ivanti Neurons

Sanità IT, Biomedicale, Sicurezza

Guida al miglioramento della visibilità e alla mitigazione dei rischi per la sicurezza dei dispositivi medici

Contenuti

Introduzione

I dispositivi medici connessi rappresentano un'enorme sfida per le organizzazioni sanitarie IT, biomediche e di sicurezza. Sono intrinsecamente vulnerabili alle minacce informatiche, e gli attacchi informatici andati a buon fine possono avere conseguenze terribili. Eppure le misure di sicurezza informatica tradizionali non possono essere applicate a questi dispositivi e possono persino rischiare di interferire con attività cliniche critiche.

In questa guida illustriamo un processo in tre fasi per aumentare la visibilità sui dispositivi medici e migliorare la mitigazione dei rischi per la sicurezza. L'implementazione di livelli di sicurezza informatica per i dispositivi medici è un processo continuo a più fasi, che può avere successo se parte da una base solida e adotta un approccio metodico e sistematico.

Impara come scoprire, valutare e mitigare i rischi per la sicurezza informatica associati ai dispositivi medici connessi. Le tre fasi che presentiamo in questa guida non costituiscono un processo una tantum, ma, piuttosto, dovrebbero essere considerate come un ciclo. I team IT e di sicurezza dei centri sanitari dovrebbero attuare continuamente queste fasi, esaminando l'ambiente, valutando i rischi e affrontando i problemi di sicurezza che scoprono giorno per giorno.

Quanto sono vulnerabili i dispositivi medici agli attacchi informatici?

Sempre più dispositivi medici sono connessi alle reti o ad altri dispositivi, e, per questo, rappresentano una grave vulnerabilità della sicurezza per ospedali e operatori sanitari. Molti di questi dispositivi non sono sicuri e non sono gestiti attivamente, il che apre la porta a un'ampia gamma di minacce alla sicurezza informatica.

Perché i dispositivi medici sono vulnerabili?

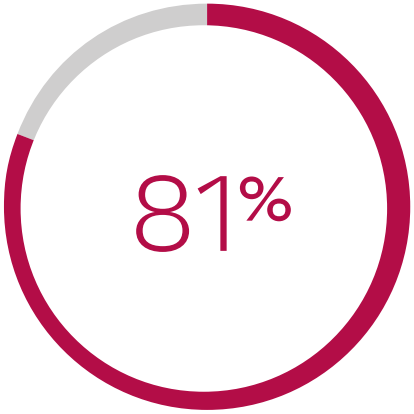
- Il codice software non è stato sottoposto a un controllo della sicurezza.
- L'autenticazione è debole o inesistente.
- I canali di trasferimento dei dati sono spesso insicuri e non crittografati.
- Visibilità limitata sui dispositivi che vengono utilizzati attivamente.
- Incapacità di monitorare l' attività del dispositivo e gli incidenti di sicurezza.

Capire l'ambiente
Scoprire quali dispositivi medici e IT esistono, classificarli accuratamente, comprendere il loro contesto clinico e identificare le loro esigenze di rete.

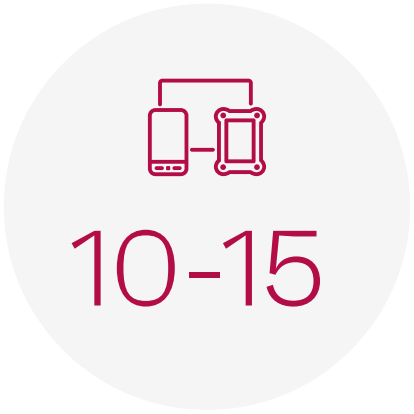
Valutazione del rischio
Identificare le vulnerabilità dei dispositivi e i rischi relativi alla rete, assegnando a ciascun dispositivo un indice di rischio e fornendo suggerimenti per la bonifica.

Dispositivi di protezione
Affrontare la sicurezza a livello di dispositivo, isolando i dispositivi all'interno della LAN, prevenendo comunicazioni indesiderate su LAN/WAN e preparando una strategia per rilevare gli incidenti di sicurezza quando si verificano.

