The Forrester Wave™ : les plateformes d'analyse de la sécurité, 4e trimestre 2020

Les 11 principaux fournisseurs et leur place sur le marché

Par Joseph Blankenship et Claire O'Malley

1er décembre 2020

Pourquoi lire ce rapport

Dans notre évaluation à 27 critères des fournisseurs de plateformes d'analyse de la sécurité, nous avons identifié les 11 plus importants : Exabeam, FireEye, Gurucul, IBM Security, LogRhythm, Micro Focus, Microsoft, Rapid7, RSA, Securonix et Splunk. Nous les avons étudiés, analysés et notés. Ce rapport montre comment chaque fournisseur se positionne par rapport à ses concurrents et aide les professionnels de la sécurité et la gestion des risques à sélectionner des solutions adaptées à leurs besoins.

Points clés à retenir

IBM Security, Splunk, Securonix, Exabeam et Microsoft mènent la danse

Les recherches de Forrester ont révélé un marché sur lequel IBM Security, Splunk, Securonix, Exabeam et Microsoft arrivent en tête ; LogRhythm, Gurucul, Micro Focus, Rapid7 et RSA sont des acteurs majeurs ; et FireEye est un prétendant.

La personnalisation, le mappage MITRE ATT&CK et la livraison SaaS sont des facteurs de différenciation clés

Tandis que la technologie de gestion des événements et des informations de sécurité (SIEM) devient obsolète et moins efficace, les plateformes d'analyse de sécurité dans le cloud proposant des détections personnalisées prendront la tête du secteur. Les fournisseurs qui proposent la personnalisation, le mappage MITRE ATT&CK et la livraison SaaS sont en mesure de fournir à leurs clients une meilleure détection, des enquêtes plus rapides et une flexibilité accrue.

The Forrester Wave™ : les plateformes d'analyse de la sécurité, 4e trimestre 2020

Les 11 principaux fournisseurs et leur place sur le marché

Par Joseph Blankenship et Claire O'Malley
Avec Stephanie Balaouras, Alexis Bouffard et Peggy Dostie

1er décembre 2020

Sommaire

Documents de recherche connexes

The Forrester Wave™: Security Analytics Platforms, Q3 2018

Now Tech: Security Analytics Platforms, Q3 2020

The State Of Network Security: 2018 To 2019

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 États-Unis
+1 617-613-6000 | Fax : +1 617-613-5000 | forrester.com

L'avenir de l'analyse de la sécurité est dans le cloud

Par le passé, les fournisseurs proposaient des systèmes SIEM traditionnels en tant que déploiements matériels ou logiciels sur site. Par conséquent, les professionnels de la sécurité avaient du mal à gérer et à mettre à jour ces systèmes, ainsi qu'à ajouter continuellement du stockage pour les volumes de logs en constante augmentation. Dans *L'Empire contre-attaque*, Lando Calrissian déclare à la princesse Leia : « You truly belong here with us among the clouds. » (Comprenez : Vous êtes faite pour vivre dans les nuages avec nous). Il en va de même pour les plateformes d'analyse de la sécurité. Alors que les entreprises ont déplacé leurs propres workloads vers le cloud pour tirer parti de son évolutivité, de sa flexibilité et de sa disponibilité, les fournisseurs de solutions de sécurité ont finalement commencé à suivre la même voie en livrant leurs solutions d'analyse de sécurité dans le cloud. Cette transition et l'entrée de fournisseurs cloud natifs indiquent que l'analyse de la sécurité fait partie du cloud.

