mead
YOUR DIGITAL INTEGRATOR

Technological Partners

FORTINET

MEDIGATE

ADVANCED HEALTHCARE PROTECTION

La piattaforma di Cyber Sicurezza per la Sanità

MEAD INFORMATICA S.R.L

Pubblicato in Italia, November 2021

MEDIGATE

mead
YOUR DIGITAL INTEGRATOR

Gestione dei rischi: una panoramica

Le lacune nella gestione dei rischi

Panoramica della soluzione

Il settore sanitario è sotto attacco. Health IT Security ha dichiarato che, da novembre, c'è stata un'impennata del 45% nel numero di attacchi ai danni di strutture sanitarie, e che il 79% di tutte le violazioni di dati denunciate nel 2020 ha riguardato il settore sanitario. Questi dati allarmanti rendono ancora più urgente adottare le misure necessarie per ridurre al minimo i rischi che mettono in pericolo le risorse e l'operatività degli ecosistemi sanitari.

Considerata la complessità degli ambienti informatici di tipo medico – che contengono un numero di dispositivi, protocolli e flussi di lavoro in continua espansione e su cui le strutture sanitarie fanno affidamento per erogare servizi in tempo reale di notevole valore – conoscere i rischi e gestirli non è cosa da poco. Ogni ecosistema sanitario è caratterizzato da una combinazione unica di persone, processi e tecnologie che deve essere gestita al meglio per assicurare un'adeguata governance e l'adozione di misure di mitigazione dei rischi in linea con i risultati aziendali desiderati.

Sfortunatamente, la mancanza di visibilità, comunicazione e coordinamento tra responsabili della sicurezza, il team biomedico, il reparto di ingegneria clinica e gli stakeholder delle strutture sanitarie crea delle lacune nei programmi di gestione dei rischi e rende i sistemi informatici del settore medico vulnerabili agli attacchi e alle interruzioni del servizio. Se gli ecosistemi sanitari vogliono mantenere i livelli di rischio dell'ambiente informatico entro parametri accettabili, queste lacune devono essere individuate e colmate.

Medigate colma le lacune

Medigate aiuta le organizzazioni a creare un programma completo di gestione dei rischi associati ai dispositivi medici che consente alle strutture sanitarie di raggiungere e mantenere i livelli di rischio entro parametri accettabili. Quando dispongono di un'unica fonte di informazioni affidabile circa i dispositivi medici, IoMT e IoT presenti nell'ambiente informatico, gli stakeholder delle strutture sanitarie possono collaborare in modo efficace per gestire in sicurezza le proprie attività principali e secondarie.

La piattaforma di sicurezza per i dispositivi Medigate (MDSP) ha ridefinito il concetto di visibilità delle reti mediche. Eseguendo un monitoraggio costante, Medigate raccoglie quelle informazioni granulari sui dispositivi e le attività di cui la struttura sanitaria ha bisogno per definire la strategia di gestione dei rischi più appropriata. Le ampie capacità di integrazione, e le istruzioni di remediation generate automaticamente e rivolte a vulnerabilità e dispositivi specifici, consentono alle strutture sanitarie di migliorare la propria sicurezza e di mantenere livelli di rischio accettabili nell'ambiente informatico.

Valutazione accurata dei rischi associati ai dispositivi

I framework a cui le aziende solitamente fanno riferimento per elaborare i propri programmi di gestione dei rischi, come quello del NIST, sono totalmente sprovvisti del contesto clinico necessario per essere efficaci in un ambiente di tipo medico. L'approccio esclusivo di Medigate, invece, consiste nel combinare competenze in materia di cybersecurity con conoscenze approfondite circa dispositivi medici, IoMT e IoT, protocolli di comunicazione e flussi di lavoro dell'ambito sanitario. Questo ha permesso di elaborare un framework efficace e adeguato per il contesto medico per la valutazione dei rischi associati ai dispositivi connessi. I punteggi di rischio guidano la definizione della priorità delle attività di mitigazione e remediation che consentono alle strutture sanitarie di gestire correttamente i rischi nel proprio ambiente.

Gestione delle vulnerabilità

Medigate valuta i rischi tenendo conto del contesto clinico e analizza i dispositivi connessi all'ambiente della struttura sanitaria per capire le vulnerabilità e le potenziali minacce che questi dispositivi introducono e suggerire il modo migliore per affrontarle. Oltre agli indicatori di compromissione (IoC) di tipo generico e alle vulnerabilità e falle di sicurezza note (CVE), Medigate monitora gli avvisi del produttore per individuare i dispositivi che rischiano di essere compromessi.

Combinando queste informazioni con il contesto clinico di ogni dispositivo, Medigate consiglia misure di mitigazione e remediation in grado di preservare la disponibilità e l'integrità dei dispositivi. Dal momento che questi dispositivi sono impiegati per erogare cure, i rischi vengono gestiti in modo totalmente diverso rispetto a quanto avviene negli ambienti IT tradizionali perché è necessario assicurarsi che la sequenza dei processi resti immutata e l'operatività non subisca interruzioni. Medigate offre la prospettiva clinica necessaria per gestire le vulnerabilità in modo rapido e sicuro.

Igiene informatica in ambito sanitario

Per mantenere l'integrità delle reti mediche e prevenire la diffusione di minacce al loro interno è necessario adottare un buon programma di igiene informatica. Medigate aiuta le strutture sanitarie ad adottare l'approccio rigoroso necessario per mantenere i livelli di rischio entro parametri accettabili. La capacità che offre Medigate di rilevare, valutare e gestire i rischi informatici che i dispositivi medici, clinici e di altro tipo (come i dispositivi IoT non gestiti) introducono nella rete permette alle strutture sanitarie di gestire i rischi dell'intera organizzazione, migliorare le misure di sicurezza e ottimizzare le pratiche di gestione delle risorse.

Protezione sistematica di tutti gli elementi dell'ecosistema sanitario

Medigate aiuta gli ecosistemi sanitari connessi grandi e piccoli a restare operativi e a funzionare al meglio. La capacità di Medigate di aiutare fornitori di servizi sanitari di qualsiasi tipo e dimensione a connettersi in modo sicuro è dimostrata dalle oltre 500 sue implementazioni in tutto il mondo, dai più piccoli ambulatori alle più grandi strutture ospedaliere degli Stati Uniti.

Operatività costante dei programmi di gestione dei rischi

Medigate collabora con partner certificati per aiutare le strutture sanitarie a formulare e applicare un programma per la sicurezza in ambito medico (MCSSP) che consenta di proteggere in modo efficace e costante gli ambienti che ospitano dispositivi medici e IoMT. Medigate potenzia la sicurezza per i dispositivi medici offrendo alle strutture sanitarie il contesto clinico necessario per comprendere e gestire efficacemente i rischi associati al loro ambiente.

MEDIGATE

mead
YOUR DIGITAL INTEGRATOR

Gestione dei rischi e igiene informatica in ambito sanitario

Panoramica

L'utilizzo massiccio di dispositivi connessi, l'aumento delle minacce informatiche in ambito sanitario e la scoperta sistematica di sempre nuove vulnerabilità sono motivi di grande preoccupazione per le strutture sanitarie. I responsabili delle reti e della sicurezza sono consapevoli dei rischi legati all'utilizzo di dispositivi medici e IoT connessi, ma la carenza di risorse rende spesso difficoltoso gestire il volume di avvisi generati dai software di sicurezza. Hanno bisogno di un approccio sistematico per valutare e gestire i rischi delle reti mediche, ma in genere non hanno a disposizione i dati, un framework affidabile e le informazioni dall'immediato valore pratico necessari per mantenere i livelli di rischio entro parametri accettabili.

Dati: i dispositivi connessi spesso non vengono rilevati o sono classificati in modo errato

Le soluzioni di sicurezza tradizionali non sono in grado di individuare le informazioni critiche di cui hanno bisogno gli ecosistemi sanitari per gestire e proteggere in modo efficace i propri dispositivi IoT e medici. I dati indispensabili per scoprire le potenziali vulnerabilità e mappare i rischi includono il produttore del dispositivo, il modello, il sistema operativo, il numero di serie, il tipo di hardware e le versioni delle app. Fatta eccezione per l'indirizzo MAC o IP, alcuni dispositivi non vengono identificati in alcun modo, mentre di altri, pur se classificati come dispositivi medici, non è possibile scoprire le specifiche tecniche, la localizzazione e il contesto operativo, come il team o il reparto incaricato della loro gestione. Con dati così limitati, diventa estremamente difficile valutare il rischio associato a un determinato dispositivo e adottare le misure appropriate.

Framework: non esistono quadri di riferimento per valutare sistematicamente i rischi associati ai dispositivi medici

Una visibilità limitata sui dispositivi, associata al timore che una loro scansione attiva metta a repentaglio l'operatività di apparecchi indispensabili per curare i pazienti, complica enormemente le attività di ricerca delle vulnerabilità e il tentativo di stabilire con precisione il tipo di minaccia che ogni dispositivo connesso rappresenta per la rete. Inoltre, anche avendo a disposizione tutti i dati sui dispositivi, non esiste un quadro di riferimento ampiamente diffuso che consenta di aggregare, valutare e classificare per priorità i fattori specifici che influenzano la probabilità di compromissione e la gravità dell'impatto sull'ambiente informatico. Gli ecosistemi sanitari necessitano di un framework che innanzitutto permetta di determinare la probabilità che un dispositivo della rete medica presenti una falla e che in seguito permetta di calcolare la potenziale gravità delle conseguenze. Questo framework deve prevedere processi logici e continui volti a misurare, valutare e aggregare i rischi in modo che sia possibile intervenire in maniera adeguata.

Informazioni: la mancanza di contesto rende difficoltoso implementare misure di remediation e mitigazione

La mancanza di un framework coerente di valutazione dei rischi e di classificazione per priorità rende estremamente difficile dotare gli ecosistemi sanitari di un piano articolato volto a neutralizzare, mitigare e contenere i rischi che rendono vulnerabili le reti mediche. Poiché non possono permettersi di introdurre controlli di sicurezza che potrebbero interferire o addirittura bloccare l'erogazione dei servizi sanitari, i responsabili della sicurezza spesso hanno timore di agire e restano in balia delle minacce associate ai dispositivi IoT e medici. Ciò che serve è un modo sicuro per ridurre i rischi esistenti senza introdurne di nuovi. Servono informazioni di valore pratico che combinino competenze in materia di cybersecurity e conoscenze mediche: una garanzia per tutti che sia i pazienti sia l'accesso a dati e servizi sono protetti.