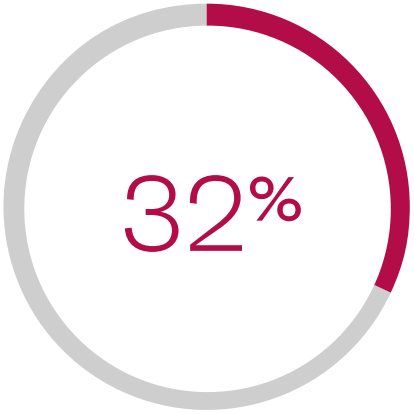
Qual è l'entità del problema?



L'81% delle organizzazioni sanitarie hanno riferito di essere state compromesse da un attacco informatico negli ultimi due anni.



Gli ospedali hanno 10-15 dispositivi medici collegati per posto letto, con oltre 3,7 milioni di dispositivi in uso.



Il 32% delle organizzazioni sanitarie afferma che i dispositivi medici costituiscono la principale preoccupazione per la sicurezza.

Fonte: KPMG, Wired

Quali vettori di minacce colpiscono i dispositivi medici?

Malware
In genere, i dispositivi medici non dispongono di protezione degli endpoint e sono particolarmente vulnerabili al malware.

Minacce interne
A causa dell'autenticazione debole, i malintenzionati possono facilmente ottenere un accesso non autorizzato e manomettere i dispositivi.

Attacchi alle applicazioni Web
Alcuni dispositivi medici possono essere gestiti tramite un'interfaccia web, il che apre la strada a una serie di rischi informatici come l'iniezione di codice, il cross-site scripting (XSS) e il path traversal.

Uso scorretto del dispositivo
I dispositivi medici connessi sono spesso basati su PC Windows. Il personale ospedaliero può utilizzare le macchine per navigare in Internet o installare software, creando rischi aggiuntivi.

Come si valutano il rischio per la sicurezza informatica e l'impatto di un attacco?

Le linee guida della FDA per i dispositivi medici forniscono un'utile classificazione dei livelli di rischio del dispositivo.

TLivello 1: rischio per la sicurezza informatica più elevato	Livello 2: rischio per la sicurezza informatica standard
Il dispositivo è:	**Il dispositivo è:**
In grado di connettersi a un altro prodotto medico o non medico, a una rete o a Internet O Un incidente di sicurezza informatica che interessasse il dispositivo potrebbe danneggiare direttamente uno o più pazienti.	In grado di connettersi a un altro dispositivo o rete, ma non può danneggiare direttamente i pazienti O In grado di danneggiare direttamente i pazienti ma non può connettersi a una rete.

Per ottenere una valutazione più granulare del rischio bisogna utilizzare un framework come il calcolo del rischio CVSS. Quando si valuta il rischio per la sicurezza informatica bisogna tenere

- Vulnerabilità del software
- Sicurezza del paziente
- Autenticazione
- Privacy
- Networking
- Interruzione del servizio

Fase I:

Comprendere l'ambiente del dispositivo connesso

Il primo passo per risolvere un problema è riconoscere che esiste e comprenderne la portata. Il problema dei dispositivi medici connessi non è ben compreso dai team IT, biomedici e di sicurezza degli ospedali e delle organizzazioni sanitarie a causa della visibilità estremamente limitata.

I team di sicurezza vedono i dispositivi medici come delle scatole nere, oppure possono non vederli affatto

La sicurezza dei dispositivi medici sta diventando una responsabilità condivisa dei team di ingegneria clinica e dei reparti IT. Sebbene le informazioni su questi dispositivi siano presenti nelle organizzazioni sanitarie, i team di sicurezza non possono accedervi prontamente.

Le seguenti importanti domande rimangono senza risposta:

1. Quanti dispositivi sono collegati?
2. Che tipo di dispositivi sono?
3. Con quali altri dispositivi o reti comunicano?
4. Il comportamento della rete è normale e previsto o anomalo?

Perché è difficile creare un inventario dei dispositivi medici collegati?

Non è possibile eseguire semplicemente una scansione di rete e identificare i dispositivi medici come si farebbe su una normale rete IT:

- I dispositivi sono sensibili: la scansione attiva della rete può interrompere il funzionamento dei dispositivi medici, quindi è necessario utilizzare il rilevamento passivo
- Invisibili agli strumenti di rilevamento di rete: gli strumenti tradizionali non rileveranno la stragrande maggioranza dei dispositivi medici collegati o potrebbero indicare erroneamente che il dispositivo è una workstation Windows. La maggior parte dei dispositivi medici connessi non pubblicizza le proprie informazioni e il loro rilevamento sulla rete richiede un'attenta analisi del traffico a livello di applicazione.
- Grande numero e varietà di dispositivi: possono esserci decine di migliaia di dispositivi di diversi tipi, fornitori e versioni.
- Flusso continuo: i dispositivi vengono costantemente aggiunti, sostituiti o rimossi dalla rete, spesso senza coinvolgere l'IT, quindi la scoperta e l'inventario devono costituire un processo continuo.

