De la dépendance à l'EDR à la résilience

Combler les failles de sécurité entre réseaux et endpoints

En bref

Les technologies EDR et XDR sont essentielles, mais elles n'ont jamais été conçues pour défendre contre l'ensemble du spectre des menaces modernes et multi-domaines. Les attaquants exploitent les failles de sécurité entre les endpoints, les réseaux, les services cloud et les environnements OT ; précisément là où la visibilité diminue et où les solutions ponctuelles peinent à assurer une corrélation des informations.

Cet e-book propose de repenser la manière dont les organisations construisent leur résilience. Il explique pourquoi les défenses centrées uniquement sur les endpoints ne suffisent plus et comment l'unification des données de processus des endpoints avec la télémétrie réseau crée une base plus solide pour la détection, l'investigation et la réponse aux menaces. Tout au long de ce document, nous mettons en lumière des exemples d'attaques ayant contourné les outils de sécurité des terminaux, la pression que ces failles de sécurité exercent sur les équipes SOC, ainsi que la voie à suivre grâce à la télémétrie combinée.

EDR/XDR : nécessaires mais incomplètes
Ces outils protègent efficacement les endpoints, mais manquent de visibilité sur les appareils non gérés, les environnements sans agent et les attaques réseau.

La télémétrie combinée comble les failles d'investigation
En associant l'activité réseau aux données de processus des endpoints, les analystes obtiennent une vision unifiée qui réduit les faux positifs, accélère le triage et permet de contenir les menaces plus tôt.

La résilience exige une nouvelle fondation pour le SOC
Les plateformes auto-apprenantes et adaptatives, ancrées dans la visibilité réseau, fournissent le contexte et l'efficacité nécessaires pour réduire l'épuisement des analystes, diminuer le MTTR et combler les angles morts entre les domaines.

Pourquoi l'EDR est nécessaire, mais insuffisante

Aujourd'hui, la majorité des entreprises ont investi dans l'EDR (Endpoint Detection and Response) ou dans son évolution la plus récente, la XDR (Extended Detection and Response).

L'EDR est **spécifiquement conçue** pour l'endpoint. Elle surveille les processus au niveau de l'hôte, la mémoire et les journaux, et permet le confinement et la remédiation directement sur l'appareil.

La XDR est apparu chez les fournisseurs EDR pour tenter de **résoudre le problème de manque de structure du contrôle,** en corrélant les alertes de plusieurs solutions de sécurité au sein d'une plateforme unique. En pratique, cependant, la plupart des offres XDR restent centrées sur l'EDR. Elles étendent la visibilité, mais demeurent ancrées sur un agent de gestion du terminal.

57 % des organisations prévoient d'ajouter des capacités NDR (Network Detection and Response) à leur gamme d'outils XDR

Gartner, 2023

Lacunes de couverture

Lorsque la détection repose principalement sur la télémétrie des terminaux, des angles morts persistent au niveau des réseaux, des appareils non gérés, des charges de travail cloud et des systèmes d'identité. Les solutions XDR centrées sur l'EDR ne peuvent pas observer les mouvements latéraux ni l'activité dans des environnements sans agent, comme l'OT, laissant des infrastructures critiques sans protection.

Réponse fragmentée

La plupart des outils NDR manquent de contexte terminal, obligeant les analystes à naviguer entre plusieurs consoles pour reconstituer une attaque. Cet effort manuel ralentit les investigations, augmente le MTTR, et permet à des menaces se déplaçant entre terminaux et réseaux de rester non détectées.

L'EDR se concentre sur...

Les menaces « known bad » (connues comme malveillantes). Cela signifie qu'une alerte n'est générée que lorsque l'activité sur le terminal correspond à des critères connus ou à des règles/signatures prédéfinies.

L'EDR ne comprend pas...

Ce qui est normal ou anormal pour un hôte donné. Elle applique des règles basées sur des comportements d'attaquants connus. Cette approche est efficace pour les menaces déjà identifiées, mais elle laisse des lacunes de couverture face à des menaces inédites ou à des attaques qui exploitent des outils légitimes pour se dissimuler à découvert.

