VARS

Whitepaper

PROTECTION CONTRE LES INTRUSIONS POUR LE SECTEUR DES SOINS DE SANTÉ

Propulsée par Cynet

Défis d'entreprise

Le secteur des soins de santé a connu une période de transformation numérique rapide. L'environnement informatique que l'on retrouve dans le secteur des soins de santé regroupe un mélange d'applications modernes et plus anciennes, et contient souvent des données intellectuelles, médicales et financières hautement confidentielles. Les données et les systèmes sont de plus accessibles par plusieurs membres de personnel, interne et externe, à l'intérieur et à l'extérieur du périmètre du réseau. Protéger l'environnement informatique et les données dans le secteur des soins de santé, tout en permettant la libre circulation d'informations critiques et urgentes, représente donc un défi de taille.

Malheureusement, les fournisseurs de soins de santé sont des cibles de choix pour les cybercriminels en raison de la valeur des données conservées ainsi que de la surface d'attaque. En octobre 2020, le FBI a lancé un avertissement quant à l'imminence d'attaques par rançongiciels visant le secteur des soins de santé dans le but de voler des données et de perturber les services. En effet, les dossiers de santé ont jusqu'à 50 fois plus de valeur que les données de cartes de crédit sur le marché noir et les attaques étatiques pour l'obtention des données de recherche médicale montent en flèche.

La plupart des petites entreprises de soins de santé ayant des budgets de sécurité limités et des équipes de sécurité réduites sont confrontées à ces risques. La vitesse à laquelle certaines attaques se produisent, comme les attaques par rançongiciels, exige des équipes de sécurité de surveiller activement leurs environnements à toute heure du jour et de la nuit. Bien entendu, cette surveillance accrue peut être impossible pour une petite équipe de sécurité. De plus, une expertise importante dans la détection de menaces persistantes et avancées est nécessaire pour réduire le délai d'intervention, ce qui représente un autre défi pour les petites équipes de sécurité.

Principaux défis en matière de sécurité

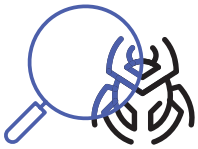
Le vaste accès aux applications et aux systèmes, anciens et modernes, par des fournisseurs internes externes de tierces parties est difficile à protéger

Des équipes de sécurité réduites qui disposent d'une expertise et de budgets limités en matière de technologies de cybersécurité

Le recours aux logiciels antivirus et de protection contre les logiciels malveillants traditionnels offre une protection limitée contre les menaces plus récentes, telles que les rançongiciels et les attaques par crypto verrouillage

Principaux défis en matière de cybersécurité

L'ampleur des systèmes, des applications et des données qui sont facilement accessibles par le personnel interne, les fournisseurs de tierces parties et les clients rend l'environnement d'une entreprise de soins de santé très difficile à protéger. La plupart des fournisseurs de soins de santé doivent en outre se conformer à des mandats réglementaires stricts, de sorte que trouver un équilibre entre la facilité d'accès et la mise en place de contrôles robustes ne fait qu'alourdir leur fardeau.



Visibilité limitée sur l'ensemble de l'environnement

Avec un grand nombre de points d'accès et de systèmes partagés, de nombreuses entreprises ne disposent pas d'une vision complète de l'environnement à protéger. Le vieux dicton selon lequel « vous ne pouvez pas protéger ce que vous ne pouvez pas voir » prend tout son sens. La visibilité est une stratégie de cybersécurité pour protéger les données et les actifs informatiques. Toutefois, il peut être difficile de garder à jour un inventaire complet des actifs, particulièrement des points d'accès qui sont généralement la cible principale des cyberattaques, et ce, dans un environnement de soins de santé hétérogène, lequel est souvent partagé et en constante évolution. En définitive, les entreprises du secteur des soins de santé ont besoin d'une visibilité totale de leur environnement qui inclut les fichiers, les hôtes, les utilisateurs et les réseaux.

De nombreuses entreprises du secteur des soins de santé ont recours à des logiciels d'antivirus et de protection contre les logiciels malveillants qui ne peuvent détecter qu'une fraction des attaques avancées. Ces logiciels offrent une protection limitée contre les nouvelles techniques d'attaque et sont particulièrement vulnérables aux attaques ciblées très avancées. La plupart des logiciels d'antivirus sont inefficaces contre les menaces persistantes et les rançongiciels avancés auxquels le secteur des soins de santé est confronté.