Passo 1. Scoperta

Cercare di creare un database di dispositivi medici con i dati relativi a ciascun dispositivo. Concentrarsi su dati di alta qualità che possono aiutare a determinare rischi e vulnerabilità. In particolare:

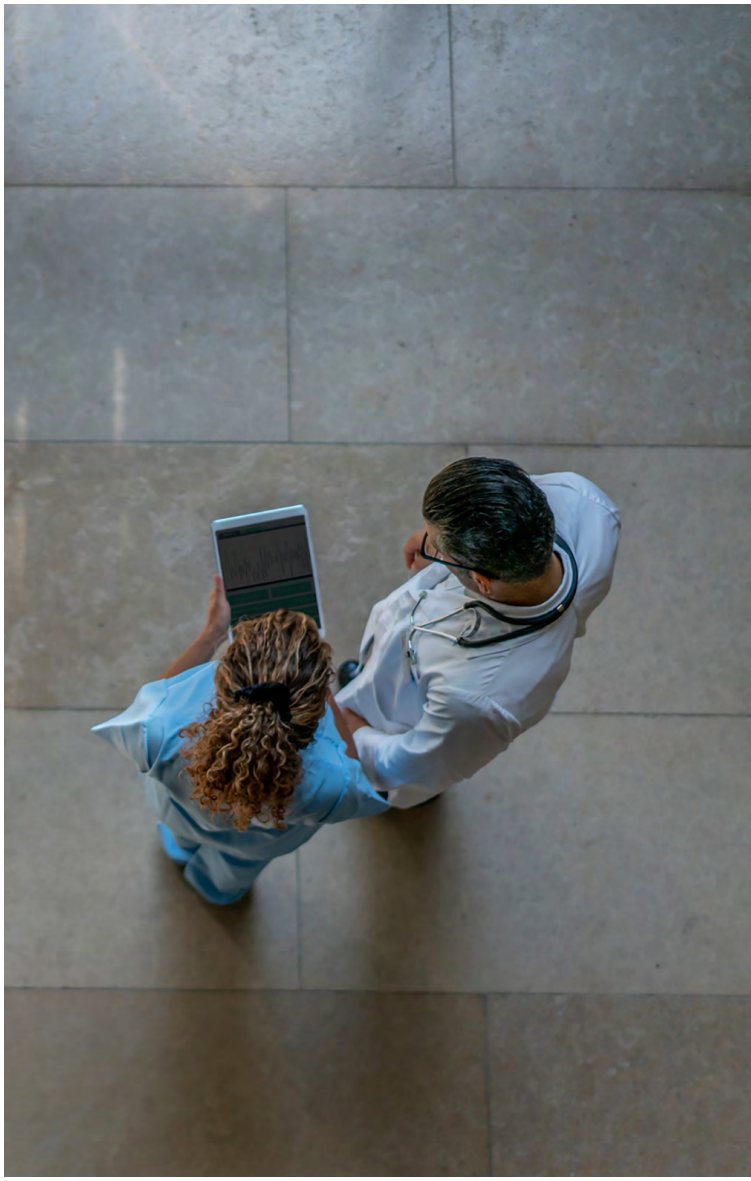
- Tipo di dispositivo
- Reparto e stanza
- Fornitore
- Modello
- Indirizzo IP
- Sistema operativo
- Versione del software applicativo
- Ultima patch di sicurezza

Passo 2. Mappatura della rete e contesto clinico

Comprendere il comportamento di rete di un dispositivo consente di capire quanto sia esposto a minacce esterne e interne. Bisogna cercare di ottenere le seguenti informazioni per ciascuno dei dispositivi collegati:

- Con quali altri dispositivi comunica?
- Questo dispositivo dispone di un accesso non necessario ad altri dispositivi, reti o Internet?
- La comunicazione di rete di questo dispositivo è isolata in una VLAN?
- Quali tipi di protocolli vengono utilizzati?
- Dove il dispositivo invia o riceve dati PHI (Public Health Information) e quale tipo di PHI?
- Comunica esternamente su Internet?
- Il dispositivo deve comunicare con il fornitore del dispositivo su base continuativa?
- Le comunicazioni Internet sono normali per questo tipo di dispositivo?
- La comunicazione Internet di questo dispositivo è isolata in un tunnel VPN?

