# La sicurezza nel settore sanitario esaminata al microscopio

Forescout analizza i dati delle implementazioni per capire meglio i rischi informatici a cui sono esposte le strutture sanitarie.

FORESCOUT®

# Sintesi

Per le strutture che operano in ambito sanitario, la tecnologia IoMT (Internet of Medical Things) continua a rappresentare un mondo di straordinarie possibilità per offrire un migliore livello di assistenza ai pazienti. La trasformazione digitale e l'incremento del numero di sistemi connessi, tuttavia, introducono nuovi rischi per la sicurezza e la riservatezza dei dati. La crescita vorticosa del panorama dei dispositivi ha moltiplicato la complessità delle reti e reso sempre più difficile la gestione della loro sicurezza.

L'obiettivo di questo studio è fornire ai responsabili della sicurezza e della gestione dei rischi che operano nel settore sanitario una panoramica completa sui tipi di dispositivi che si collegano alle loro reti e i rischi specifici che comportano, oltre che suggerire una strategia a 360 gradi per la gestione della sicurezza che vada oltre la semplice protezione dei singoli dispositivi medici.

I dati analizzati in questo studio provengono dal Forescout Device Cloud, uno tra i più grandi archivi in crowdsourcing esistenti che raccoglie dati generati da reti e host ed è alimentato da oltre 8 milioni di dispositivi unici. Ai fini dello studio, i ricercatori hanno ristretto l'analisi a 75 implementazioni che operano in ambito sanitario e che contano più di 10.000 reti locali virtuali e 1,5 milioni di dispositivi. Poiché l'aspetto su cui si concentra lo studio è lo stato dei dispositivi medici, molti risultati sono basati sull'analisi specifica di 430.000 dispositivi attivi in più di 1.500 VLAN di centri sanitari.

**Osservazioni principali**

- **Gli ambienti sanitari moderni sono estremamente diversificati:** il rapido aumento del numero e della varietà di sistemi operativi e di dispositivi medici connessi complica il compito di proteggere la rete.
- **I sistemi operativi Windows obsoleti rappresentano una vulnerabilità colossale:** molte reti utilizzano ancora sistemi operativi Microsoft Windows che non sono più supportati e un'importante scadenza di Windows ormai prossima lascerà scoperti ancora più dispositivi.
- **Mancano le strategie di segmentazione:** la segmentazione della rete, che classifica i dati in base al grado di sensibilità, alla posizione e alla criticità, è una pratica riconosciuta per limitare lo spostamento laterale degli aggressori nella rete, ma non è ancora applicata in maniera sistematica nelle moderne reti eterogenee.
- **La quantità di dispositivi di marche diverse in rete deve essere tenuta sotto controllo:** la proliferazione eccessiva delle marche di dispositivi causa problemi di interoperabilità, sicurezza e gestione delle risorse non indifferenti.
- **I servizi generici perennemente attivi rendono la rete vulnerabile:** i protocolli comuni lasciati aperti espongono la rete ad attacchi incontrollati.

# Lo stato della sicurezza informatica nel settore sanitario

La tecnologia IoMT si sta imponendo come priorità strategica perché ha il potenziale di migliorare la cura dei pazienti, fornire dati clinici più precisi, aumentare l'efficienza dei servizi e ridurre i costi dell'assistenza sanitaria. Il motivo che spinge le strutture sanitarie verso un'adozione rapida della tecnologia IoMT è chiaro: poter godere di un'infrastruttura connessa in cui i dispositivi medici, le applicazioni software, i sistemi e i servizi sanitari sono in comunicazione tra loro. La velocità di questa evoluzione, tuttavia, sta provocando il grave effetto collaterale di introdurre significative lacune nella sicurezza perché fa passare in secondo piano la necessità di gestire a livello globale la sicurezza di questi ambienti basati sulla convergenza superando il concetto di protezione dei singoli dispositivi medici.

La tecnologia IoMT, cioè IoT medicale, è un'infrastruttura che raccoglie dispositivi medici, applicazioni software, sistemi e servizi sanitari connessi. Ai fini di questo studio, IoMT copre le categorie IoT (Internet of Things) e OT (tecnologie operative).