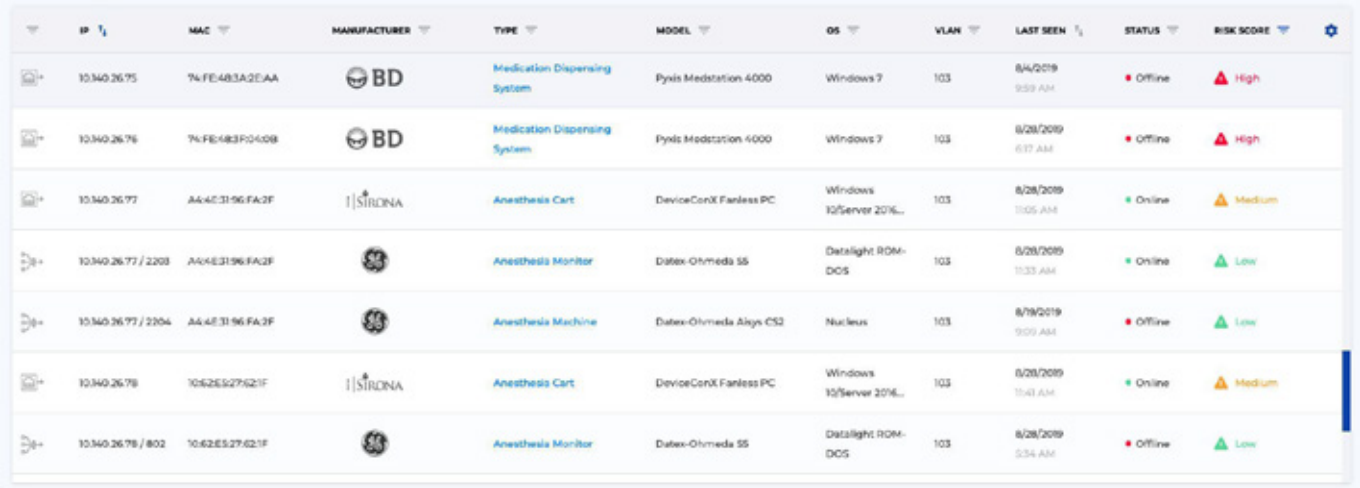
Gestione dei rischi a tutto tondo per una buona igiene informatica

Aggiungendo la piattaforma di sicurezza dei dispositivi Medigate alla rete, gli ecosistemi sanitari possono ottenere i dati, il framework e le informazioni dall'immediato valore pratico necessari per gestire i rischi di qualsiasi rete medica. Il punto di partenza è una visibilità granulare su tutti i dispositivi connessi. I dati sui dispositivi e il contesto in cui operano vengono utilizzati per calcolare il

punteggio di rischio complessivo di ogni dispositivo, da cui il team che gestisce la sicurezza può derivare il rischio relativo e classificare le minacce presenti nell'ambiente informatico in base alla priorità. I punteggi di rischio vengono aggregati e visualizzati in report che ne rivelano la distribuzione sia a livello interno, cioè nei reparti, sia a livello esterno, tra i produttori dei dispositivi, e che consentono di adottare misure appropriate ai vari livelli.

Identificazione di tutti i dispositivi medici della rete

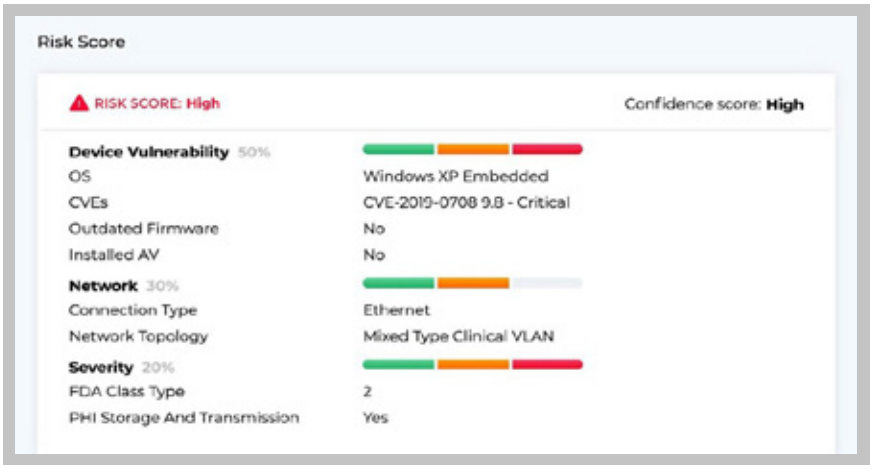
Tramite un'ispezione approfondita dei pacchetti dati (DPI) eseguita sul traffico di rete raccolto passivamente, Medigate riesce a individuare il 100% dei dispositivi connessi alla rete medica e a ottenere dati approfonditi su ognuno, come produttore, modello, sistema operativo, tipo di hardware, versioni delle app e localizzazione. Ricorrendo a speciali tecniche DPI, basate su una profonda conoscenza dei protocolli di comunicazione e dei flussi di lavoro dei dispositivi medici, Medigate semplifica la valutazione del rischio associato a ogni dispositivo.

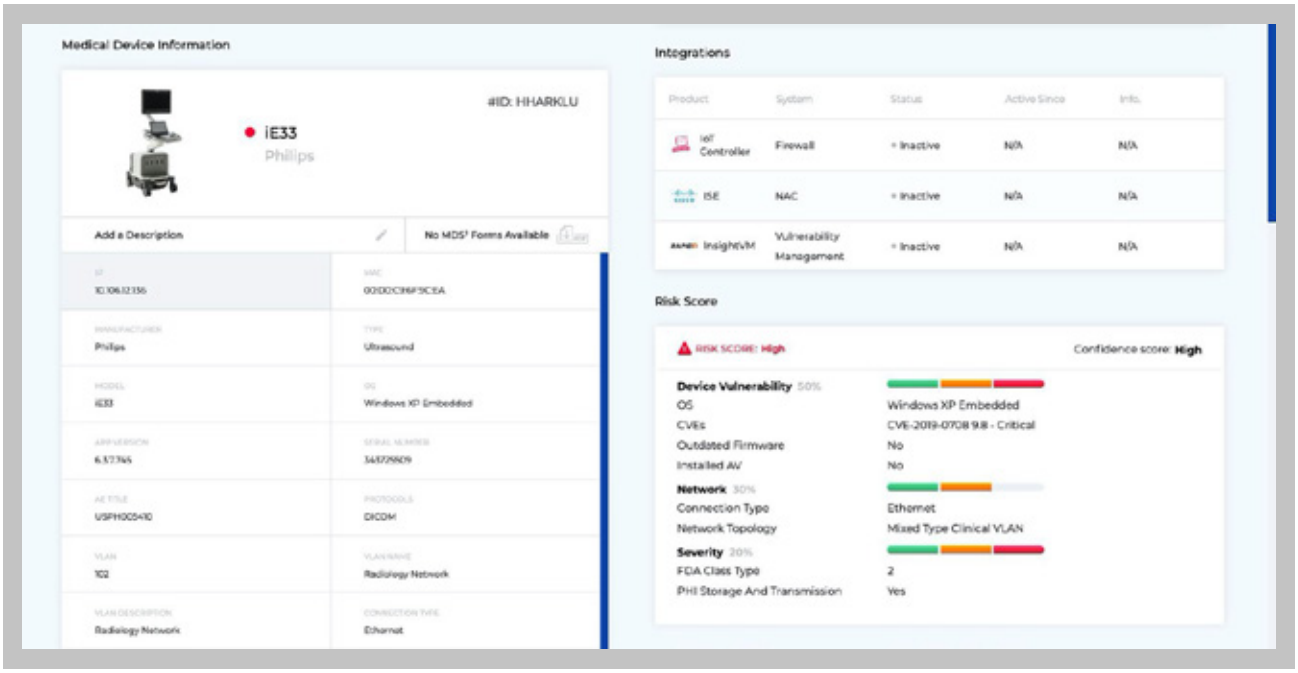


Assegnazione di un punteggio di rischio a ogni dispositivo

Per ogni dispositivo Medigate elabora un punteggio di rischio che tiene conto della probabilità di compromissione e della potenziale gravità dell'impatto di tale compromissione per l'ecosistema sanitario. Il punteggio si basa sul Risk Management Technical Information Report dell'organizzazione statunitense AAMI (Association for the Advancement of Medical Instrumentation), oltre che su framework e standard per la gestione dei rischi elaborati da organizzazioni quali FDA, ECRI, ISO e NIST. Combinando questi standard con straordinarie competenze in materia di cybersecurity e conoscenze approfondite in ambito medico, Medigate ha elaborato un framework semplice ma al contempo completo per valutare le proprietà intrinsecamente rischiose dei dispositivi, la connettività di rete, le vulnerabilità e falle di sicurezza note (CVE) e altri fattori che utilizza per assegnare un livello di

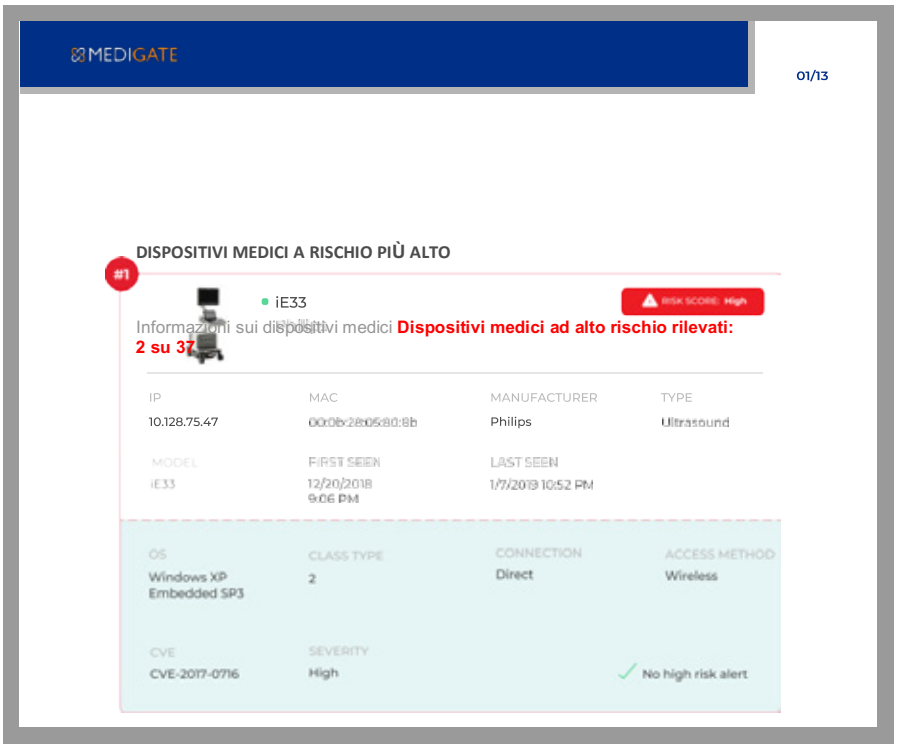
rischio prioritario a ogni dispositivo. Medigate si interfaccia inoltre con piattaforme di gestione delle vulnerabilità da cui importa informazioni precise sulle CVE derivanti dagli specifici attributi tecnici di ogni dispositivo.