Chiarire l'uso clinico di ogni dispositivo e, per estensione, la sua esposizione ai rischi. Questi dati possono essere estremamente difficili da ottenere senza l'ausilio di strumenti automatizzati.



Fase II:

Valutazione del rischio

Una volta acquisita una migliore comprensione dei dispositivi medici connessi e creato un inventario dei dispositivi, del loro contesto e del comportamento di rete, è possibile utilizzare questo inventario per valutare i rischi che interessano ogni dispositivo e il loro impatto sull'organizzazione.

Passo 1. Identificare le vulnerabilità del dispositivo e le opportunità di bonifica

Raccogliere dati sulle vulnerabilità per ciascuno dei propri modelli di dispositivo, sistemi operativi e versioni delle applicazioni. Altrettanto importante, individuare il proprietario del dispositivo e il proprio livello di accesso per risolvere i problemi di sicurezza.

Impatto delle vulnerabilità del software
Utilizzare il calcolo del rischio CVSS per identificare l'impatto delle vulnerabilità del software note nei dispositivi collegati.

Errori di configurazione
Verificare la presenza di vulnerabilità generali come password hard-coded o predefinite, sistemi operativi privi di patch o software.

Autenticazione del dispositivo
Verificare se il dispositivo dispone dell'autenticazione e, in tal caso, quanto è robusta e se sono state impostate delle password sicure.

Punto di contatto
Chi gestisce il dispositivo? Ingegneria clinica, IT, il produttore o l'appaltatore di terze parti?

Facilità di accesso
Il team di sicurezza ha accesso a questo dispositivo per implementare i controlli di sicurezza o far fronte agli incidenti?

Backup
Il dispositivo dispone di backup o ridondanza? E qual è l'impatto dell'interruzione del servizio?

Passo 2. Identificare i rischi a livello di rete

Medical device vulnerabilities are only one aspect of the risk. Analyze network connectivity and identify vectors by which attackers can connect to your devices.

Connessione a internet
Controllare se il dispositivo si connette ad altri sistemi su Internet, ad esempio a un'azienda terza o al produttore per la manutenzione o gli aggiornamenti.

Connessioni a dispositivi meno sicuri
Controllare se il dispositivo può connettersi a un dispositivo o endpoint meno sicuro, come la workstation di un medico, e se espone servizi di gestione o dati come FTP o SSH.

Crittografia
Verificare se il dispositivo trasmette o riceve flussi di dati non crittografati.

Protocolli non sicuri
Controllare se il dispositivo utilizza protocolli che offrono un'autenticazione debole, nessuna autenticazione o sono vulnerabili.

Passo 3. Identificare la gravità del rischio

Chiediti: quale sarebbe l'impatto di un attacco informatico andato a buon fine su ciascuno dei tuoi dispositivi? A differenza degli attacchi ai sistemi IT sanitari, l'impatto di un attacco sui dispositivi connessi non si limita alla sicurezza dei dati e alla privacy. Un attacco informatico riuscito potrebbe interrompere le cure mediche e causare danni diretti ai pazienti.

Si consiglia di identificare la gravità del rischio in base alle tre metriche di impatto nel calcolo del rischio CVSS:

- Riservatezza: corrisponde al rischio di esposizione delle Informazioni Sanitarie Protette (PHI, Protected Health Information) memorizzate o trasmesse dal dispositivo.
- Integrità: corrisponde al rischio per la sicurezza del paziente per i dispositivi utilizzati direttamente per la cura del paziente.
- Disponibilità: corrisponde al rischio di interruzione del servizio.