### Aumento esponenziale dei dispositivi IT e OT connessi nel se tore sanitario

La crescita incontrollata del numero di oggetti connessi amplia la superficie di attacco e rende più complesso adeguare le misure di sicurezza alla nuova realtà. Gli oggetti connessi vanno dai dispositivi di tipo medico, come i sistemi di registrazione e identificazione dei pazienti, le pompe di somministrazione e i sistemi di imaging, ai sistemi di gestione delle infrastrutture, come i sistemi di automazione degli edifici, gli impianti di sicurezza, i gruppi di continuità, i generatori di corrente e tutte quelle strumentazioni OT che sempre più spesso entrano nelle reti IT. Conseguenza diretta di questa convergenza è che la responsabilità della sicurezza OT sta entrando nell'ambito di competenza del reparto IT. Secondo Gartner, "Entro il 2021, il reparto CIO, CISO o CSO gestirà il 70% della sicurezza OT, rispetto al 35% di quanto avviene oggi".[1]

### Comprendere i rischi e classificarli in base alla gravità

La convergenza di queste due reti, che fino a poco tempo fa erano entità separate, può generare una nuova categoria di rischi per la sicurezza. I criminali informatici sono in grado di muoversi lateralmente all'interno di queste reti IT e OT interconnesse. L'elevato numero di fusioni e acquisizioni che caratterizza il settore sanitario, inoltre, contribuisce ad amplificare la portata di queste minacce per la sicurezza.

Ispirandosi al procedimento che si adotta per elaborare una diagnosi clinica e prescrivere un trattamento, i CISO devono individuare precocemente i rischi e definire la migliore linea di condotta. I responsabili della sicurezza e della gestione dei rischi che tentano di mitigare qualsiasi tipo di rischio otterranno solo risultati marginali perché è possibile ottimizzare la produttività, aumentare il ROI e ridurre il rischio complessivo per l'intera rete solo comprendendo appieno le minacce che la insidiano e individuando i dispositivi più a rischio.

### Quanto costa davvero rimandare il contenimento dei rischi

Gli ambiti della sicurezza informatica e della sanità hanno un altro punto in comune: diagnosi e intervento precoci assicurano risultati migliori e costi decisamente più bassi. Consideriamo questi dati: secondo la rivista dell'HIPAA (Health Insurance Portability and Accountability Act), nel 2018, ogni violazione avvenuta in ambito sanitario ha coinvolto in media 17.974 dati.[2] Ponemon ha calcolato che il costo medio di remediation a persona per singolo dato medico violato nel 2018 è stato di 408 dollari.[3] Ciò significa che il costo medio delle attività di contenimento, segnalazione della compromissione e notifica si attesta a 7,3 milioni di dollari per violazione. Ovviamente l'emorragia finanziaria non si ferma qui, perché le strutture sanitarie devono mettere in conto anche significativi danni alla reputazione e all'immagine del marchio, il conseguente impatto negativo sulla fedeltà dei clienti che, specialmente negli Stati Uniti, dura per anni, e infine predisporre un ciclo di verifiche continue e sistematiche per il futuro. L'assioma "paga ora o la pagherai più tardi" non è mai stato più azzeccato.

[1] "Strategic Roadmap for Integrated IT and OT Security" (Roadmap strategica per una strategia di sicurezza IT e OT integrata), Gartner, Inc., maggio 2018, www.gartner.com/doc/3873972/-strategic-roadmap-integrated-it

[2] "Analysis of 2018 Healthcare Data Breaches" (Analisi delle violazioni ai dati del settore sanitario nel 2018), HIPAA Journal, gennaio 2019, www.hipaajournal.com/analysis-of-healthcare-data-breaches/

[3] "2018 Cost of a Data Breach Study: Global Overview" (Costo delle violazioni dati nel 2018: panoramica globale), Ponemon Institute, luglio 2018, https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_ Report.pdf

### I dati medici sono un bottino appetitoso per gli attacchi informatici

Man mano che nuovi dispositivi medici vengono connessi alla rete, la superficie di attacco del settore sanitario si amplia e cresce il numero di hacker che prende di mira le strutture sanitarie per sottrarre dati medici, che figurano tra i dati più sensibili dei consumatori. I criminali informatici ambiscono a impadronirsi di questi dati che possono essere venduti a caro prezzo, visto che contengono informazioni preziose come data e luogo di nascita, dati della carta di credito, codice fiscale, indirizzo fisico ed email.