La plupart des fournisseurs inclus dans l'évaluation 2020 de Forrester sur le marché des plateformes d'analyse de la sécurité fournissent leurs produits via des modèles SaaS ou hébergés dans le cloud. Ce changement a permis aux fournisseurs de déployer plus rapidement de nouvelles fonctionnalités auprès de leurs clients et de réduire les frais de gestion de ces systèmes. Les professionnels de la sécurité qui souhaitent remplacer leurs solutions sur site existantes doivent rechercher des fournisseurs qui offrent la plupart de leurs fonctionnalités, sinon toutes, dans le cloud. De ce fait, les clients de plateforme d'analyse de la sécurité doivent rechercher des fournisseurs capables de répondre aux besoins suivants :

- **Offrir une personnalisation aux clients.** La plupart des fournisseurs proposent des contenus prêts à l'emploi (OOTB) qui peuvent être personnalisés par les entreprises pour répondre à leurs besoins individuels. Les utilisateurs plus avancés souhaitent également développer des détections personnalisées pour des scénarios spécifiques. Certains fournisseurs mettent leurs modèles de machine learning à la disposition des clients qui veulent créer leurs propres modèles.
- **Offrir de véritables analyses et opérations.** De nombreux fournisseurs d'analyses de la sécurité proposent des analyses de base, axées sur le comportement des utilisateurs, et peu ou pas d'automatisation. Les fournisseurs les plus puissants offrent des fonctionnalités d'analyse avec plusieurs types de machine learning et incluent l'orchestration, l'automatisation et la réponse de sécurité (SOAR). La combinaison de l'analyse et de l'automatisation permet aux plateformes d'analyse de la sécurité de proposer des opérations intelligentes capables d'identifier les menaces et d'y répondre automatiquement.
- **Mapper la structure MITRE ATT&CK.** Les professionnels de la sécurité ont rapidement adopté la structure MITRE ATT&CK dans le cadre de leurs opérations de sécurité. Les fournisseurs d'analyse de sécurité ont répondu en mappant leurs solutions en fonction du cadre de détection, d'investigation et de recherche de menaces. Ceux disposant des fonctionnalités les plus avancées montrent également quelles parties de MITRE ATT&CK sont couvertes dans les environnements des clients.
- **Avoir une vision de la détection et de la réponse étendues (XDR).** La détection et la réponse des points de terminaison (EDR) et l'analyse de la sécurité sont en concurrence depuis longtemps. Le chevauchement de ces fonctionnalités combine l'EDR aux analyses d'autres technologies, offrant ainsi une télémétrie hautement enrichie, des investigations rapides et des actions de réponse automatisées.

Résumé de l'évaluation

L'évaluation Forrester Wave™ met en évidence les leaders, les acteurs majeurs, les prétendants et les challengers. Cette évaluation des principaux fournisseurs du marché ne représente pas l'ensemble des fournisseurs. Vous trouverez plus d'informations sur ce marché dans le rapport Forrester « Now Tech: Security Analytics Platforms, Q3 2020 ».

Nous souhaitons que cette évaluation soit un point de départ qui incite les clients à consulter les évaluations produit et à adapter la pondération des critères à l'aide de l'outil de comparaison des fournisseurs de type Excel (voir les figures 1 et 2). Cliquez sur le lien Forrester.com figurant au début de ce rapport pour télécharger l'outil.

FIGURE 1 Forrester Wave™ : les plateformes d'analyse de la sécurité, 4e trimestre 2020