Pour étendre la protection au-delà des solutions d'antivirus, les entreprises ont recours à des outils supplémentaires tels que les outils de détection et d'intervention sur les points d'accès (EDR) et sur les réseaux (NDR). Les solutions EDR sont nées de la constatation que les menaces sont détectées une fois après avoir réussi à contourner un point d'accès, puisqu'un logiciel antivirus n'arrive pas à les anticiper. Les solutions EDR surveillent donc en permanence les points d'accès afin de détecter les activités malveillantes et les comportements du système qui indiqueraient une intrusion.

Les solutions NDR étendent la protection au réseau afin de fournir une visibilité supplémentaire sur l'ensemble de l'environnement. Si une attaque contourne d'une manière ou d'une autre un logiciel antivirus et une solution EDR, la possibilité de détecter les mouvements latéraux et d'autres indicateurs de trafic réseau pourrait permettre de découvrir un acteur menaçant qui a réussi à s'infiltrer dans l'environnement.

Dispositifs de contrôle de sécurité cloisonnés

Bien que chacun des contrôles de sécurité décrits précédemment améliore la visibilité nécessaire dans l'ensemble de l'environnement, ils ne sont pas sans inconvénient. Tout d'abord, les solutions EDR et NDR sont reconnues pour générer des fausses alertes. Les analystes de sécurité traquent celles-ci ou ont tendance à ignorer toutes les alertes, sauf celles qui semblent présenter les plus grands risques. Dans le premier cas, les analystes perdent un temps considérable. Dans le second cas, ignorer des alertes est contraire aux bonnes pratiques de sécurité et expose l'entreprise à des risques d'intrusion.

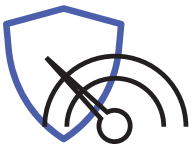
Principaux défis en matière de cybersécurité

(suite)

Dispositifs de contrôle de sécurité cloisonnés

(suite)

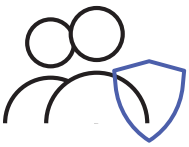
Les dispositifs de contrôle cloisonnés signifient également que l'équipe de sécurité doit surveiller et accéder à un plus grand nombre de « tableaux de bord » lorsqu'elle examine des menaces potentielles. Comme chaque outil de sécurité dispose d'une console de gestion distincte et présente les informations différemment, il est difficile pour les analystes de sécurité de donner un sens à toutes les informations présentées, puis de lier les activités entre les différents contrôles de sécurité pour avoir une vue d'ensemble. C'est pourquoi les attaques furtives sont capables de contourner les environnements dotés de plusieurs niveaux de contrôle.



Des équipes de sécurité réduites avec des ressources limitées

Si l'on met de côté les dispositifs de contrôle cloisonnés, lesquels impliquent plusieurs manipulations, la plupart des outils de sécurité nécessitent un investissement humain significatif pour fonctionner. Lorsque des menaces sont découvertes, les analystes en sécurité doivent investiguer pour en déterminer la cause, puis découvrir l'étendue complète de l'attaque dans l'ensemble de l'environnement.

Une fois la cause et l'étendue de la menace déterminées, il faut remédier à toutes les composantes de celle-ci. Cela implique souvent d'accéder à plusieurs systèmes, ce qui peut s'avérer un processus long et fastidieux.



Des équipes de sécurité réduites avec une expertise limitée en matière de cybersécurité

Avec l'évolution rapide du spectre des menaces, même les équipes de sécurité les plus importantes et les mieux financées sont vulnérables envers celles-ci. Il suffit d'étudier les intrusions commises dans les grandes entreprises pour se rendre compte que même les meilleurs experts en cybersécurité, dotés d'outils de pointe, ont du mal à protéger leurs organisations. Pour les équipes de sécurité réduites qui disposent de budgets technologiques et d'une expertise en cybersécurité limités, le risque d'intrusion augmente de façon exponentielle.

L'approche Cynet-VARS

Cynet a été conçu pour les équipes de cybersécurité réduites dont les ressources, l'expertise en cybersécurité et les budgets technologiques sont limités. Cynet XDR fournit une plateforme unique et unifiée pour prévenir et détecter automatiquement les vecteurs d'attaque auxquels sont confrontées les entreprises de soins de santé, investiguer sur ceux-ci et y remédier. La visibilité sur les points d'accès, les réseaux et les activités des utilisateurs, ainsi que la puissance de la simulation de ressources, offrent la protection la plus élargie et la plus approfondie contre toutes les menaces.