### Attacchi informatici comuni che prendono di mira le strutture sanitarie

- **Attacchi ransomware con trojan come WannaCry e NotPetya:** si tratta di malware che codifica i file e impedisce al personale medico di accedere ai sistemi e ai dati medici dei pazienti fino al pagamento di un riscatto. Nel maggio 2018 il ransomware WannaCry ha gettato nello scompiglio il sistema sanitario del Regno Unito causando la cancellazione di oltre 19.000 appuntamenti medici. Il Ministero della Salute britannico ha calcolato che il danno finanziario provocato dagli attacchi WannaCry si attesta a 92 milioni di sterline[4]. Nel 2016 l'ospedale Hollywood Presbyterian Medical Center è stato preso di mira da attacchi simili che hanno provocato il blocco della rete informatica per una settimana e impedito l'erogazione di qualsiasi servizio fino al pagamento di un riscatto di 17.000 dollari.[5]
- **Attacchi DoS e DDoS:** l'aggressore satura la rete e i server connessi a Internet di pacchetti di dati al punto da impedire il flusso del traffico regolare per arrivare a un blocco pressoché totale del sistema e delle applicazioni. Questi attacchi sono talvolta utilizzati per distogliere l'attenzione dei responsabili della sicurezza mentre viene contemporaneamente messo in atto un furto di dati. Nel 2014, il gruppo di hacker Anonymous ha sferrato un attacco DDoS ai danni del Boston Children's Hospital. Secondo l'organizzazione Center for Internet Security, l'ospedale ha dovuto sostenere una spesa superiore a 300.000 dollari per rispondere all'attacco e contenerne l'impatto.[6]
- **Furto dell'identità dei dispositivi:** un dispositivo inaffidabile che si spaccia per legittimo si connette alla rete per raccogliere dati. I pirati informatici ricorrono a questa tecnica per sottrarre dati medici o per penetrare nei sistemi di backend. I primi timori per l'hacking degli apparecchi medici emersero quando il Vice Presidente degli Stati Uniti Dick Cheney richiese un intervento sul suo pacemaker per metterlo al riparo dagli hacker. Secondo Wired, i criminali che oggi usano questo tipo di hacking impiegano intenzionalmente un vecchio malware per attaccare dispositivi medici che usano sistemi operativi obsoleti come Windows XP e Windows Server 2003.[7]
- **Attacco Man-in-the-Middle:** un hacker si inserisce in uno scambio di messaggi tra due parti, generalmente con un tipo di frode detta phishing, per raccogliere dati o per spacciarsi per uno dei due. Nell'aprile del 2017, l'Office for Civil Rights del Dipartimento della salute e dei servizi umani degli Stati Uniti d'America ha consigliato alle entità interessate e ai loro partner commerciali di proteggere i dati medici sensibili con il protocollo HTTPS.[8]
- **Malware fileless:** i criminali informatici hanno imparato ad aggirare gli strumenti antimalware tradizionali ricorrendo a un nuovo tipo di malware che risiede unicamente nella memoria dinamica del computer host. Il Ponemon Institute prevede che nel 2019, il 38% degli attacchi conterranno malware fileless.9 Oltre a introdursi tramite browser non aggiornati o non protetti, questi attacchi in memoria spesso sfruttano i punti deboli di Microsoft Windows, come PowerShell e il protocollo RDP (Remote Desktop Protocol).

[4]"Securing Cyber Resilience in Health and Care" (Proteggere la resilienza informatica nel settore sanitario), ottobre 2018, www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update

[5]Articolo del Los Angeles Times, 18 febbraio 2016, www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

[6]"DDOS Attacks: In the Healthcare Sector" (Attacchi DDoS nel settore sanitario), Center for Intenet Security, www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/

[7]"Medical Devices are the Next Security Nightmare" (I dispositivi medici sono il nuovo incubo per la sicurezza), WIRED, marzo 2017, www.wired.com/2017/03/medical-devices-next-security-nightmare/

[8]"Healthcare Organizations Warned of Risk of Man-In-The-Middle Attacks" (Strutture sanitarie bersaglio di attacchi Man-in-the-Middle), HIPAA Journal, aprile 2017, www.hipaajournal.com/healthcare-organizations-warned-risk- man-middle-attacks-8757/

[9]"State of Endpoint Security Risk" (Stato della sicurezza degli endpoint), Ponemon Institute, ottobre 2018, https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf

# Rischi causati dai dispositivi connessi

## Metodologia

Questo studio analizza una porzione dei dati che risiedono nel Forescout Device Cloud, uno tra i più grandi archivi in crowdsourcing esistenti che raccoglie dati generati da reti e host e che è alimentato da oltre 8 milioni di profili di dispositivi unici. I dati del Device Cloud provengono da migliaia di diversi dispositivi di oltre un migliaio di clienti Forescout che condividono dati resi anonimi. Forescout analizza i profili dei dispositivi del suo cloud, identificando funzione, marca, modello, sistema operativo e versione, e compila automaticamente un inventario completo e approfondito dei sistemi.

Ai fini dello studio, i ricercatori hanno ristretto l'analisi a 75 implementazioni che operano in ambito sanitario e che contano più di 10.000 reti locali virtuali e 1,5 milioni di dispositivi. Poiché l'aspetto su cui si concentra lo studio è lo stato dei dispositivi medici, molti risultati sono basati sull'analisi specifica di 430.000 dispositivi attivi in più di 1.500 VLAN di centri sanitari.

## Categorie di dispositivi presenti nelle VLAN del settore medico

Il fatto che molte reti siano organizzate per compartimenti stagni crea lacune nella gestione della sicurezza. I tecnici clinici spesso si occupano della sicurezza dei dispositivi medici connessi mentre le squadre operative e i responsabili delle infrastrutture si occupano della protezione dei sistemi di automazione degli edifici. Dato che queste attività avvengono in ambiti separati che non comunicano tra loro, chi è responsabile della sicurezza globale?

Come primo passo, le strutture sanitarie devono sapere quali dispositivi IT, IoT e OT si collegano alle loro reti. È questa consapevolezza che frantuma l'approccio separato alla sicurezza, stimola i gruppi a parlare di strategie di sicurezza e pone le basi per un approccio olistico alla protezione dell'ambiente aziendale.

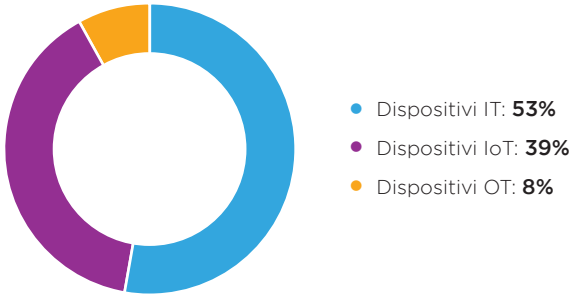
Dato che sempre più dispositivi medici si connettono alle reti, è probabile che il numero di unità in ciascuna delle categorie di dispositivi connessi cambi nel tempo, il che rende fondamentale effettuare una rivalutazione periodica delle misure di sicurezza.

**Figura 1: Categorie di dispositivi nelle VLAN del settore medico**

**Dispositivi IT:** PC, laptop, workstation create appositamente, server, thick client e thin client, hypervisor per la virtualizzazione e strumentazione di rete.

**Dispositivi OT:** dispositivi medici, sistemi per la terapia intensiva, sistemi di automazione degli edifici, impianti di climatizzazione, generatori di elettricità, lettori di badge, telecamere di sicurezza connesse tramite IP e impianti di sicurezza.

**Dispositivi IoT:** telefoni VoIP, stampanti di rete, dispositivi mobili, tablet, controller e convertitori, dispositivi per videoconferenze, sistemi di presentazione, smart TV, console di intrattenimento, accessori vari.