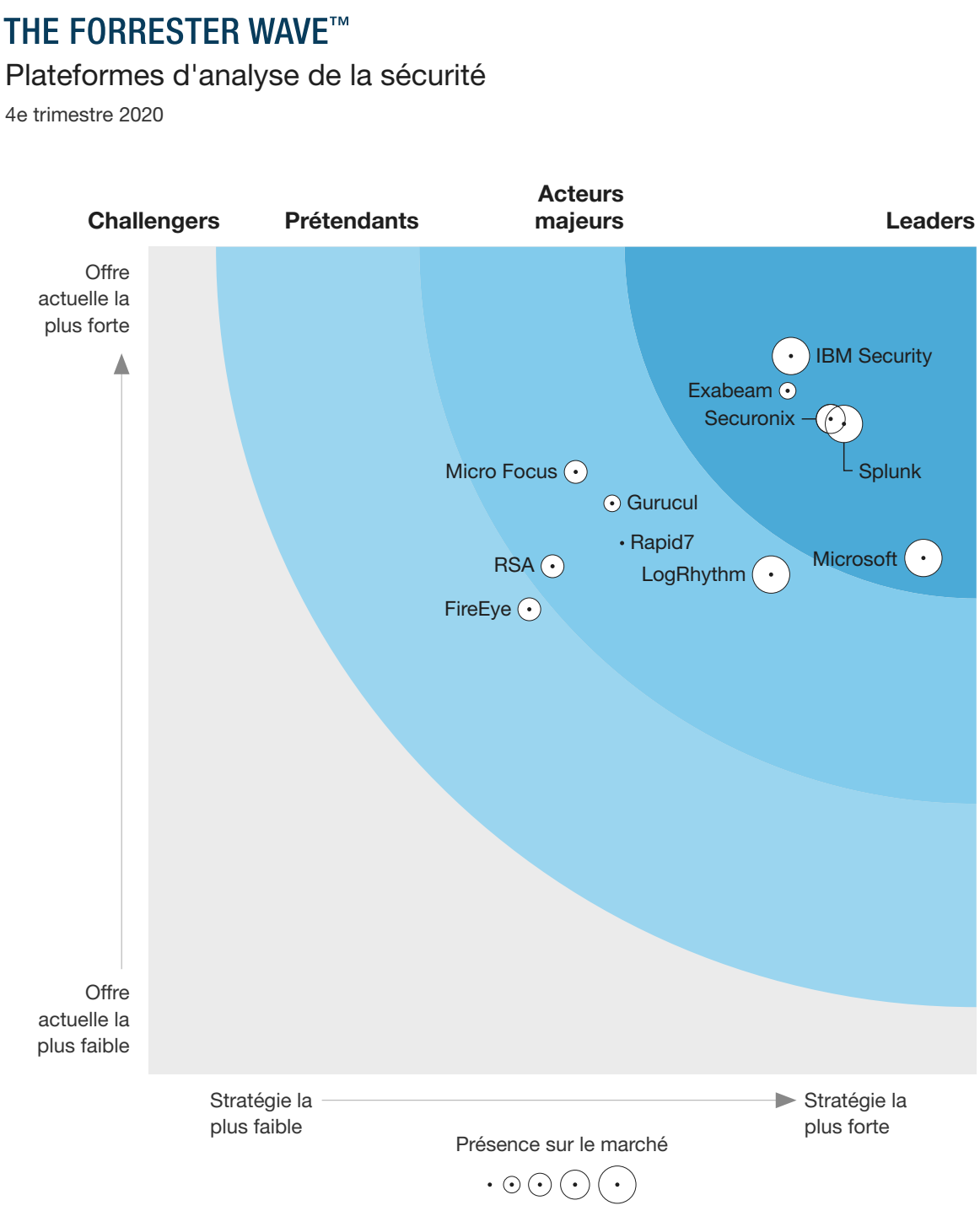

FIGURE 2 Forrester Wave™ : le tableau de bord des plateformes d'analyse de la sécurité, T4 2020