Cynet XDR est la seule solution qui déclenche une investigation automatisée à la suite de chaque alerte quant aux points d'accès, aux utilisateurs ou aux réseaux, en dévoilant entièrement la cause et la portée de l'alerte et en appliquant toutes les mesures correctives nécessaires pour éliminer complètement la menace. Cynet offre également un large éventail d'actions correctives automatisées et pouvant être personnalisées pour traiter les incidents en fonction de vos préférences. De plus, Cynet offre les services d'une équipe d'experts en cybersécurité pour renforcer et guider votre équipe 24 heures sur 24, 7 jours sur 7. Cette offre est incluse dans la plateforme Cynet 360.

Les avantages de Cynet pour le secteur des soins de santé

Facile à déployer et à exploiter

L'agent Cynet peut être déployé sur plus de 5 000 points d'accès en moins d'une heure. Alors que de nombreuses solutions nécessitent des mois pour être déployées et devenir pleinement fonctionnelles, Cynet est prêt dans les 24 heures suivant le déploiement et fournit toutes les informations et protections disponibles dans la plateforme. La console Cynet a été conçue pour être intuitive et sans effort, de sorte que les petites équipes de sécurité n'ont pas besoin de plusieurs années d'expertise pour l'utiliser.

Visibilité totale dès la première utilisation

Cynet XDR offre une visibilité complète et de multiples points de télémétrie, ce qui permet de réduire les faux positifs et de détecter rapidement les menaces furtives. Une plateforme unique et unifiée de détection et d'intervention étendues (XDR) fournit un antivirus de nouvelle génération (NGAV), la détection et l'intervention sur les points d'accès (EDR), la détection et l'intervention sur le réseau (NDR), une analyse du comportement des utilisateurs et des entités (UEBA) et une technologie de simulation, le tout entièrement intégré et facilement configurable avec le tableau de bord unique qui est inclus.

Les avantages de Cynet pour le secteur des soins de santé

(suite)

Protection automatisée

L'*Incident Engine* de Cynet effectue automatiquement toutes les investigations sur les menaces et les mesures d'intervention requises, en identifiant la cause fondamentale et la portée complète des menaces à haut risque et en prenant les mesures appropriées pour éradiquer complètement la menace dans l'ensemble de l'environnement. Cynet offre en outre une liste de stratégies qui peuvent être exécutées automatiquement en réponse à une menace détectée pour une intervention immédiate ou qui peuvent être déclenchées manuellement pour fournir plus de supervision et de contrôle. Les actions d'intervention autonomes de Cynet offrent la protection complète que les petites équipes de sécurité surchargées recherchent.

Supervision de la détection et des interventions gérées incluse

Tous les clients de Cynet sont automatiquement protégés par un service complet de détection et d'interventions gérées (MDR), lequel est inclus dans la plateforme Cynet sans frais supplémentaires. Les petites équipes de sécurité des entreprises du secteur des soins de santé peuvent compter sur l'équipe MDR de Cynet (CyOps) pour surveiller de façon proactive leur environnement 24 heures sur 24, 7 jours sur 7, afin de s'assurer que rien n'est négligé. Elles peuvent contacter VARS à tout moment pour obtenir des conseils sur la configuration de la plateforme Cynet. CyOps leur offre une expertise en matière d'investigation des attaques et les guide dans toutes les interventions nécessaires. CyOps devient un prolongement de l'équipe de sécurité de l'entreprise de soins de santé, ajoutant des ressources et une expertise de classe mondiale en matière de cybersécurité.

Résumé

Protéger les environnements de soins de santé des cyberattaques représente un véritable défi, surtout avec une équipe de sécurité réduite et moins expérimentée. Avec des budgets limités, la plupart des entreprises de soins de santé de petite et de moyenne taille ne peuvent pas obtenir, intégrer et exploiter les contrôles de sécurité nécessaires pour protéger leur organisation contre les menaces avancées. Les entreprises de soins de santé peuvent compter sur la plateforme intuitive et complète de protection contre les intrusions de Cynet pour résoudre leurs enjeux de sécurité, tout en sachant qu'elles bénéficient toujours d'une équipe d'experts en cybersécurité pour les appuyer.