Aggregazione dei punteggi di rischio in report dettagliati e operativi

Medigate consente di redigere report personalizzabili che delineano chiaramente la distribuzione del rischio sia a livello interno (per reparto) che esterno (per produttore). La piattaforma per la sicurezza dei dispositivi Medigate si interfaccia inoltre con piattaforme di gestione delle vulnerabilità a cui trasmette dati identificativi dettagliati che le procedure di scansione e reporting utilizzano per avviare interrogazioni non intrusive.



Avvio di attività di remediation o mitigazione per i rischi più seri

I dati e le informazioni raccolti dalla piattaforma Medigate migliorano immediatamente la capacità delle strutture sanitarie di individuare i dispositivi rischiosi e le persone responsabili della loro gestione. A questo punto, i team preposti possono avviare le attività di remediation o mitigazione appropriate per migliorare l'igiene informatica dell'ambiente connesso. Oltre ad aiutare le strutture sanitarie a definire la priorità delle attività di gestione dei rischi, queste informazioni aggiungono un nuovo livello di sicurezza per l'acquisto di nuovi dispositivi connessi.

Gestione dei rischi in tutta l'organizzazione

Grazie a Medigate, i team che gestiscono la sicurezza possono usufruire di una visibilità in tempo reale su tutti i dispositivi connessi della rete medica, con informazioni sulla loro localizzazione e sulla

persona o il reparto responsabile della loro manutenzione. Facendo riferimento ai punteggi di rischio granulari assegnati a ogni dispositivo e aggregati in report personalizzabili, gli ecosistemi sanitari possono individuare i reparti, i produttori e i tipi di dispositivo che presentano il rischio più elevato nell'ambiente e intraprendere le misure appropriate.

Migliore protezione

Le valutazioni dei rischi di Medigate aiutano i team a implementare i processi di remediation e le strutture a gestire i rischi delle reti mediche in collaborazione con i produttori. Per ridurre il profilo di rischio delle strutture, la piattaforma Medigate propone anche misure di mitigazione personalizzate, come la segmentazione della rete in base ai dispositivi e l'imposizione di policy di sicurezza tramite i firewall o le soluzioni di controllo degli accessi (NAC) esistenti, provvedimenti che possono essere implementati automaticamente ricorrendo a integrazioni efficaci con soluzioni di produttori di punta.

Acquisti di dispositivi IoT e medici più mirati

Essere consapevoli di quali dispositivi presentano il rischio più elevato per l'ambiente permette di migliorare i criteri in base ai quali le strutture sanitarie scelgono i nuovi prodotti da connettere alla rete.

Conclusioni

Grazie a Medigate, con un solo strumento i responsabili della sicurezza possono individuare tutti i dispositivi connessi alla rete, assegnare a ciascuno un punteggio di rischio complessivo e generare report di valutazione dei rischi con informazioni immediatamente operative che consentono di mitigare e neutralizzare le minacce.

MEDIGATE

mead
YOUR DIGITAL INTEGRATOR

Sicurezza e disponibilità dei dispositivi in ambito sanitario

Protezione continua dei dispositivi alla "periferia" della rete

Panoramica

Cresce a vista d'occhio il numero di ecosistemi sanitari connessi e "smart" che si ingrandiscono o stringono alleanze con realtà mediche più piccole per proporre servizi altamente specializzati, interventi di primo soccorso e medicina di base. Secondo la rivista di tutela dei consumatori Consumer Reports, ad esempio, tra il 2014 e il 2018, negli Stati Uniti il numero di centri di pronto soccorso è passato da 6.400 a 8.100, e di altri 500/600 era prevista l'apertura a breve. La pandemia di Covid-19 ha accelerato questo trend di trasformazione della modalità di erogazione dell'assistenza sanitaria, dal momento che ha reso necessario curare i pazienti al di fuori dei grandi ospedali.

Strutture mediche piccole e specializzate (centri radiologici, centri prelievi, laboratori e così via), poliambulatori e cliniche offrono ai pazienti un'ampia gamma di servizi facilmente accessibili in qualsiasi momento. Tuttavia, nonostante la portata e la varietà dei servizi offerti siano più contenute, queste strutture devono comunque soddisfare i medesimi requisiti in materia di privacy e sicurezza delle grandi realtà ospedaliere. Questa "periferia" digitalizzata dell'ecosistema sanitario deve essere gestita e protetta nel modo più rigoroso possibile per assicurare conformità e disponibilità nel tempo dei servizi offerti ai pazienti.

Le strutture sanitarie devono tutelare l'operatività e gestire i rischi

Molte strutture sanitarie faticano a garantire la sicurezza dei propri dispositivi, a gestirli, a mantenerli operativi e a prevenire gli attacchi informatici che rischiano di ripercuotersi sull'erogazione delle cure. Secondo il centro di ricerca Cybersecurity Ventures, il numero di cyberattacchi che subirà nel 2021 il settore sanitario, che vale 1,2 migliaia di miliardi di dollari, sarà il doppio o addirittura il triplo rispetto a quello che subiranno altri settori. Il problema è che per garantire la sicurezza di un numero di dispositivi medici, IoMT e IoT che cresce e si diversifica senza sosta, e su cui le strutture sanitarie fanno affidamento per offrire servizi connessi di notevole valore, serve uno speciale mix di competenze in materia di cybersecurity e conoscenze mediche non sempre facilmente reperibile.

I dispositivi medici e IoMT sono generalmente sistemi chiusi che utilizzano sistemi operativi e protocolli proprietari che le soluzioni di sicurezza tradizionali non conoscono e non sanno gestire. Inoltre, all'aumento del volume dei sensori e dei dispositivi IoT connessi all'infrastruttura digitale di una struttura sanitaria corrisponde un aumento del numero di nuovi vettori di attacco che non possono essere gestiti con le normali misure e pratiche di cybersecurity.

Una misura che può essere considerata accettabile per neutralizzare un rischio in una rete informatica standard è spesso improponibile in un ambiente di tipo medico perché le sue ripercussioni sarebbero troppo gravi: bloccare le comunicazioni o impedire la connessione di un dispositivo impiegato in un protocollo di cura, ad esempio, potrebbe avere effetti negativi sulla terapia o il paziente. Alle strutture sanitarie serve un approccio graduale e interfunzionale che consenta di gestire e proteggere le proprie risorse rispettando la complessità dell'ambiente in cui operano. Nello specifico, devono essere in grado di:

- Compilare e mantenere aggiornato un inventario preciso di tutti i dispositivi connessi all'ambiente, con un'indicazione del rischio relativo associato a ognuno.
- Adottare strategie di remediation efficaci e scalabili che tengano conto della criticità, del costo e delle interdipendenze dei dispositivi in questione.
- Migliorare la collaborazione con i team biomedici e i vertici finanziari dei partner ospedalieri per massimizzare la resilienza e il valore delle risorse.

Perché Medigate

MDSP, la piattaforma per la sicurezza dei dispositivi Medigate, è stata creata appositamente per raccogliere i dati e le informazioni operative che servono alle strutture sanitarie per migliorare la gestione e la sicurezza dei dispositivi medici connessi. Medigate trova, identifica ed esegue la profilazione di ogni dispositivo connesso fornendo alle strutture sanitarie la visibilità e le informazioni operative di cui hanno bisogno per prendere decisioni più oculate in fase di acquisto e gestione del ciclo di vita dei dispositivi, nonché per implementare misure di valutazione dei rischi, mitigazione e remediation più efficaci.

Comprendere i rischi

Medigate acquisisce, classifica e cataloga in modalità passiva tutti i dati di un dispositivo: marca, modello, indirizzo IP, ma anche attributi quali firmware, numero di serie, stato della rete, livello di sicurezza, localizzazione e mappatura delle comunicazioni. Combinando questi dati con informazioni sul contesto, Medigate elabora un inventario dinamico di tutti i dispositivi connessi con l'indicazione del punteggio di rischio di ognuno. Un tale livello di dettaglio consente di tenere traccia delle patch applicate e del livello di esposizione alle vulnerabilità, in modo da scegliere le risorse e le attività prioritarie da implementare per mantenere i livelli di rischio entro parametri accettabili.

Migliorare il livello di sicurezza

L'inventario completo, dettagliato e compilato dinamicamente di tutti i dispositivi connessi alla rete della struttura sanitaria può essere integrato con l'infrastruttura di sicurezza esistente – come un firewall, una soluzione di controllo degli accessi (NAC), di gestione delle vulnerabilità (VM) o SIEM – per ottimizzare la visibilità e l'efficacia degli interventi. Grazie alle raccomandazioni accuratamente vagliate per il contesto clinico da Medigate, è possibile affrontare in modo preciso ed efficace le minacce e ridurre i rischi senza incidere sull'erogazione dei servizi avviando scansioni in tutta sicurezza e coordinando l'imposizione automatica di policy. Le strutture sanitarie possono implementare strategie di segmentazione che hanno lo scopo di contenere la propagazione di eventuali attacchi per ridurre al minimo l'impatto delle violazioni e i tempi di ripristino.

Ottimizzare la gestione delle risorse e il loro valore

I dati sulla localizzazione e l'utilizzo dei dispositivi che raccoglie Medigate possono essere usati da vari team (biomedico, di ingegneria clinica, reparti Finance e acquisti) per studiare e migliorare le prestazioni e l'utilità delle risorse. Con i dati forniti da Medigate, ad esempio, le strutture sanitarie possono elaborare strategie e programmi di manutenzione dei dispositivi basati sull'utilizzo piuttosto che sul tempo, così da ottimizzare il ciclo di vita delle risorse. I dati consentono inoltre di prendere decisioni più informate circa quando e dove implementare, disattivare, acquistare o noleggiare le risorse.