	Pondération de Forrester	Exabeam	FireEye	Gurucul	IBM Security	LogRhythm	Micro Focus	Microsoft	Rapid7	RSA	Securonix	Splunk
Offre actuelle	50 %	4,13	2,81	3,45	4,34	3,02	3,64	3,12	3,21	3,07	3,96	3,93
Déploiement et architecture de données	5 %	3,40	3,40	3,80	3,40	3,40	2,20	4,20	3,80	1,80	5,00	2,20
Visibilité	10 %	3,00	3,00	3,00	5,00	3,00	3,00	1,00	3,00	5,00	3,00	3,00
Fonctionnalités de corrélation	10 %	5,00	3,00	5,00	5,00	3,00	5,00	5,00	5,00	3,00	5,00	5,00
Détection des menaces	20 %	4,60	3,00	3,40	4,60	4,20	4,20	2,60	4,20	3,00	3,80	4,20
Mappage ATT&CK	10 %	5,00	3,00	3,00	5,00	3,00	3,00	3,00	1,00	3,00	3,00	3,00
Détections personnalisées	5 %	5,00	3,00	5,00	5,00	3,00	3,00	3,00	1,00	3,00	5,00	5,00
Orchestration de la sécurité	10 %	3,00	5,00	1,00	5,00	1,00	3,00	3,00	3,00	3,00	3,00	3,00
Conformité	5 %	3,00	1,00	1,00	5,00	5,00	5,00	3,00	3,00	3,00	3,00	5,00
Expérience de la plateforme	5 %	3,60	3,60	1,60	3,00	3,00	3,00	3,00	3,60	1,60	3,00	4,40
Analyse	10 %	3,60	1,60	5,00	3,00	1,60	4,40	4,40	3,00	3,00	5,00	3,60
Notation et hiérarchisation des risques	10 %	5,00	1,00	5,00	3,00	3,00	3,00	3,00	3,00	3,00	5,00	5,00
Stratégie	50 %	3,86	2,30	2,80	3,88	3,76	2,58	4,68	2,86	2,44	4,12	4,20
Vision du produit	25 %	3,00	3,00	3,00	5,00	3,00	3,00	5,00	3,00	3,00	5,00	5,00
Améliorations prévues	25 %	5,00	3,00	3,00	3,00	5,00	3,00	5,00	3,00	3,00	3,00	5,00
Performances	25 %	5,00	1,00	3,00	3,00	3,00	1,00	5,00	3,00	1,00	5,00	3,00
Modèle commercial	15 %	3,40	3,00	3,00	4,20	3,40	2,20	4,20	3,40	2,60	3,80	3,00
Partenaires technologiques	10 %	1,00	1,00	1,00	5,00	5,00	5,00	3,00	1,00	3,00	3,00	5,00
Présence sur le marché	0 %	1,40	3,00	1,80	4,60	4,60	3,00	4,20	1,00	3,00	3,40	5,00
Adoption par les entreprises	80 %	1,00	3,00	1,00	5,00	5,00	3,00	5,00	1,00	3,00	3,00	5,00
Valeur moyenne des transactions	20 %	3,00	3,00	5,00	3,00	3,00	3,00	1,00	1,00	3,00	5,00	5,00

Tous les résultats sont basés sur une échelle de 0 (faible) à 5 (fort).

Offres des fournisseurs

Forrester a inclus 11 fournisseurs dans cette évaluation : Exabeam, FireEye, Gurucul, IBM Security, LogRhythm, Micro Focus, Microsoft, Rapid7, RSA, Securonix et Splunk (voir figure 3). Les entreprises Fortinet et McAfee, invitées à participer à cette enquête Forrester Wave, ont choisi de se désister, et nous n'avons pas pu estimer suffisamment leurs capacités pour les inclure dans l'évaluation en tant que fournisseurs non participants.

FIGURE 3 Informations sur les produits et les fournisseurs évalués

Fournisseur	Produit évalué
Exabeam	Exabeam Security Management Platform 2020.1
FireEye	FireEye Helix
Gurucul	Unified Security and Risk Analytics (USRA) 8.0
IBM Security	IBM Security QRadar 7.4.0 ; IBM Security Resilient v37
LogRhythm	LogRhythm NextGen SIEM Platform 7.5
Micro Focus	ArcSight 2020.2
Microsoft	Azure Sentinel
Rapid7	InsightIDR
RSA	RSA NetWitness Platform v11.4 ; RSA NetWitness Orchestrator v6.0
Securonix	Securonix Next-Gen SIEM 6.3
Splunk	Splunk Enterprise 8.0 ; Splunk Cloud ; Splunk Enteprise Security (ES) 6.2 ; Splunk User Behavior Analytics (UBA) 5.0 ; Splunk Phantom 4.9 ; Splunk Mission Control (MC)

Profils des fournisseurs

Les points forts et les points faibles de chaque fournisseur mis en évidence par notre analyse sont présentés ci-dessous.

Leaders

› **IBM Security développe une plateforme de sécurité ouverte dans le cloud.** L'avenir de la plateforme d'analyse de la sécurité d'IBM repose sur sa plateforme CloudPak For Security, basée sur l'architecture cloud native OpenShift et sur son acquisition de RedHat, dont l'objectif est de fournir plusieurs services de sécurité dans le cloud IBM. Des fonctionnalités telles qu'IBM QRadar Advisor avec Watson, X-Force Threat Intelligence et l'intégration des services de sécurité gérés d'IBM sont des

facteurs de différenciation. La fonction SOAR est fournie via IBM Security Resilient en tant que module complémentaire. Les options de tarification incluent une licence basée sur la consommation déterminée par la quantité d'événements ingérés dans le système, et une licence illimitée pour l'acquisition, l'analyse et le stockage en fonction du nombre de serveurs dans l'environnement.