Sicurezza del paziente	Privacy	Interruzione del servizio
BASSO: dispositivo medico FDA classe I; rischio da basso a moderato per il paziente o l'utente.	**BASSO:** il dispositivo non memorizza PHI.	**BASSO:** il guasto del dispositivo non può interrompere la cura del paziente.
MEDIO: dispositivo medico FDA classe II; rischio da moderato ad alto.	**MEDIO:** il dispositivo memorizza una piccola quantità di PHI per un periodo di tempo limitato relativamente a un test o a una cura.	**MEDIO:** il guasto del dispositivo può interrompere la cura del paziente ma non un trattamento medico critico.
ALTO: dispositivo FDA Classe III; rischio elevato, dispositivi per il mantenimento in vita o per il sostegno vitale, sono impiantati o presentano un alto rischio di malattie o lesioni.	**ALTO:** il dispositivo memorizza grandi quantità di PHI relative a più test o cure.	**ALTO:** il guasto del dispositivo può interrompere trattamenti medici critici come interventi chirurgici, apparecchiature respiratorie o la somministrazione di farmaci salvavita.

Fase III:
Proteggere i dispositivi medici connessi

Il vantaggio della nostra procedura strutturata per la scoperta e la valutazione del rischio sta nel fatto di poter classificare i dispositivi in base ai rischi che rappresentano. A ogni dispositivo deve essere attribuito un punteggio di impatto del rischio (per la sicurezza del paziente, la privacy e l'interruzione del servizio).

La propria organizzazione può definire un livello di rischio accettabile. Il team di sicurezza può concentrarsi sulla protezione dei dispositivi il cui punteggio di rischio sia oltre il livello accettabile e può applicare le misure di sicurezza appropriate ai dispositivi con diversi punteggi di rischio.

Consigliamo di proteggere i dispositivi medici collegati in quattro fasi:

1. Protezione del livello dispositivo: applicazione di patch, disabilitazione di servizi vulnerabili, adozione di una configurazione best practice.
2. Protezione del livello rete: isolamento a livello LAN, blocco delle comunicazioni non necessarie all'interno della rete locale e isolamento a livello WAN, consentendo al dispositivo di comunicare solo con entità esterne note.
3. Rilevamento degli incidenti: implementazione di una strategia per rilevare gli incidenti di sicurezza quando questi si verificano.
4. Metriche e analisi: analisi continua dei risultati, modifiche e miglioramenti del programma di sicurezza.

Passo 1. Protezione del dispositivo

Come accade con qualsiasi dispositivo informatico, è necessario assicurarsi che i dispositivi medici connessi dispongano delle patch di sicurezza e degli aggiornamenti software più recenti. La configurazione deve essere rafforzata per abilitare l'autenticazione sicura. Chiudere le porte inutilizzate, limitare le funzioni non necessarie e, in generale, ridurre la superficie di attacco.

La maggior parte dei dispositivi medici funziona con sistema operativo Windows. Tuttavia, applicare una patch non è semplice quanto farlo su una workstation o un server Windows.

Difficoltà nella protezione dei dispositivi medici

- Le patch di sicurezza di Windows devono essere verificate e approvate dal produttore del dispositivo.
- L'ingegneria clinica deve verificare patch o aggiornamenti che non influiscono sulla funzionalità del dispositivo medico.

Linee guida

- Non si riuscirà a distribuire tutte le patch di sicurezza o a proteggere tutti i dispositivi.
- Concentrarsi sui dispositivi con un punteggio di rischio elevato.
- Dare priorità alle patch di sicurezza o alle modifiche alla configurazione che risolvono le vulnerabilità note identificate nella fase di valutazione del rischio.

Passo 2. Isolamento di rete

Una strategia chiave per proteggere i dispositivi medici connessi consiste nell'isolarli, per quanto possibile, dalla comunicazione clinica non critica, per limitare la superficie di attacco. Questa strategia ha due componenti:

- Definizione della segmentazione della rete per garantire che i dispositivi medici connessi possano comunicare solo con dispositivi o sistemi che fanno parte del loro processo clinico.
- Blocco della comunicazione esterna per garantire che i dispositivi medici connessi non si colleghino mai a Internet, a meno che ciò non sia necessario per comunicare con il fornitore del dispositivo o altre entità note.

Considerazioni sull'isolamento dei dispositivi medici

- Isolare i flussi di dati clinici dai flussi di dati non clinici.
- La comunicazione clinica è essenziale, ma qualsiasi altra comunicazione dovrebbe essere bloccata.

Linee guida

- Implementare criteri di accesso rigorosi e segmentazione della rete per limitare le comunicazioni non essenziali da/verso i dispositivi.
- Implementare criteri di segmentazione per affrontare i rischi e le vulnerabilità scoperti nell'analisi dell'impatto.
- Impedire al dispositivo di connettersi a Internet, a meno che ciò non sia assolutamente necessario per il funzionamento del dispositivo e solo per entità conosciute.
- Collaborare strettamente con l'ingegneria clinica e l'Healthcare Technology Management (HTM) per assicurarsi di non interrompere i flussi di dati critici.