Integrazioni con piattaforme healthcare

Medigate è la soluzione che offre le capacità di integrazione più ampie del settore sanitario. Oltre ad acquisire, normalizzare e arricchire i dati raggiungendo straordinari livelli di precisione e fruibilità, la piattaforma Medigate fornisce un maggior numero di esempi pratici di come i dati che mette a disposizione possano essere utilizzati per migliorare i processi decisionali con casi d'uso che riguardano soluzioni VM, CMMS, NAC e SIEM. Oltre a offrire Data Exchange basati su API e interfacce di sistema, Medigate propone speciali integrazioni concepite appositamente per estrarre un reale valore operativo dall'intero ambiente informatico della struttura sanitaria.

Riepilogo

Combinando straordinarie competenze in materia di cybersecurity con conoscenze approfondite dei flussi di lavoro e degli ambienti informatici di tipo medico, Medigate offre la visibilità e le informazioni operative di cui le strutture sanitarie hanno bisogno per gestire e proteggere i propri dispositivi medici, IoMT e IoT nell'ottica di ridurre i rischi dell'ambiente informatico, risparmiare e aumentare i profitti.

Le modalità di erogazione dei servizi sanitari stanno subendo una trasformazione epocale. I vantaggi che derivano dal modello "salute in tempo reale" dipendono dal livello di sicurezza di ogni singola struttura sanitaria che opera nell'ecosistema.

Le strutture sanitarie possono usare Medigate per:

- Creare un'unica fonte di informazioni affidabile che il team biomedico, i responsabili della sicurezza e la proprietà possono utilizzare per monitorare e gestire l'inventario delle risorse in tempo reale.
- Identificare i rischi per dispositivo e sede, sulla base delle vulnerabilità presenti e della probabilità che vengano sfruttate, per scoprire e gestire i livelli di rischio complessivi.
- Implementare attività di remediation e mitigazione adatte al contesto clinico per migliorare la resilienza, consolidare il livello di conformità e incrementare la sicurezza.
- Aumentare il livello di utilizzo complessivo di ogni dispositivo per ottimizzare il valore delle risorse e i profitti della struttura.

FORTINET

WHITE PAPER

Fortinet Security Fabric promuove l'innovazione digitale

Ampia, integrata e automatizzata

Sintesi preliminare

Un numero sempre maggiore di organizzazioni sta adottando iniziative di innovazione digitale (DI, Digital Innovation) per accelerare il business, ridurre i costi, migliorare l'efficienza e garantire una migliore esperienza ai clienti. Le iniziative comuni prevedono lo spostamento di applicazioni e flussi di lavoro nel cloud, l'implementazione di dispositivi Internet-of-Things (IoT) sulla rete aziendale e l'espansione dell'impronta dell'organizzazione in nuove filiali.

Questa infrastruttura in evoluzione implica anche rischi per la sicurezza. Le organizzazioni devono far fronte a superfici di attacco sempre più vaste, minacce avanzate, maggiore complessità dell'infrastruttura e un panorama normativo in espansione. Per ottenere i risultati di innovazione digitale desiderati, gestendo in modo efficace i rischi e riducendo al minimo le complessità, le organizzazioni devono adottare una piattaforma di sicurezza informatica che garantisca visibilità dell'intero ambiente e una soluzione che consenta di gestire facilmente sia la sicurezza che le operazioni di rete.

Fortinet Security Fabric risolve queste problematiche con soluzioni ampie, integrate e automatizzate che consentono di realizzare reti basate sulla sicurezza, accesso alla rete zero-trust, sicurezza dinamica del cloud e operazioni di sicurezza basata su intelligenza artificiale (IA). L'offerta Fortinet è arricchita da un ecosistema di prodotti di terzi perfettamente integrati che riducono al minimo le lacune delle architetture di sicurezza aziendali, sfruttando al massimo il ritorno sull'investimento (ROI).

L'84% dei responsabili della sicurezza ritiene che il rischio di attacchi informatici aumenterà[1]

Il 77% dei professionisti della sicurezza afferma che la propria organizzazione ha spostato applicazioni o infrastrutture nel cloud nonostante i noti problemi di sicurezza.[3]

L'innovazione digitale sta trasformando tutti i settori

In tutti i settori economici del mondo, l'innovazione digitale è vista come un imperativo per la crescita del business e per migliorare l'esperienza dei clienti. I CIO si dichiarano generalmente favorevoli in termini di iniziative di innovazione digitale, con il 61% che afferma di avere già avviato operazioni significative in fatto di cloud, IoT e mobile.[2]

Dal punto di vista dei leader IT e della sicurezza informatica dei fornitore di servizi cloud, l'innovazione digitale si traduce in un'ampia gamma di cambiamenti nei loro ambienti di rete. Gli utenti sono sempre più mobili e accedono alla rete da luoghi ed endpoint che non sempre sono sotto il controllo dell'IT aziendale. Si collegano anche direttamente ai cloud pubblici per utilizzare le principali applicazioni aziendali, come Office 365. A superare in numero gli endpoint controllati dall'uomo sono i dispositivi IoT, che sono ampiamente distribuiti, spesso in postazioni remote e non presidiate. Infine, le impronte aziendali dei fornitore di servizi cloud si stanno diffondendo in numerose filiali, alcune delle quali anche geograficamente distanti: la maggior parte di queste si connette direttamente ai servizi cloud e mobili, aggirando i data center aziendali.

Tutti questi cambiamenti rendono obsoleto il concetto di perimetro di rete difendibile, richiedendo ai fornitori di servizi cloud di adottare una nuova strategia di difesa in profondità basata su più livelli.

Migrazione di applicazioni e carichi di lavoro nel cloud

Quasi tutte le aziende hanno iniziato a spostare alcuni carichi di lavoro e applicazioni nel cloud, o almeno prevedono di farlo. Queste decisioni sono spesso guidate dal desiderio di ridurre i costi e migliorare l'efficienza operativa e la scalabilità sfruttando la flessibilità offerta dal cloud.

I fornitori di servizi cloud offrono un'ampia gamma di possibili modelli di distribuzione. Le aziende possono usufruire di applicazioni e servizi Software-as-a-Service (SaaS) come Salesforce o Box. In alternativa, le applicazioni progettate e distribuite in ambienti on-premise possono essere trasformate in distribuzioni Infrastructure-as-a-Service (IaaS) o Platform-as-a-Service (PaaS) come Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, Oracle Cloud Infrastructure e IBM Cloud.

Diffidando della dipendenza esclusiva dai fornitori di servizi cloud e mirando a distribuire ogni applicazione e carico di lavoro nel cloud per il quale è più adatto, molte organizzazioni hanno adottato un'infrastruttura multi-cloud. L'aspetto negativo di tale libertà di scelta è la necessità di apprendere le idiosincrasie di ogni ambiente cloud. Inoltre, devono utilizzare diversi strumenti per gestire l'ambiente e le sue disposizioni di sicurezza, con il rischio di offuscare la visibilità e richiedere l'uso di più console per la gestione delle policy, il reporting e altro ancora.

Profusione di endpoint in più ambienti

Gli endpoint sono probabilmente i nodi più vulnerabili della rete del fornitore di servizi cloud. I fornitori più grandi hanno migliaia di dipendenti, ognuno dei quali utilizza diversi dispositivi di lavoro e personali per accedere alle risorse di rete. Garantire l'integrità informatica e l'aggiornamento della sicurezza degli endpoint su tutti questi dispositivi è un compito piuttosto arduo. Ancora più scoraggiante è la proliferazione dei dispositivi IoT. Verso la fine del 2019, il numero di dispositivi attivi ha superato i 26,66 miliardi e, nel corso del 2020, gli esperti stimano che questo numero raggiungerà i 31 miliardi.[5]

I dispositivi IoT sono presenti in numerosi contesti aziendali. Propongono esperienze personalizzate ai clienti del commercio al dettaglio e dell'ospitalità, tengono traccia dell'inventario nella produzione e nella logistica e monitorano i dispositivi nelle fabbriche o nelle centrali elettriche.

Spesso robusti ed efficienti dal punto di vista energetico, i dispositivi IoT si concentrano sulle prestazioni, in molti casi a scapito delle caratteristiche di sicurezza e dei protocolli di comunicazione sicuri. E a differenza della maggior parte dei dispositivi collegati in rete, le apparecchiature IoT sono comunemente distribuite in sedi distaccate, all'esterno o in strutture non dotate di personale o con poco personale (come le centrali elettriche). Da questi luoghi insicuri, le apparecchiature trasmettono spesso dati critici e sensibili a data center on-premise e a servizi cloud.

Espansione della presenza commerciale nei mercati e nelle aree geografiche distribuite

Man mano che le aziende espandono la loro presenza globale aprendo nuove strutture, filiali e altre sedi secondarie, si trovano a dover far fronte a crescenti limitazioni della larghezza di banda delle reti WAN. Sebbene le applicazioni SaaS, i video e il Voice over IP (VoIP) aumentino la produttività e consentano nuovi servizi, contribuiscono anche a una crescita esponenziale del volume di traffico WAN.

La tecnologia MPLS (Multiprotocol Label Switching), di per sé estremamente affidabile, è stata la tecnologia di connettività WAN di elezione per molti anni. Tuttavia, con questa è difficile ottimizzare l'uso della larghezza di banda WAN e variare i livelli di qualità del servizio in base alle esigenze delle diverse applicazioni. Di conseguenza, l'espansione delle filiali e il miglioramento del servizio possono portare rapidamente all'esplosione dei costi della WAN.

Di conseguenza, le organizzazioni si stanno orientando verso la tecnologia SD-WAN (Software-Defined WAN), che fa un uso efficiente di MPLS, delle connessioni Internet e persino dei collegamenti di telecomunicazione. Inoltre, questa tecnologia instrada dinamicamente ogni tipo di traffico sul collegamento ottimale.