Le résultat...

Les ransomwares, l'exfiltration de données et les campagnes multi-étapes réussissent malgré une forte couverture des terminaux. L'EDR reste très efficace pour surveiller l'activité des hôtes, mais les adversaires modernes ne se limitent plus aux terminaux : ils exploitent les zones de jonction entre les domaines, là où la visibilité diminue et où les analystes peinent à corréler les informations.

Éléments de preuve
Là où la visibilité EDR s'arrête

Contournement de l'EDR via des outils de neutralisation d'agents

Les attaquants utilisent des outils tels que EDRKillShifter et EDRSilencer pour désactiver les agents de gestion des terminaux, aveuglant instantanément les défenses reposant uniquement sur le terminal. Ces techniques démontrent à quel point les adversaires peuvent neutraliser facilement des solutions de sécurité basées sur des agents, quel que soit leur niveau de sophistication.

Enseignements des équipes Red Team de la CISA

Une évaluation de la CISA portant sur des infrastructures critiques américaines a révélé qu'une dépendance excessive à l'EDR laissait des failles de sécurité majeures au niveau du réseau. Les adversaires ont pu maintenir une présence pendant plusieurs mois sans déclencher d'alertes au niveau des hôtes, preuve qu'une visibilité isolée n'est pas suffisante.

Exploitation de vulnérabilités zero-day au niveau du réseau

Lors de l'exploitation d'Ivanti Connect Secure en 2024, la télémétrie réseau a détecté des anomalies 11 jours avant la divulgation publique, révélant des abus d'identifiants et des activités de commande et contrôle (C2) invisibles pour les outils de sécurité des terminaux. La NDR a fourni la visibilité nécessaire pour contenir la menace de manière anticipée.

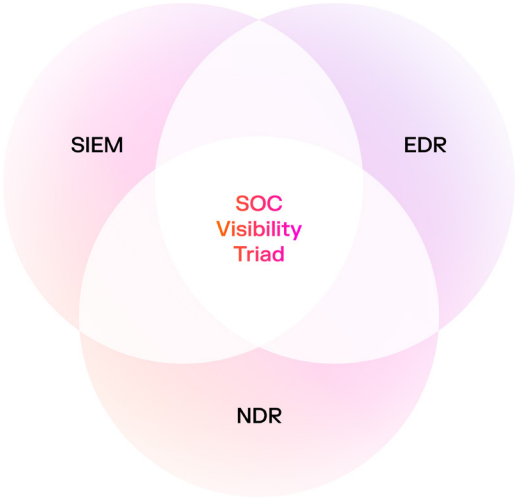
Construire une défense résiliente

L'EDR constitue un socle essentiel, mais ce n'est qu'en la reliant à une visibilité réseau complète qu'elle devient un élément d'une architecture de sécurité véritablement résiliente. Même les solutions XDR, bien qu'offrant une couverture plus large, reposent encore fortement sur la surveillance au niveau de l'hôte et manquent souvent de visibilité réseau native.

Visibilité unifiée sur les terminaux, les réseaux, le cloud, l'OT et les identités

Télémétrie intégrée provenant d'actifs gérés et non gérés.

Systèmes adaptatifs capables de comprendre le comportement normal et de détecter l'inconnu.



Contournement de l’EDR
Activités post-exploitation des appliances Ivanti CS/PS

Exemple d’attaque

Cette campagne Ivanti montre que les attaquants savent précisément là où s’arrête la visibilité sur les endpoints. Ils exploitent des actifs réseau non gérés, se déplacent latéralement et se dissimulent dans le trafic chiffré. Mais pour les équipes de défense, le véritable défi ne s’arrête pas à la détection : il repose sur les équipes SOC, qui doivent analyser, corréler et donner du sens à l’ensemble de ces signaux.