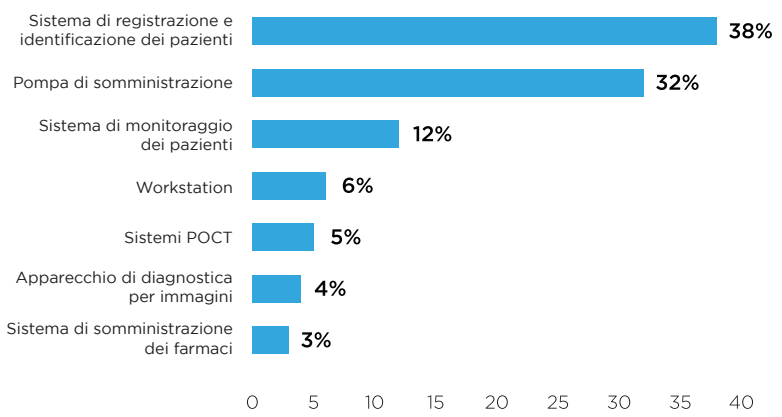


## I dispositivi medici più comunemente connessi

Le strutture mediche di degenza presentano una percentuale maggiore di dispositivi a cui il paziente è collegato. Non c'è da stupirsi che i dispositivi per uso singolo, come i sistemi di registrazione e identificazione, le pompe di somministrazione e i sistemi di monitoraggio, la facciano da padrone nelle reti cliniche, visto che ne viene impiegato uno per ogni paziente.

I sistemi condivisi, come gli apparecchi per la diagnostica di laboratorio e la diagnostica per immagini, sono infatti un numero inferiore. I sistemi più costosi sono quelli che vengono sostituiti meno spesso e che tendono a diventare obsoleti oltre che difficili da aggiornare.

**Figura 2: Dispositivi medici più comunemente connessi**



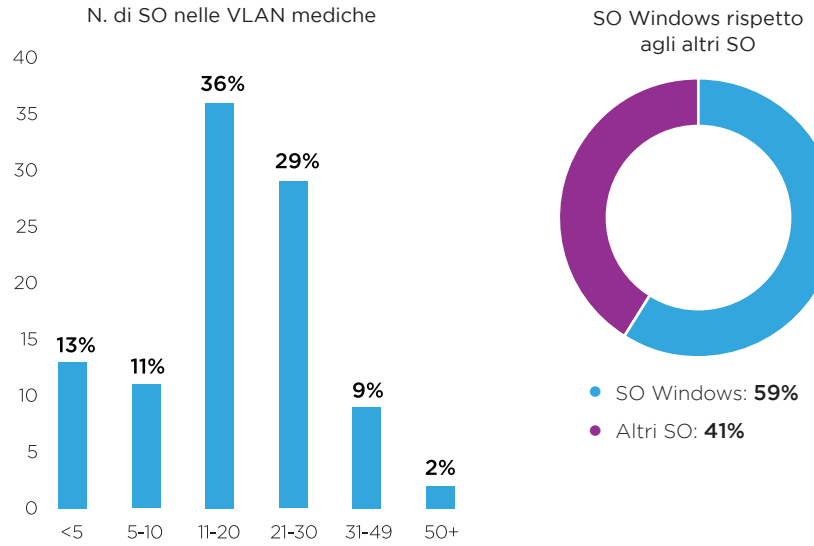

## Eterogeneità dei sistemi operativi

L'eterogeneità dei sistemi operativi contribuisce a complicare la gestione della sicurezza. Dallo studio è emerso che nel 40% delle VLAN del settore medico erano presenti più di 20 diversi sistemi operativi.

Di questi, più della metà (59%) erano sistemi operativi Windows e il 41% un mix che include sistemi operativi mobili, firmware incorporato e infrastrutture di rete. Le operazioni di aggiornamento e applicazione delle patch di sicurezza comportano delle difficoltà, in particolare nei reparti di terapia intensiva, perché i dispositivi devono rimanere online e disponibili. Su alcuni dispositivi medici non è possibile applicare patch di sicurezza, in altri le patch devono essere applicate manualmente e in altri ancora è richiesta l'approvazione della casa produttrice.

Nel 40% delle VLAN del settore medico sono presenti più di 20 diversi sistemi operativi.

**Figura 3: Eterogeneità di sistemi operativi nelle VLAN del settore medico**



### Il problema dei sistemi Windows obsoleti

All'interno del nostro campione di dati, il 70% dei dispositivi con sistema operativo Windows, tra cui Windows 7, Windows 2008 e Windows Mobile, è destinato a rimanere senza supporto a partire dal 14 gennaio 2020. L'utilizzo di sistemi operativi non supportati comporta un rischio che pregiudica la conformità a molte normative.

Con ogni probabilità, i dispositivi gestiti da sistemi operativi obsoleti non verranno sostituiti perché gli aggiornamenti sono costosi e i tempi di inattività che comporta un aggiornamento potrebbero essere semplicemente inaccettabili per i sistemi di terapia intensiva. Tra l'altro, è possibile che alcune vecchie applicazioni non siano compatibili con versioni più recenti di Windows per mancanza di supporto, incompatibilità o problemi di licenze. Dato che le aziende dovranno convivere con la necessità di utilizzare dispositivi medici con sistemi operativi obsoleti ancora per un po', è fondamentale inserire questi dispositivi in segmenti di rete in cui sia possibile proteggere gli importanti dati e servizi che contengono.