Quattro considerazioni per la progettazione dell'architettura di sicurezza

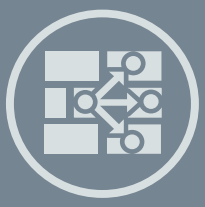
Poiché le organizzazioni stanno adottando con entusiasmo le iniziative di innovazione digitale, le implicazioni per la sicurezza della rete sono spesso trascurate o minimizzate. Infatti, quasi l'80% delle organizzazioni aggiunge nuove innovazioni digitali più velocemente di quanto non possa proteggerle dalle minacce informatiche.[9]

I leader IT devono affrontare quattro principali problematiche nella progettazione di architetture sicure per le loro aziende che innovano digitalmente:

Gli ambienti cloud sono dinamici: il 74% delle aziende ha spostato un'applicazione nel cloud per poi riportarla on-premise.[4]

L'84% delle imprese ha adottato una strategia multi-cloud. L'81% considera la sicurezza una delle principali problematiche del cloud.[6]

Dal 2017 al 2019, si è registrato un aumento del 73% del numero di organizzazioni che hanno subito violazioni dei dati a causa di dispositivi o applicazioni IoT non protetti.[7]



La tecnologia SD-WAN garantisce migliori prestazioni e sicurezza a un costo inferiore rispetto a MPLS.[8]

Espansione della superficie di attacco

I dati sensibili possono potenzialmente risiedere ovunque e possono viaggiare su numerose connessioni al di fuori del controllo dell'azienda. Le applicazioni nel cloud sono esposte a Internet in modo che ogni nuova istanza cloud crei una nuova sfaccettatura della superficie di attacco dell'impresa. I dispositivi IoT estendono la superficie di attacco a postazioni remote e non presidiate da personale. In queste parti oscure della superficie di attacco, le intrusioni possono passare inosservate per settimane, se non addirittura per mesi, seminando il caos nel resto dell'impresa. I dispositivi mobili e gli endpoint di proprietà degli utenti causano imprevedibilità nella superficie di attacco mentre gli utenti si aggirano tra le sedi aziendali, in spazi pubblici e oltre i confini nazionali. Infatti, la massiccia migrazione verso il cloud, l'ampio uso delle piattaforme mobili e l'uso estensivo dei dispositivi IoT sono fattori che amplificano il costo per record di una violazione dei dati di centinaia di migliaia di euro.[10]

Questa superficie di attacco dinamica ed espansa dissolve il perimetro di rete, una volta ben definito, e le protezioni di sicurezza ad esso associate. È molto più facile per gli aggressori infiltrarsi nella rete: una volta all'interno, spesso trovano pochi ostacoli, riuscendo a raggiungere indisturbati i loro obiettivi. Pertanto, la sicurezza nelle imprese che promuovono l'innovazione digitale deve essere a più livelli, con controlli su ogni segmento di rete, partendo dal presupposto che prima o poi il perimetro verrà violato. E l'accesso alle risorse di rete deve essere basato sul minor privilegio possibile e sull'attendibilità continuamente verificata.

Panorama delle minacce avanzate

Il panorama delle minacce informatiche è in rapida crescita, mentre gli utenti malintenzionati cercano di aggirare e sconfiggere le tradizionali difese della sicurezza informatica. Fino al 40% delle nuove minacce malware rilevate in un dato giorno è di tipo zero-day o sconosciuta in precedenza.[15] Che ciò sia dovuto all'aumento dell'uso di malware polimorfico o alla disponibilità di toolkit di malware, la crescita del malware zero-day rende meno efficaci gli algoritmi di rilevamento del malware tradizionali basati su signature. Inoltre, gli utenti malintenzionati continuano a utilizzare l'ingegneria sociale sfruttando i metodi di attendibilità statici utilizzati negli approcci di sicurezza tradizionali. Gli studi rivelano che l'85% delle organizzazioni ha subito attacchi di phishing o di ingegneria sociale nell'ultimo anno.[16]

Man mano che le minacce informatiche diventano sempre più sofisticate, gli incidenti e le violazioni dei dati sono più difficili da rilevare e da risolvere. Tra il 2018 e il 2019, il tempo necessario per identificare e contenere una violazione di dati è passato da 266 a 279 giorni.[17] Oltre alla capacità di individuare e prevenire un tentativo di attacco, le organizzazioni devono anche essere in grado di identificare e risolvere rapidamente un attacco sferrato con successo. Oltre l'88% delle organizzazioni ha dichiarato di aver subito almeno un incidente nell'ultimo anno, a dimostrazione del fatto che tutte le organizzazioni sono a rischio di attacco e che la resilienza informatica è fondamentale.[18]

Maggiore complessità dell'ecosistema

Secondo quasi la metà dei CIO, l'aumento della complessità è la principale problematica di una superficie d'attacco in espansione.[19] Questa maggiore complessità è dovuta al fatto che molte organizzazioni si affidano a una serie di prodotti specifici non integrati per la sicurezza. Infatti, l'impresa media utilizza oltre 75 soluzioni di sicurezza distinte.[20]

Questa mancanza di integrazione della sicurezza significa che tali organizzazioni non sono in grado di trarre vantaggio dall'automazione nella distribuzione della sicurezza. Infatti, il 30% dei CIO indica il numero di processi manuali come una delle principali problematiche di sicurezza nella propria organizzazione.[21] Senza automazione della sicurezza, i CIO hanno bisogno dei professionisti della sicurezza informatica più qualificati per monitorare e proteggere la rete.

Tuttavia, molte organizzazioni non riescono ad assumere personale con solide competenze di sicurezza informatica. Le stime indicano che oltre 4 milioni di posizioni lavorative nell'ambito della sicurezza informatica sono attualmente non occupate e il numero è in

Il 61% dei CISO dichiara di svolgere già attività in termini di cloud, IoT e mobile.[11]

Fino al 40% del nuovo malware rilevato in un determinato giorno è zero-day o precedentemente sconosciuto.[12]

Le iniziative di innovazione digitale implicano che i team di sicurezza dell'impresa debbano distribuire protezioni per 17 diversi tipi di endpoint.[13]

Nell'ultimo anno, un terzo delle imprese ha subito una violazione dei dati business-critical, che potrebbe causare sanzioni normative.[14]

costante crescita.[22] Questa impossibilità di accesso ai talenti necessari sta mettendo a rischio le organizzazioni: il 67% dei CIO, infatti, afferma che la carenza di competenze in materia di sicurezza informatica inibisce la loro capacità di tenere il passo con il ritmo del cambiamento.[23]

Gli aggressori sono ben consapevoli di queste problematiche e le sfruttano a loro vantaggio.

Requisiti normativi sempre più numerosi e rigorosi

Il Regolamento generale sulla protezione dei dati personali (GDPR) dell'Unione Europea (UE) e il California Consumer Privacy Act (CCPA) sono due dei più noti regolamenti in materia di protezione dei dati. Tuttavia, non sono gli unici. In ogni Stato americano è attualmente in vigore una legge sulla notifica delle violazioni dei dati, e molti di essi stanno attuando ulteriori misure di protezione della privacy dei consumatori. Spinti dalla pressione politica e sociale, si prevede un'espansione delle normative nei prossimi anni e le sanzioni per il mancato rispetto delle stesse stanno diventando sempre più esose e diffuse.

Fortinet Security Fabric

- Esteso
- Automatizzato
- Integrati

FORTINET Fabric-Ready

Le organizzazioni sono inoltre tenute a rispettare gli standard di settore, e molte ci riescono con enormi sforzi. Infatti, meno del 37% delle organizzazioni supera l'audit di conformità agli standard PCI DSS (Payment Card Industry Data Security Standard) ad interim.[24] Poiché il PCI DSS è sostituito dal PCI Software Security Framework (PCI SSF), è probabile che queste organizzazioni debbano affrontare ostacoli ancora maggiori per continuare a garantire la conformità.

La necessità di soddisfare e continuare a garantire la conformità alle normative ha un impatto significativo sulla capacità di un'organizzazione di raggiungere gli obiettivi di trasformazione della sicurezza. Ad esempio, del 71% delle organizzazioni che hanno trasferito applicazioni basate sul cloud nei data center on-premise, il 21% lo ha fatto per continuare a garantire la conformità con le normative.[25]

Il Fortinet Security Fabric

Il Fortinet Security Fabric affronta le sfide di sicurezza sopra menzionate proponendo un'ampia visibilità e controllo dell'intera superficie di attacco digitale di un'organizzazione per ridurre al minimo il rischio, una soluzione integrata che riduce la complessità del supporto di più prodotti specifici e un flusso di lavoro automatizzato per aumentare la velocità di funzionamento.

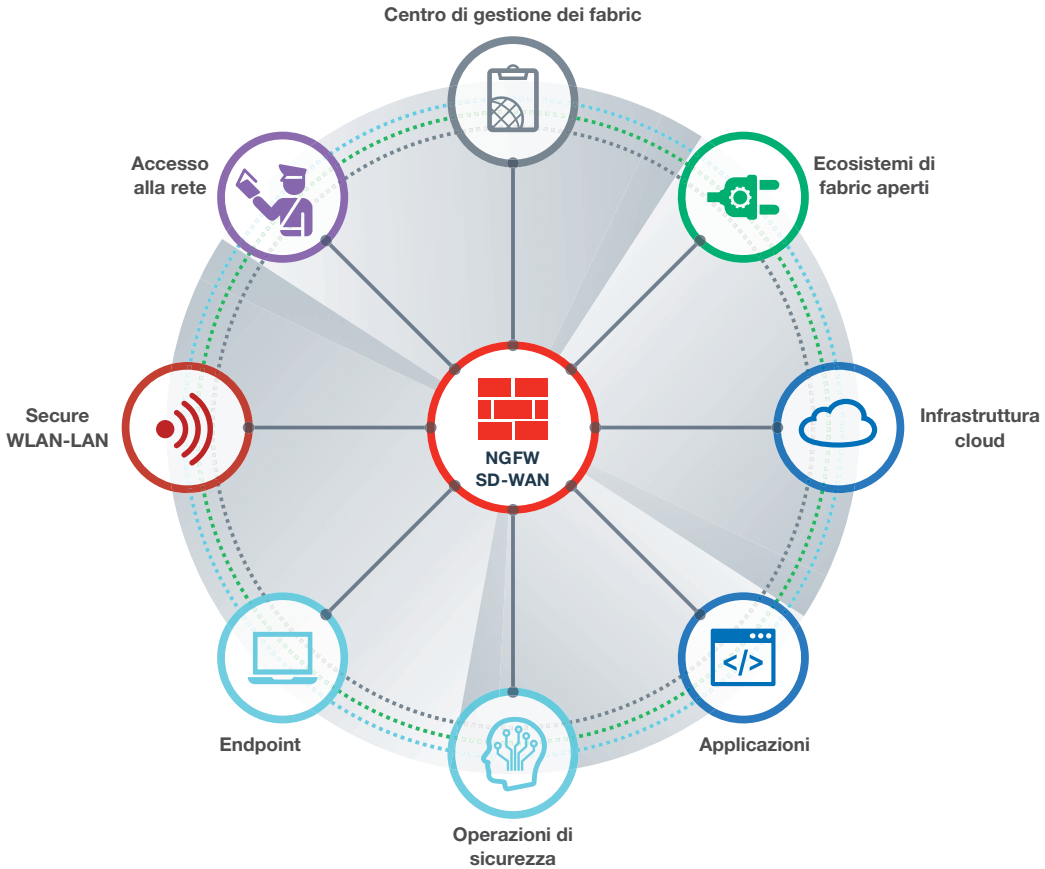


Figura 1: il Fortinet Security Fabric favorisce la perfetta integrazione di più tecnologie di sicurezza in tutti gli ambienti, supportate da un'unica fonte di threat intelligence in un'unica interfaccia. Elimina inoltre le lacune di sicurezza nella rete e accelera le risposte ad attacchi e violazioni.