Passo 3. Rilevamento degli incidenti e incident response

È impossibile proteggere la maggior parte dei dispositivi medici connessi da tutte le potenziali minacce perché ci saranno sempre dispositivi legacy critici che non possono essere sostituiti e non possono essere completamente "patchati" o isolati. Il che significa che è possibile limitare la superficie di attacco ma non eliminarla. Inoltre, l'isolamento può consistere in un processo lungo e, nel frattempo, alcuni dispositivi rimarranno vulnerabili. Ecco perché è fondamentale monitorare i dispositivi e rilevare e avvisare immediatamente quando si verificano attività insolite.

Considerazioni sul monitoraggio degli incidenti di sicurezza

- Utilizzare il monitoraggio passivo, come un network TAP o una porta mirror, per evitare di interrompere il funzionamento del dispositivo
- Sfruttare le informazioni raccolte sul contesto clinico di ciascun dispositivo per capire cosa rappresenta la normale comunicazione clinica
- Confrontare il comportamento attuale con le specifiche del fornitore, il comportamento pregresso e il comportamento di un gruppo di dispositivi analoghi nel tuo ambiente e in altre organizzazioni

Linee guida

- Monitorare continuamente tutti i dispositivi, prestando particolare attenzione a quelli con un punteggio di rischio elevato
- Stabilire una strategia per confrontare la comunicazione in corso con la normale comunicazione clinica.
- Avvisare la sicurezza di qualsiasi deviazione importante dal comportamento normale.
- Integrare con terze parti che possano aiutare a eseguire bonifiche rapide da remoto, come la segmentazione della rete on-demand.

Passo 4. Metriche e analisi

La sicurezza informatica dei dispositivi medici consiste in un processo lungo, che deve essere mantenuto e migliorato nel tempo per far fronte a un panorama delle minacce in continua evoluzione.

Monitorare i tuoi progressi può aiutarti a capire se ti stai muovendo nella giusta direzione e permetterti di apportare correzioni ove il tuo lavoro non migliori la situazione della sicurezza. Di seguito riportiamo alcune linee guida per monitorare lo stato di avanzamento del progetto di sicurezza dei dispositivi medici.

- Creare una scorecard per i dispositivi medici con una sequenza temporale dei punteggi di rischio, assicurandoti che il rischio si riduca nel tempo Impostare dei KPI in base al rischio di dispositivi importanti e monitorare il miglioramento; collegare i KPI agli obiettivi aziendali come la sicurezza dei pazienti e la disponibilità del servizio per ottenere il consenso della dirigenza
- Identificare attività e strategie che abbiano migliorato i KPI e ridotto gli indici di rischio complessivi.
- Impostare dei KPI in base al rischio di dispositivi importanti e monitorare il miglioramento; collegare i KPI agli obiettivi aziendali come la sicurezza dei pazienti e la disponibilità del servizio per ottenere il consenso della dirigenza.
- Raccogliere dati sugli indici di rischio e sul comportamento storico dei dispositivi e usarli per prendere decisioni migliori in fatto di approvvigionamenti.

Migliorare la visibilità delle risorse e la mitigazione dei rischi per la sicurezza per i dispositivi medici con Ivanti Neurons for Healthcare

Ivanti® Neurons for Healthcare migliora la visibilità delle risorse e la mitigazione dei rischi per la sicurezza per i dispositivi medici. La soluzione rileva e profila in modo intelligente i dispositivi medici e Internet of Medical Things (IoMT), valutando i rischi per la sicurezza, segnalando le minacce e riconciliando le informazioni sui dispositivi tra più fonti di dati. Scopri di più sui vari dispositivi specifici per l'assistenza sanitaria nelle tue strutture, inclusa la classificazione dei dispositivi e le informazioni sull'utilizzo, con i dettagli per ridurre i rischi per la sicurezza o per intervenire in caso di anomalie. Raccogli e riconcilia i dati dei fornitori, creando una "single source of truth" per tutti i tuoi dispositivi medici.

Per ulteriori informazioni, visitare ivanti.it/neurons

ivanti Neurons

ivanti.it/neurons
contact@ivanti.it