Il 71% dei dispositivi utilizzerà sistemi operativi Windows non supportati a partire dal 14 gennaio 2020.

### Utilizzo delle VLAN per la segmentazione

La segmentazione della rete riduce significativamente le superfici di attacco del sistema perché consente agli utenti di vedere unicamente i server e i dispositivi di cui hanno bisogno per svolgere le proprie mansioni. I segmenti vengono creati raggruppando tipi di utenti simili e limitando l'accesso alle sole risorse della rete necessarie per il loro lavoro.

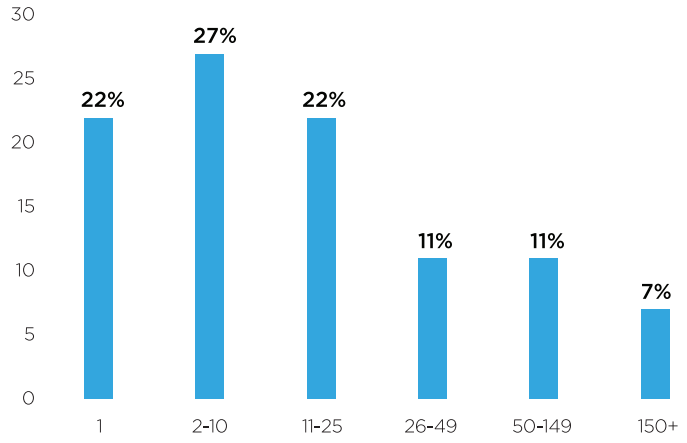
È possibile segmentare la rete in diversi modi. Al livello più basso, si usano le VLAN per segmentare le reti in base alle esigenze e alle priorità dell'azienda, così da isolare efficacemente i dati più critici, segregare i dispositivi simili per funzione o limitare l'accesso a dati, sistemi e altre risorse tramite l'impiego di credenziali. I dati esaminati da questo studio indicano una scarsa presenza di VLAN contenenti dispositivi medici, il che segnala che alcune strutture sanitarie non hanno ancora provveduto a investire nella segmentazione della rete.

Nel 49% delle implementazioni i dispositivi medici sono dislocati in un massimo di 10 VLAN, da cui si evince che la segmentazione è a uno stadio iniziale.

**Figura 4: Sistemi operativi Windows - Il buono, il brutto e il cattivo**

| Il buono | Il cattivo | Il brutto |
|---|---|---|
| 29% | 0,4% | 71% |
| Dispositivi con sistemi operativi Windows per cui è previsto supporto per più di un anno. | Dispositivi con sistemi operativi Windows obsoleti o non supportati. | Dispositivi con sistemi operativi Windows non supportati a partire dal 14 gennaio 2020. |

**Figura 5: N. di VLAN con dispositivi medici**



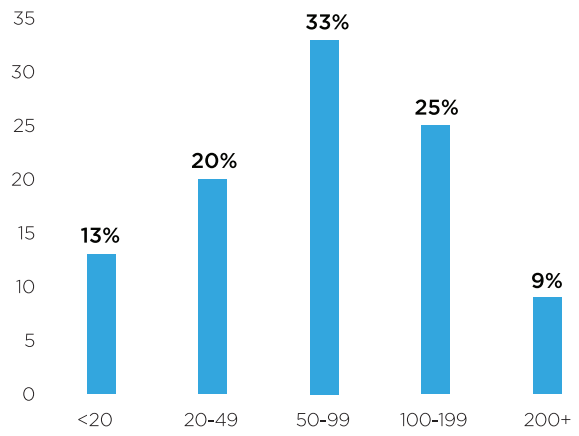
### Aumenta la proliferazione di dispositivi di marca diversa

Le moderne strutture sanitarie sono ambienti tecnologicamente saturi. Dal momento che i fabbricanti dei dispositivi non hanno storicamente progettato i loro prodotti considerando la sicurezza una priorità, ora è più difficile gestirli e mantenerli protetti. Si tratta tra l'altro di dispositivi destinati a connettersi alla rete eludendo le misure e i protocolli di sicurezza. I reparti IT e i responsabili della sicurezza riescono magari a rilevare questi dispositivi connessi senza autorizzazione, ma spesso non sono in grado di classificarli o di localizzarli con facilità.