Ampia visibilità della superficie di attacco

Con l'espansione dei perimetri organizzativi a seguito delle trasformazioni legate all'innovazione digitale, anche la superficie di attacco si espande. Il Fortinet Security Fabric affronta la sfida di una superficie di attacco in espansione garantendo sicurezza e visibilità end-to-end alle organizzazioni nell'intera infrastruttura di rete. Con la più ampia gamma di soluzioni di rete a elevate prestazioni e basate sulla sicurezza per data center, filiali e piccole imprese e tutti i principali fornitori di servizi cloud, il Fortinet Security Fabric offre tutta la flessibilità necessaria per proteggere ogni segmento della rete.

Tutti i componenti sono configurati, gestiti e monitorati da un unico sistema di gestione centralizzata. Oltre a eliminare i compartimenti stagni associati alle infrastrutture di sicurezza dei prodotti specifici, l'interfaccia unica per tutti i componenti di sicurezza riduce l'onere di formazione del personale. Il sistema di gestione facilita anche la distribuzione di componenti remoti zero-touch, riducendo i costi di trasporto e abbattendo ulteriormente i costi operativi.

Architettura di sicurezza integrata

Con tutti i componenti gestiti dallo stesso sistema operativo di rete FortiOS, il Fortinet Security Fabric garantisce una configurazione uniforme, oltre alla gestione delle policy e una comunicazione in tempo reale e senza sforzo nell'ambito dell'infrastruttura di sicurezza. In questo modo, si riducono al minimo i tempi di rilevamento e attenuazione delle minacce, nonché i rischi per la sicurezza derivanti da errori di configurazione e dalla compilazione manuale dei dati, con una risposta tempestiva e accurata agli audit di conformità.

Oltre all'integrazione dei prodotti e delle soluzioni Fortinet, il Security Fabric include connessioni API predefinite per oltre 70 Fabric-Ready Partner che garantiscono una solida integrazione tra tutti gli elementi del Security Fabric.

Per i prodotti di sicurezza che non fanno parte dell'ecosistema Fabric-Ready Partner, le API REST e gli script delle operazioni di sviluppo (DevOps) ne semplificano e velocizzano l'aggiunta nel Security Fabric.

Operazioni, orchestrazione e risposta automatizzate

Oltre alla perfetta integrazione, il Fortinet Security Fabric è leader del settore nell'applicazione di tecnologie di apprendimento automatico che contribuiscono a stare al passo con il panorama delle minacce informatiche in rapida evoluzione. Il Fortinet Security Fabric include funzionalità avanzate di orchestrazione della sicurezza, automazione e risposta (SOAR, Security Orchestration, Automation, and Response), così come il rilevamento proattivo delle minacce, la correlazione delle minacce, gli avvisi di condivisione dell'intelligence e la ricerca e l'analisi delle minacce.

L'accelerazione delle attività di risposta agli incidenti richiede anche di garantire che il personale di sicurezza non sia distratto da altre problematiche, come la raccolta di dati e la generazione di report per la conformità normativa o i dirigenti. In questo caso, il Fortinet Security Fabric offre aggregazione automatizzata dei registri, correlazione dei dati e generazione di report utilizzando modelli integrati.

Quasi la metà dei CISO considera l'integrazione della sicurezza e il miglioramento dell'analisi tra le principali priorità della loro strategia tecnologica di sicurezza informatica. [26]

I firewall NGFW FortiGate garantiscono il più alto rapporto prezzo-prestazioni nelle valutazioni di terzi durante la scansione del traffico crittografato. Raggiungono prestazioni SSL a 5,7 Gbps bloccando il 100% delle evasioni.[27]

La riduzione dei tempi di rilevamento delle violazioni e di risposta può favorire una riduzione del 25% dei costi complessivi di una violazione di dati.[28]

Soluzioni Security Fabric

Il Fortinet Security Fabric offre soluzioni in cinque aree principali: accesso zero-trust, reti basate sulla sicurezza, sicurezza dinamica del cloud, operazioni di sicurezza basate sull'intelligenza artificiale ed ecosistema di partnership. Ognuna di queste include le migliori soluzioni della categoria, che hanno ricevuto più premi e sono state valutate e raccomandate dai principali test di terzi, come NSS Labs, e riconosciute dai principali analisti, tra cui Gartner. [29,30]

Figura 2: struttura concettuale del Fortinet Security Fabric.

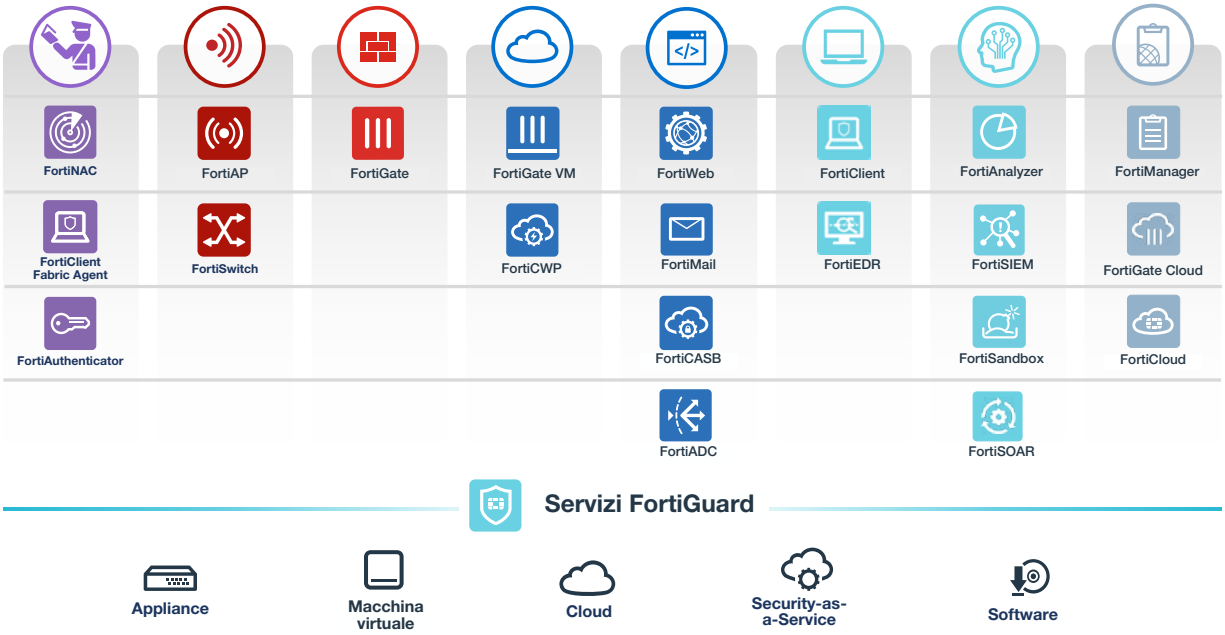


Figura 3: offerte principali in ciascuna delle aree delle soluzioni Security Fabric.

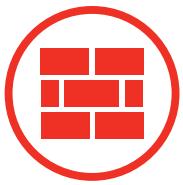
Accesso alla rete zero-trust

Poiché le minacce informatiche diventano sempre più sofisticate, un modello di sicurezza incentrato sul perimetro non è più sufficiente. I furti di credenziali e il malware consentono alle minacce esterne di accedere ad account legittimi all'interno della rete aziendale. Il Fortinet Security Fabric consente alle aziende di implementare una policy di accesso alla rete zero-trust nell'intera WAN aziendale.

Il primo passo per far rispettare l'accesso zero-trust su una rete è il rilevamento dei dispositivi collegati alla rete. Le soluzioni **FortiNAC** per il controllo dell'accesso alla rete (NAC, Network Access Control) forniscono rilevamento automatico dei dispositivi connessi alla WAN aziendale. I dispositivi collegati sono sottoposti a scansione di sicurezza e il team di sicurezza di un'organizzazione può definire policy specifiche da applicare ai dispositivi. Dopo aver approvato un dispositivo per l'accesso alla rete, viene monitorato continuamente per rilevare eventuali anomalie comportamentali che potrebbero indicare un'infezione o l'uso da parte di un utente malintenzionato.

Se in grado di identificare i dispositivi collegati alla rete, le organizzazioni possono implementare l'accesso zero-trust per individuare gli utenti che utilizzano tali dispositivi. Il server di gestione delle identità degli utenti FortiAuthenticator offre autenticazione integrata e controllo degli accesso basato sui ruoli (RBAC, Role-Based Access Control), consentendo alle organizzazioni di implementare il minor numero possibile di privilegi e separazioni dei ruoli sulle reti. I token di autenticazione a due fattori FortiToken rafforzano l'autenticazione degli utenti abilitando l'autenticazione a più fattori, garantendo che le credenziali degli utenti compromesse non concedano a un aggressore l'accesso autenticato all'account di un utente.

Quando i dispositivi sono collegati alla rete aziendale, il monitoraggio dei dispositivi e l'applicazione delle policy possono essere eseguiti sulla rete. Tuttavia, l'uso aziendale dei dispositivi mobili è in continua e rapida crescita, per cui i dispositivi aziendali possono essere utilizzati offline o su altre reti. L'installazione di **FortiClient** Fabric Agent fornisce visibilità negli endpoint e implementa il controllo dinamico degli accessi sia dentro che fuori la rete aziendale.