Une première activité de beaconing vers une adresse IP externe rare a été observée. Les agents de gestion des terminaux n’étaient pas en jeu ici, l’appliance Ivanti compromise étant un actif réseau et non un endpoint traditionnel. Seule la visibilité réseau a permis de révéler cette anomalie précoce.

Une activité de beaconing secondaire vers un autre hôte inhabituel a ensuite été détectée. Les adversaires ont étendu leurs points d’appui via la couche réseau. Sans couverture par agent, les outils EDR n’auraient eu aucune donnée à corréler.

Des activités de validation d’exploitation utilisant des services OAST ont été identifiées. Les attaquants ont réussi l’exploitation via des canaux hors bande. Ces vérifications n’ont jamais impliqué la pile endpoint, soulignant pourquoi la télémétrie réseau est essentielle.

D’importants transferts POST de fichiers .dat et .sys vers un serveur externe ont révélé une exfiltration de données de l'hôte. Des fichiers système sensibles ont été exfiltrés via le réseau. Les outils de sécurité des terminaux surveillant les processus hôtes ne pouvaient pas voir ce trafic sortant.

Des charges utiles ELF Rust malveillantes ont été livrées depuis des endpoints AWS S3. La distribution des charges utiles s’appuyait sur un service cloud. Même si l'EDR était présente ailleurs dans l’environnement, ces implants ont contourné les défenses basées sur l’hôte en entrant par la périphérie réseau.

Des web shells et des stealers JavaScript ont été déployés pour collecter des identifiants. L’activité de vol d'identifiants s’est déroulée au niveau d’une appliance réseau, et non sur un endpoint utilisateur. Cela signifie que la compromission des identités est née en dehors du champ de visibilité EDR.

Des scans réseau et des mouvements latéraux ont été observés à l’intérieur de l’environnement. Il s’agit d’un cas typique d’exploitation d’actifs non gérés, que les attaquants traversent librement. L'EDR ne pouvant instrumenter ces appareils, les analystes restent aveugles sans NDR.

Un trafic de commande et contrôle chiffré, dissimulé via DNS tunneling, a ensuite été détecté, suivi du déploiement d’un cryptominer. Ces canaux réseau furtifs ont permis une persistance durable. Les solutions basées sur les endpoints ne sont pas en mesure de détecter de façon fiable les abus de DNS chiffré : cela nécessite une détection des anomalies au niveau du réseau.

La télémétrie réseau a permis de mettre en évidence ces comportements plusieurs jours avant la divulgation publique des vulnérabilités. La détection ne provenait ni de signatures ni de journaux endpoint, mais de déviations comportementales dans le trafic réseau, démontrant pourquoi une couverture multi-domaines est aujourd’hui indispensable.

Le point de rupture du SOC

Angles morts, épuisement des équipes et risque pour l'entreprise

Au-delà de la visibilité

Les méthodes de détection centrées sur l'attaquant peinent à identifier les menaces inédites, car elles reposent sur des règles statiques et des données d'attaques historiques, en se concentrant sur l'identification du « known bad ». Ces outils passent souvent à côté d'activités malveillantes qui paraissent légitimes en apparence, telles que :

- Living off the Land (LotL)
- Abus d'identifiants valides
- Menaces internes
- Applications tierces autorisées

Plus de complexité = plus de problèmes

Dans les environnements OT, la plupart des fournisseurs se concentrent sur la visibilité des actifs ou sur des détections basées sur des règles, sans modéliser la manière dont les attaquants peuvent se déplacer de l'IT vers l'OT, exploiter des CVE exposées ou perturber des opérations critiques via une segmentation mal configurée.

Sans véritable modélisation de la convergence, les défenseurs se retrouvent avec des vues cloisonnées et une protection contre les menaces incomplète.

La solution
Renforcer la résilience grâce à une télémétrie combinée

La réponse à ces défis consiste à unifier les données de processus au niveau des endpoints et la télémétrie réseau la plus fine au sein d'un flux unique. En fusionnant ces sources de données dès le point de collecte :

Des investigations plus rapides
unifient les données de processus endpoint et de l'activité réseau pour accélérer l'analyse.