Gli ambienti informatici che gestiscono più sedi mediche sono, da un punto di vista tecnologico, totalmente eterogenei, tanto che il 30% delle VLAN di strutture sanitarie conta più di 100 diverse marche di dispositivi. E questa babilonia non include le marche presenti nelle reti delle altre aree funzionali, come il back office e il front office. In molti casi, sono i fabbricanti stessi che si fanno carico dell'aggiornamento e della manutenzione dei sistemi clinici specializzati.

**Il 34% delle VLAN di strutture mediche suppor ta dispositivi di oltre 100 marche diverse.**

**Figura 6: N. di marche di dispositivi nelle VLAN del settore medico**




### I servizi generici perennemente attivi rendono la rete vulnerabile

In un sorprendente numero di dispositivi appartenenti a VLAN del settore medico, alcuni servizi ad alto rischio risultano attivi, costituendo un punto di accesso non sorvegliato che gli aggressori possono sfruttare per introdursi nella rete per poi spostarsi lateralmente. I requisiti di accesso stabiliti dai fabbricanti e dai fornitori dei dispositivi medici spesso prevedono l'abilitazione di servizi di protezione come il protocollo RDP di Microsoft. In altri casi, le porte di rete rimangono aperte come prassi all'insaputa del personale IT e dei responsabili della sicurezza.

- **Protocollo Server Message Block (SMB)**: SMB è il protocollo di trasporto che i computer Windows usano per la condivisione dei file, delle stampanti e per l'accesso a servizi remoti di Windows. WannaCry e NotPetya sono due esempi di ransomware che sfruttano le vulnerabilità del protocollo SMB.
- **Protocollo RDP**: altro protocollo comune sfruttato dalle moderne minacce informatiche, come il malware fileless.
- **Protocolli FTP, SSH, Telnet e protocollo di imaging DICOM**: protocolli meno comuni ma che rappresentano vettori spesso sfruttati perché non proteggono né crittografano i dati delle sessioni di rete. I modelli di sicurezza sono scarsamente efficaci negli ambienti legacy in cui troppi dispositivi utilizzano servizi che non prevedono la codifica dei dati.

**Nell'85% dei dispositivi con sistemi operativi Windows, il protocollo è SMB attivato.**

| Servizio Windows | % in cui è attivo |
|---|---|
| SMB | 85% |
| RDP | 32% |
| FTP* | 1% |
| SSH | <1% |
| Protocollo Telnet* | <1% |
| Protocollo di imaging DICOM | <1% |

* Trasmissione in chiaro

# Consigli

È certo: il numero di dispositivi che si connettono alle reti delle strutture mediche è destinato a crescere e l'ambiente diventerà sempre più complesso. Ora è il momento di iniziare a formulare e a implementare una strategia di gestione della sicurezza e dei rischi a livello aziendale basata sulla prevenzione.

**Abilitare l'individuazione senza agent dei dispositivi**
Non c'è dubbio che i dispositivi su cui sono installati agent software possono essere contattati e monitorati più facilmente dai responsabili IT e della sicurezza, però molti dispositivi medici non supportano l'installazione di agent. Ecco perché diventa fondamentale la capacità di individuare tutti i dispositivi con connessione IP nell'intera rete estesa senza ricorrere ad agent.

**Identificare e classificare automaticamente i dispositivi**
Limitarsi ad acquisire gli indirizzi IP dei dispositivi connessi alla rete non è sufficiente. È necessario poterli classificare in modo rapido e preciso per stabilirne lo scopo, il proprietario e lo stato di sicurezza. Queste informazioni devono inoltre essere registrate in un inventario di risorse aggiornato in tempo reale che controlla le policy di accesso e aiuta i responsabili della sicurezza a reagire prontamente agli attacchi diretti a dispositivi o sistemi operativi specifici.