Rete basata sulla sicurezza

Con l'espansione delle reti aziendali e delle superfici di attacco legata all'innovazione digitale, aumenta la necessità di proteggere queste reti. La rete basata sulla sicurezza comporta una solida integrazione dell'infrastruttura di rete con l'architettura di sicurezza di un'organizzazione, consentendo alla rete di scalare e cambiare senza compromettere la sicurezza. Tale integrazione riduce la complessità riducendo al minimo il numero dei vari prodotti specifici. Inoltre, consente di sfruttare facilmente i miglioramenti delle prestazioni, poiché le appliance di rete e di sicurezza sono ottimizzate per la collaborazione.

I firewall NGFW **FortiGate** sono la prima linea di difesa di un'organizzazione contro le minacce avanzate. Tuttavia, offrono molto più di un semplice firewall. Poiché quasi un terzo delle violazioni dei dati comporta attacchi di phishing[31], che si basano su collegamenti o allegati dannosi per infettare gli endpoint o sottrarre le credenziali degli utenti, i firewall NGFW FortiGate includono un Secure Web Gateway (SWG) che identifica e blocca i tentativi di connessione a URL dannosi o sospetti.

I firewall NGFW FortiGate eseguono anche la decodifica e l'ispezione SSL (Secure Sockets Layer)/TLS (Trasport Layer Security). Si tratta di un requisito critico oggi, con circa il 75% del traffico di rete aziendale protetto con SSL/TLS e circa l'82% del traffico dannoso che utilizza la crittografia.[32,33] In risposta, i firewall **NGFW FortiGate** utilizzano processori di sicurezza (SPU) realizzati appositamente per ridurre al minimo l'impatto sulle prestazioni dell'ispezione del traffico SSL/TLS. L'integrazione dell'ispezione del traffico crittografato a elevate prestazioni nel firewall NGFW di un'organizzazione consente inoltre all'azienda di evitare le spese generali associate all'acquisizione e alla distribuzione di appliance standalone nell'infrastruttura di rete.

Se le minacce non vengono rilevate nel perimetro della rete, è essenziale impedire che si spostino lateralmente in tutta la rete. La segmentazione intent-based consente alle organizzazioni di realizzare questo obiettivo in tutta semplicità, abilitando la segmentazione della rete in base alle esigenze aziendali. Le connessioni interne sospette o dannose sono bloccate per impostazione predefinita e, se dopo l'infezione viene identificata una minaccia zero-day, la threat intelligence viene comunicata tramite il Security Fabric per garantire che non si verifichino infezioni secondarie.

Perché questo funzioni, un'organizzazione richiede l'integrazione della sicurezza in tutta la rete aziendale, comprese le filiali. **Fortinet Secure SD-WAN** fornisce prestazioni di rete ottimizzate e integrazione di sicurezza per le filiali. I firewall NGFW FortiGate integrati nelle appliance SD-WAN eseguono l'ispezione del traffico in ogni filiale, migliorando le prestazioni della rete, garantendo connettività diretta a Internet per le applicazioni e i servizi SaaS e consentendo di ridurre i costi della WAN.

All'interno di una filiale, **Fortinet Secure SD-Branch** consente di estendere la visibilità di un'organizzazione e la gestione centralizzata della sicurezza fino al livello di switching. Fortinet Secure SD-Branch è composto da soluzioni FortiNAC, switch di accesso protetti da FortiSwitch e access point wireless **FortiAP** monitorati e controllati da un firewall NGFW FortiGate. Integrando la sicurezza in tutte le WAN aziendali, le aziende semplificano le operazioni eliminando la ridondanza e garantendo una risposta rapida e coordinata alle minacce avanzate.

Sicurezza dinamica del cloud

Nel momento in cui le organizzazioni passano al cloud, è essenziale espandere l'implementazione della sicurezza dell'organizzazione alle risorse basate su cloud. Il Fortinet Security Fabric integra una gamma di soluzioni native per il cloud per garantire sicurezza per qualsiasi applicazione e ambiente di distribuzione.

Le soluzioni di sicurezza Fortinet offrono sicurezza di rete, visibilità e controllo sia nelle distribuzioni di cloud privato che pubblico. I firewall NGFW FortiGate sono disponibili in un fattore di forma VM, che fornisce automazione della sicurezza nativa per il cloud, connettività VPN, segmentazione della rete, Intrusion Prevention e un SWG.

Oltre a fornire protezione dai contenuti dannosi, le organizzazioni devono anche garantire che le loro distribuzioni cloud siano configurate correttamente. Gli errori di configurazione della sicurezza sono un problema importante nel cloud pubblico, con il 99% dei problemi che non vengono segnalati.[34] L'analisi della sicurezza del cloud **FortiCWP** garantisce visibilità e controllo nell'infrastruttura di cloud pubblico, compreso il monitoraggio delle configurazioni, la sicurezza dei dati e la conformità, nonché la gestione integrata delle minacce.

Una volta messa in sicurezza l'infrastruttura cloud stessa, è necessario proteggere le applicazioni eseguite in questa. Un uso comune delle distribuzioni di cloud pubblico è l'hosting di applicazioni web e API web. **FortiWeb** fornisce a queste ultime una sicurezza nativa per il cloud. I firewall WAF FortiWeb proteggono le applicazioni web da minacce sia note che sconosciute utilizzando una combinazione di rilevamento delle signature, apprendimento automatico e intelligenza artificiale. Inoltre, poiché la maggior parte delle applicazioni web utilizza le API per collegarsi ai servizi web e integrarsi con altri strumenti, è fondamentale proteggere tali API web utilizzando la convalida dello schema e la sicurezza OpenAPI per garantire protezione da attività bot potenzialmente dannose come scraping e analisi.

Le organizzazioni si stanno inoltre orientando sempre più verso soluzioni e-mail basate sul cloud, ad esempio Google G Suite e Microsoft Office 365. Poiché gli attacchi di phishing sono una delle principali cause di incidenti di sicurezza e di violazioni dei dati, la sicurezza delle e-mail basata sul cloud è essenziale. Disponibili come appliance fisiche e virtuali o come servizio in hosting, le soluzioni di sicurezza per la messaggistica **FortiMail** proteggono sia le distribuzioni e-mail on-premise che quelle basate su cloud, bloccando anche le minacce e-mail tradizionali e avanzate e fornendo funzionalità di backup per evitare la perdita di informazioni sensibili.

Oltre alle applicazioni web e alle e-mail, molte organizzazioni si affidano ad applicazioni SaaS come Google G Suite, Box, Microsoft Office 365, Dropbox e Salesforce. I CASB (Cloud Access Security Broker) di **FortiCASB** gestiscono i rischi di errata configurazione della sicurezza, forniscono visibilità centralizzata e controllo amministrativo, garantiscono la sicurezza dei dati nelle applicazioni SaaS e assicurano che le configurazioni delle applicazioni SaaS continuino a rispettare la conformità alle normative.

Operazioni di sicurezza basate sull'intelligenza artificiale

L'aumento dei volumi e della sofisticazione degli attacchi dannosi rendono insufficienti le tradizionali soluzioni di sicurezza informatica. Le soluzioni di rilevamento del malware basate su signature sono in grado di rilevare solo la metà degli attacchi malware.[35] L'uso delle funzionalità di intelligenza artificiale e apprendimento automatico è essenziale per rilevare e prevenire questi attacchi.

FortiGuard AI consente alle organizzazioni di tenere il passo con i criminali informatici. FortiGuard Labs raccoglie dati sulle minacce da milioni di sensori in tutto il mondo e collabora con oltre 200 organizzazioni globali. Utilizzando oltre 5 miliardi di nodi, FortiGuard AI identifica le caratteristiche univoche sia delle minacce note che sconosciute. I volumi gestiti dai FortiGuard Labs sono immensi: il team elabora oltre 100 miliardi di query web ogni giorno e blocca oltre 3.600 richieste di URL dannosi al secondo.

Con l'aumentare della sofisticazione delle minacce, la massima prevenzione non è più possibile. Le funzionalità di rilevamento delle minacce avanzate sono essenziali per aiutare le organizzazioni ad evitare violazioni. Le funzionalità di intelligenza artificiale e apprendimento automatico integrate in **FortiDeceptor, FortiSandbox e FortiInsight** consentono alle organizzazioni di identificare avversari e malware sconosciuti e a rilevare e rispondere alle minacce interne.

Con l'accelerazione delle minacce informatiche, le organizzazioni devono sfruttare l'automazione strategica per contenere e risolvere più rapidamente le minacce. Utilizzando **FortiSIEM** e **FortiAnalyzer,** un'organizzazione può ottenere una visibilità globale della propria infrastruttura di rete e accedere ad analisi di sicurezza basate sull'intelligenza artificiale. Sulla base dei dati raccolti, gli analisti della sicurezza possono determinare la natura e la gravità delle minacce, con il supporto dell'analista virtuale **FortiAI**. Ma il rilevamento e la prevenzione delle minacce non sono sufficienti; **FortiSOAR** utilizza l'orchestrazione e l'automazione per risolvere le intrusioni delle minacce che aiutano i team del Security Operations Center (SOC) a scalare e a concentrarsi sulla ricerca delle minacce e su altre attività mission-critical.

Anche gli endpoint richiedono risorse basate sull'intelligenza artificiale durante tutto il loro processo di risposta agli incidenti. La tecnologia EDR (Endpoint Detection and Response) di **FortiEDR** e FortiClient offrono una protezione avanzata degli endpoint che include la scansione delle vulnerabilità, l'applicazione di patch e patch virtuali, nonché la prevenzione degli exploit sia in ambienti online che isolati. Inoltre, se un endpoint viene infettato, il rilevamento delle minacce e la protezione post-infezione di FortiEDR impediscono al malware di comunicare con i server di Command&Control o di spostarsi lateralmente nella rete. Infine, FortiEDR offre una risposta alle minacce basata sul rischio e il ripristino online con il supporto di ricette di risoluzione automatica.

Centro di gestione dei fabric

Il Fortinet Security Fabric è stato progettato per semplificare la gestione dell'intera architettura di sicurezza di un'organizzazione. Il Fabric realizza questo obiettivo integrando tutti i prodotti dei punti di sicurezza distribuiti, consentendo di monitorarli e gestirli a livello centrale.

La piattaforma di gestione centralizzata **FortiManager** e la registrazione e il reporting centralizzati di **FortiAnalyzer** si combinano per fornire visibilità e gestione dell'intera infrastruttura di rete di un'organizzazione. Sono incluse la gestione, l'analisi e l'automazione dei flussi di lavoro da un'unica interfaccia.