Une vision unifiée des incidents
permet de suivre les activités de processus et les mouvements latéraux sans avoir à reconstituer manuellement des fragments provenant de multiples outils.

De meilleurs résultats
réduisent les faux positifs, raccourcissent les cycles de triage et renforcent les capacités de confinement.

Il est important de souligner que cette approche **ne remplace pas** les investissements existants en EDR ou XDR, mais les complète. Les défenses endpoint restent fondamentales, mais associées à une visibilité au niveau réseau, leur couverture s'étend aux appareils non gérés, aux charges de travail cloud et au trafic chiffré.

Il en résulte une pile de sécurité alignée sur la réalité des menaces modernes, et non limitée par une visibilité centrée uniquement sur les endpoints.

Repenser les fondations du SOC

Pour dépasser les défenses fragmentées, les équipes de sécurité ont besoin d'une base capable de structurer l'ensemble du SOC. Cette base, c'est le réseau. Chaque endpoint, chaque charge de travail cloud, chaque équipement OT ou chaque identité laisse inévitablement une trace dans le trafic réseau. En considérant le réseau comme un « point d'ancrage », les organisations disposent d'un prisme commun pour comprendre tous les autres domaines.

Cette base n'implique pas une approche uniforme. Chaque organisation possède un environnement numérique unique, combinant services cloud, infrastructures héritées, endpoints distants et environnements OT. Les détections statiques et prédéfinies ne peuvent pas anticiper tous les nouveaux chemins d'attaque ni les dérives de configuration. Ce qu'il faut, c'est de l'adaptabilité : un système capable d'apprendre les comportements normaux de votre environnement, d'évoluer avec lui et de mettre en évidence les anomalies dès leur apparition.

En s'appuyant sur la visibilité réseau comme point d'ancrage, une plateforme unifiée apporte des bénéfices clés :

Adaptabilité, grâce à un apprentissage autonome et continu, capable d'évoluer au rythme des environnements et des menaces.

Efficacité, en consolidant la détection et la réponse à travers les différents domaines, réduisant la prolifération des outils et des fournisseurs.

Résilience, en corrélant la télémétrie en temps réel, en éliminant le bruit et en faisant ressortir les incidents réellement critiques.

Pourquoi Darktrace ?

Darktrace est reconnu comme leader du marché de la NDR, grâce à sa Self-Learning AI ™, qui comprend ce qui est normal pour l'ensemble de votre réseau, détecte intelligemment les anomalies et contient les menaces sophistiquées sans nécessiter de données d'attaques historiques.

Cette approche, basée sur un apprentissage automatique avancé et non supervisé, permet à Darktrace de détecter des menaces inédites, inconnues ou internes que les outils traditionnels manquent, et que d'autres fournisseurs ne peuvent identifier.

Au moment où les attaques s'étendent à la messagerie électronique, au cloud, à l'OT, aux applications SaaS et aux endpoints, Darktrace a franchi une étape majeure : unifier la télémétrie et le contexte à travers ces domaines et appliquer une investigation pilotée par l'IA à grande échelle. En combinant les données de processus au niveau des endpoints avec la visibilité réseau, Darktrace permet aux équipes de sécurité de voir l'ensemble du cycle de vie d'une attaque et agit de manière autonome, réduisant ainsi les angles morts, le temps d'investigation et la charge des analystes.

« Darktrace n'est pas seulement une technologie. C'est un outil qui permet **d'instaurer la confiance, tout en justifiant et soutenant une croissance intelligente** sur l'ensemble de notre paysage système et de cybersécurité. »

- **CIO**

  Services gouvernementaux

Consultez la

Présentation de la solution Darktrace / Endpoint

Télécharger la présentation

Demandez une démo

Découvrez ce que Darktrace détecte dans votre environnement

Réserver une démo