**Monitorare continuamente i dispositivi**
I dispositivi medici devono essere monitorati ininterrottamente affinché gli eventuali cambi di stato possano essere rilevati. Un'analisi sporadica può favorire la diffusione di una mentalità che porta ad affidarsi alla cieca alle soluzioni configurate, trascurando la conformità ed esponendosi ai rischi. Un monitoraggio continuo degli ambienti clinici e OT tramite tecniche di ricerca attive e/o passive, invece, offre una consapevolezza della situazione in tempo reale sulla base della quale i responsabili della sicurezza possono monitorare dati e comportamento dei dispositivi in modo efficiente e produttivo.

**Segmentare la rete**
La segmentazione della rete è una pratica di riconosciuta efficacia, ma non è facile da gestire e da applicare all'intera rete. I dispositivi ad alto rischio, come i sistemi obsoleti notoriamente vulnerabili, vanno inseriti in segmenti di rete in grado di limitare le possibili violazioni e contenere i rischi.

# Conclusioni

I responsabili della sicurezza e della gestione dei rischi che operano in ambito sanitario non possono ignorare la necessità di proteggere tutti i dispositivi connessi alla rete estesa. Limitarsi a mettere in sicurezza singoli dispositivi medici, anziché intere categorie di sistemi, rischia di creare lacune significative nel piano di sicurezza. Per adottare un approccio olistico alla sicurezza della rete, è necessario disporre di visibilità e controllo continui sull'intero ecosistema di dispositivi connessi, ma soprattutto comprendere il prezioso ruolo che svolge una piattaforma di visibilità e controllo in grado di coordinare le azioni svolte da strumenti di gestione IT e di sicurezza così eterogenei.

Come già accennato, l'inerzia può avere un costo elevatissimo. Ogni secondo in cui un dispositivo resta non conforme amplia la finestra delle vulnerabilità e incrementa il rischio di mettere a repentaglio la sicurezza dei pazienti nonché di esporre la struttura sanitaria a seri danni commerciali e finanziari. Le strutture sanitarie hanno la possibilità di scegliere: investire ora in una soluzione proattiva di pianificazione e contenimento dei rischi o pagare dopo e affrontare l'ira delle autorità di regolamentazione della sicurezza, dei pazienti e dei legislatori.

# Informazioni su Forescout Technologies

Forescout Technologies è il leader nel settore della visibilità e del controllo dei dispositivi. La nostra piattaforma di sicurezza unificata consente ad aziende e pubbliche amministrazioni di ottenere un quadro dettagliato completo dei loro ambienti aziendali estesi e di coordinare azioni per ridurre il rischio informatico e operativo. I prodotti Forescout vengono distribuiti rapidamente e offrono funzionalità di individuazione e classificazione senza agent in tempo reale di qualsiasi dispositivo con connessione IP, oltre che una valutazione continua dello stato della sicurezza. Al 31 dicembre 2018, ben 3.300 clienti di oltre 80 paesi avevano scelto di affidarsi alla soluzione indipendente dall'infrastruttura di Forescout per ridurre il rischio di interruzioni dell'attività causate da incidenti o violazioni della sicurezza, garantire e dimostrare la conformità di sicurezza e migliorare la produttività delle procedure di sicurezza. Scopri come su forescout.it.

I ricercatori di Forescout hanno limitato la portata dello studio e il campione di dati per coerenza e per facilitare l'elaborazione di un report singolo. Sono stati rilevati dei limiti causati dal tipo di studio e dalla tempistica, dal campo di applicazione, dall'anonimizzazione dei dati, dai metodi di acquisizione passiva dei dati e dagli errori di classificazione di funzioni, sistemi operativi e marche dei dispositivi commessi dall'intelligenza artificiale. Lo scotto da pagare per l'utilizzo di dati reali provenienti da un ambiente di produzione è la sporadica presenza di imperfezioni. Nonostante questi vincoli, i ricercatori di Forescout hanno fatto del loro meglio per creare un report coerente, affidabile e di elevata integrità.

FORESCOUT

orescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 Stati Uniti

**E-mail** info-italia@forescout.com
**Tel. (internazionale)** +1-408-213-3191
**Assistenza** +1-708-237-6591

Maggiori informazioni su forescout.it

© 2019 Forescout Technologies, Inc. Tutti i diritti riservati Forescout Technologies, Inc. è una società del Delaware. Un elenco dei nostri marchi e brevetti è reperibile alla pagina www.forescout.com/company/legal/ intellectual-propertypatents-trademarks. Altri marchi, prodotti o nomi di servizi possono essere marchi o marchi di servizio dei rispettivi titolari.