Tali funzionalità sono supportate da una serie di integrazioni basate su API con i Fortinet Fabric-Ready Partner. Dodici Fabric Connector garantiscono una solida integrazione con soluzioni di terzi e l'integrazione basata su API è disponibile per oltre 135 Fabric-Ready Partner. Per le soluzioni non partner, il Fortinet Security Fabric include un'API REST e script DevOps che favoriscono una facile integrazione.

Poiché molte organizzazioni stanno spostando le operazioni nel cloud, è necessaria una soluzione single-point-of-access e single-sign-on (SSO) per ridurre la complessità delle implementazioni multi-cloud. **FortiCloud** fornisce SSO e portali a 15 soluzioni Fortinet SaaS e Metal-as-a-Service (MaaS), oltre a un portale **FortiCare** Services. Con il supporto per tutti i principali fornitori di cloud pubblici, il Fortinet Security Fabric semplifica qualsiasi distribuzione multi-cloud.

Combinando FortiManager, FortiAnalyzer e FortiCloud, le organizzazioni possono integrare completamente le loro distribuzioni on-premise e cloud. Questa integrazione consente l'uso dell'automazione e dell'orchestrazione per semplificare la gestione della sicurezza. Inoltre, sfruttando i Fabric Connector e le API, i team di sicurezza possono ricevere informazioni sull'integrità della rete in tempo reale, automatizzare la gestione dei registri di rete e semplificare il reporting sulla conformità, il tutto da un'unica interfaccia.

Gestire i rischi, perseguire le opportunità

L'innovazione digitale consente alle organizzazioni di raggiungere nuovi livelli di efficienza e di risparmio sui costi, nonché migliorare le esperienze dei propri clienti. Tuttavia, le iniziative di innovazione digitale ampliano e modificano anche la superficie di attacco dell'organizzazione, consentendo alle minacce informatiche di sfruttare nuovi vettori di attacco.

Per le organizzazioni che adottano iniziative di innovazione digitale, il riconoscimento, l'accettazione e la corretta gestione dei rischi sono di fondamentale importanza. Il Fortinet Security Fabric rappresenta la base di tutto questo. Unifica le soluzioni di sicurezza in un'unica interfaccia, rende visibile la crescente superficie di attacco digitale, integra la prevenzione delle violazioni basata sull'intelligenza artificiale e automatizza le operazioni, l'orchestrazione e la risposta. In sintesi, consente alle organizzazioni di sfruttare nuovi vantaggi in termini di innovazione digitale senza compromettere la sicurezza dell'agilità, delle prestazioni e della semplicità del business.

[1] Nick Lansing, "Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources", Forbes e Fortinet, 2019.

[2] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maggio 2019.

[3] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments", IHS Markit, 2019.

[4] Ibid.

[5] Gilad David Maayan, "The IoT Rundown For 2020: Stats, Risks, and Solutions", Security Today, 13 gennaio 2020.

[6] "2019 State of the Cloud Report", Flexera, 2019.

[7] Larry Ponemon, "Third-party IoT risk: companies don't know what they don't know", ponemonsullivanreport.com, visitato il 4 febbraio 2020.

[8] Nirav Shah, "SD-WAN vs. MPLS: Why SD-WAN is a Better Choice in 2019", Fortinet, 9 settembre 2019.

[9] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study", Accenture Security e Ponemon Institute, 2019.

[10] "2019 Cost of a Data Breach Report", IBM Security e Ponemon Institute, 2019.

[11] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maggio 2019.

[12] In base a dati interni di FortiGuard Labs.

[13] "6 Obstacles to Effective Endpoint Security: Disaggregation Thwarts Visibility and Management for IT Infrastructure Leaders" Fortinet, 8 settembre 2019.

[14] In base ai dati della ricerca interna di Fortinet.

[15] In base a dati interni di FortiGuard Labs.

[16] Kelly Bissell, et al.,"The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study", Accenture Security e Ponemon Institute, 2019.

[17] "2019 Cost of a Data Breach Report", IBM Security e Ponemon Institute, 2019.

[18] In base a una ricerca interna di Fortinet.

[19] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maggio 2019.

[20] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating", CSO, 14 marzo 2016.

[21] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maggio 2019.

[22] ""Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019", (ISC)², 2019.

[23] "CIO Survey 2019: A Changing Perspective", Harvey Nash e KPMG, 2019.

[24] "2019 Payment Security Report", Verizon, 2019.

[25] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments", IHS Markit, 2019.

[26] "Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources", Forbes e Fortinet, 2019.

[27] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests", Fortinet, 14 ottobre 2019.

[28] "2019 Cost of a Data Breach Report", IBM Security e Ponemon Institute, 2019.

[29] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests", Fortinet, 14 ottobre 2019.

[30] "Gartner Magic Quadrant Reports", Fortinet, visitato il 22 gennaio 2020.

[31] "2019 Data Breach Investigations Report", Verizon, 2019.

[32] Alex Samonte, "TLS 1.3: What This Means For You", Fortinet, 15 marzo 2019.

[33] Robert Lemos, "Attackers Are Messing with Encryption Traffic to Evade Detection", Dark Reading, 15 maggio 2019.

[34] Charlie Osborne, "99 percent of all misconfigurations in the public cloud go unreported", ZDNet, 24 settembre 2019.

[35] Robert Lemos, "Only Half of Malware Caught by Signature AV", Dark Reading, 11 dicembre 2019.

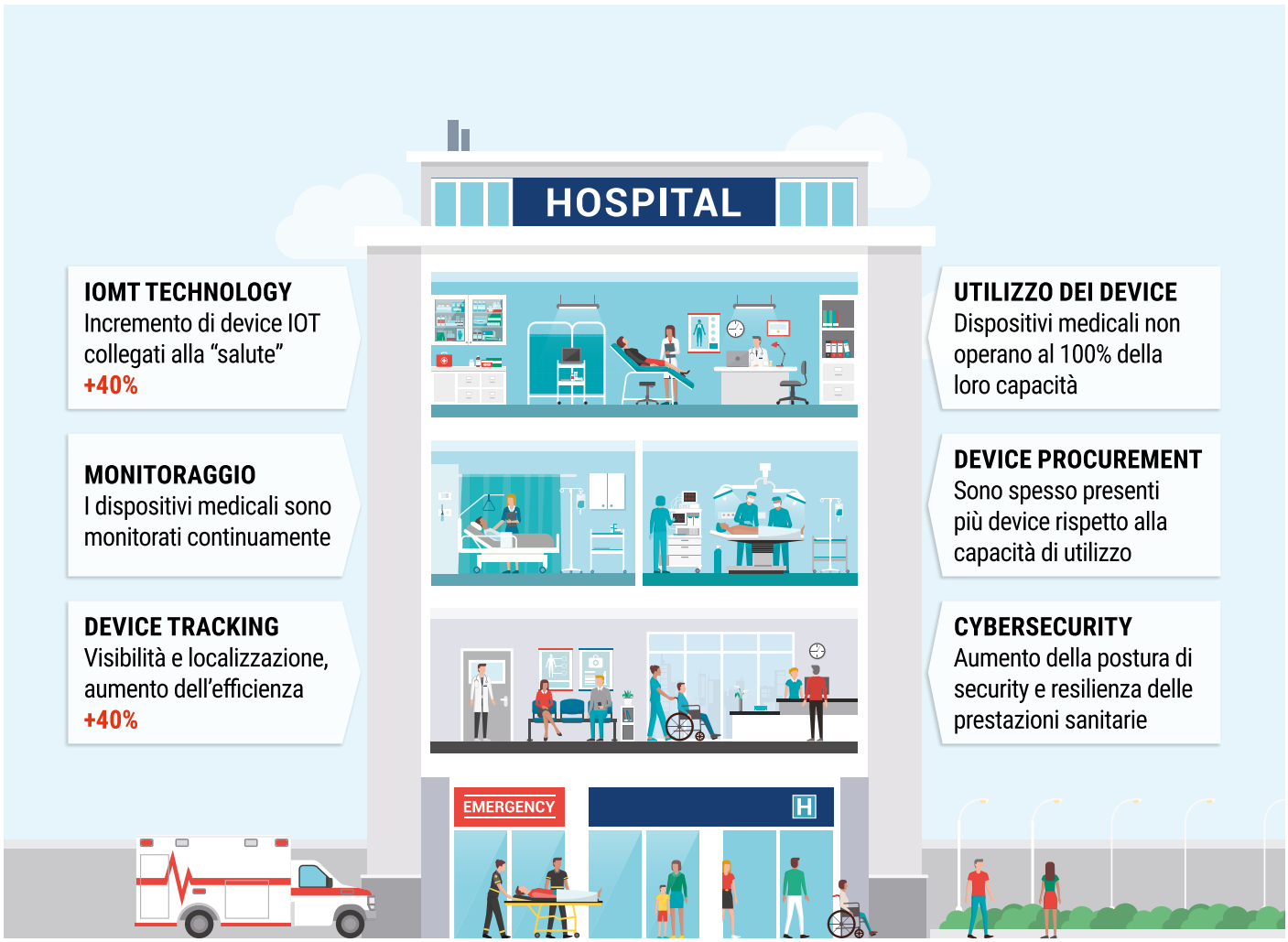
FORTINET

www.fortinet.com

giugno 30, 2020 9:41 AM

570099-0-0-IT

C:\Users\marcel.kotkowski\Downloads\Fortinet\P-358235\09_wf\Work\A-358235-1090227_Fortinet IT\wp-FA-fortinet-security-fabric-enables-digital-innovation-2132020-129AM_IT\wp-FA-fortinet-security-fabric-enables-digital-innovation-2132020-129AM_IT



Utilizzare la piattaforma corretta può trasformare le informazioni contenute nei device in valore aggiunto per ogni reparto

CLINICAL ASSET PLANNING

Prevedere correttamente gli acquisti in modo da utilizzare al meglio il budget

LIFECYCLE MANAGEMENT

Pianificare le manutenzioni in base al reale utilizzo

UTILIZZO DISPOSITIVI

Aumentare la disponibilità dei device e soddisfare le richieste degli utenti

JOB SATISFACTION

Migliorare la qualità del lavoro dedicandolo ad attività importanti

mead
YOUR DIGITAL INTEGRATOR

mead
YOUR DIGITAL INTEGRATOR

MEAD INFORMATICA S.R.L

Via G. Ferraris, 2 - 42122 Reggio Emilia

Tel. +39 0522 265800

Fax +39 0522 393306

info@meadinformatica.it

www.meadinformatica.it

REGGIO EMILIA

ROMA

AGRATE BRIANZA (MB)

MARCON (VE)