluzioni smart. Quando vuoi, siamo qui per aiutarti.

Contatta il rappresentante commerciale Lenovo Health o il Business Partner locale

Visita **www.lenovo.com/health**

FONTI

1 https://www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.html

2 https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats

3 https://healthitsecurity.com/news/data-breaches-cost-healthcare-6.5m-or-429-per-patient-record

4 https://www.itprotoday.com/cloud-security/malware-taking-new-shape-malware-service

5 https://healthitsecurity.com/news/mobile-devices-in-healthcare-increase-as-do-security-challenges

6 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-1.pdf

7 https://www.healthcareitnews.com/news/protecting-endpoints

8 Statistica fornita da Imprivata nel webinar "Shielding Healthcare Data from Cyberthreats: Tools You Can Use from A to V", maggio 2019.

9 Statistica fornita da Imprivata nel webinar "Shielding Healthcare Data from Cyberthreats: Tools You Can Use from A to V", maggio 2019.

10 https://orb.binghamton.edu/cgi/viewcontent.cgi?article=1001&context=alpenglowjournal

11 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6210060/

12 https://www.myamericannurse.com/mobile-devices-healthcare-associatedinfections/

13 https://www.healthcareitnews.com/news/ensuring-computers-notebooks-andmobile-devices-are-included-disinfection-mix

14 https://www.healthypeople.gov/2020/topics-objectives/topic/healthcareassociated-Infections

15 https://www.beckershospitalreview.com/healthcare-information-technology/how-single-sign-on-within-ehrs-can-save-clinicians-time-reduce-hospital-costs-improve-patient-care.html

Lenovo