Les clients interrogés apprécient la portée mondiale, l'assistance technique et l'innovation d'IBM. Ils ont noté que de nombreuses nouvelles fonctionnalités sont fournies sous forme d'applications, et non d'améliorations du produit de base, et que certaines visualisations semblent obsolètes. Les faiblesses mentionnées incluent la complexité des installations sur site et la difficulté à trouver la documentation produit et les pages d'assistance. IBM peut convenir aux grandes entreprises internationales ayant des besoins complexes en matière de sécurité.

› **Splunk s'est donné pour mission l'analyse de la sécurité.** La plupart des entreprises utilisent Splunk à des fins de surveillance de l'infrastructure, d'analyse des applications ou de sécurité. Concernant la sécurité, Splunk construit son avenir autour de sa plateforme de sécurité unifiée basée sur le cloud, Mission Control. Splunk a mis plus de temps à adopter le cloud que certains autres participants à cette évaluation et que les nouveaux arrivants cloud natifs sur le marché de l'analyse de la sécurité, mais l'entreprise fait désormais du cloud une priorité pour l'avenir. Splunk propose une gamme d'options de tarification, notamment basées sur les workloads, les cas d'utilisation et le modèle traditionnel basé sur la consommation et déterminé par le volume de données ingéré par la plateforme.

  La flexibilité et la possibilité d'effectuer des recherches rapides sur de gros volumes de données sont des fonctionnalités clés de Splunk. Les clients interrogés indiquent que la vitesse, la polyvalence et la personnalisation sont les principaux points forts. Ils louent également Splunk pour son immense communauté d'utilisateurs engagés. En revanche, les prix restent un point faible. Splunk a fait des efforts pour améliorer sa tarification et offrir plus de flexibilité, mais les clients interrogés s'accordent à dire que le coût est une faiblesse. Splunk pourrait convenir aux entreprises qui recherchent une solution hautement personnalisable permettant des recherches rapides sur de gros volumes de données.

› **Securonix offre une analyse de la sécurité multi-tenante livrée en mode SaaS.** Securonix a débuté en tant que fournisseur SUBA en 2008, avant d'ajouter la fonctionnalité SIEM en 2016 afin de pouvoir rivaliser avec les autres plateformes d'analyse de la sécurité. Le fournisseur a depuis ajouté l'automatisation sous forme de fonctionnalité complémentaire ou via des intégrations tierces. Securonix a adopté une stratégie de déploiement SaaS axée sur le cloud, avec des options de déploiement flexibles, telles que la multi-tenancy, ce qui le rend attrayant pour les partenaires MSSP. L'approche tarifaire du fournisseur repose sur le nombre d'identités surveillées.

  Selon les témoignages des clients, l'approche basée sur l'analyse, l'analyse comportementale et l'enrichissement en temps réel de Securonix sont des atouts. Concernant les inconvénients, les clients interrogés notent des retards concernant l'ingestion de logs et de petits bogues dans l'interface utilisateur. Securonix peut convenir aux entreprises de taille moyenne à la recherche d'une plateforme d'analyse de la sécurité flexible ou d'une solution multi-tenant.

› **Exabeam excelle dans l'expérience utilisateur.** Lors de son lancement en 2014, Exabeam était davantage axé sur SUBA. Il a lancé ses offres SIEM et SOAR en 2017, et a connu une croissance rapide. La plateforme de gestion de la sécurité Exabeam combine des fonctions d'analyse intégrées, de gestion des logs et de SOAR qui peuvent fonctionner comme une plateforme combinée ou comme des solutions autonomes. Les incidents sont en grande partie basés sur le comportement et les

ressources des utilisateurs, et les analystes en sécurité peuvent visualiser l'historique des évènements pour leurs enquêtes. Exabeam propose plusieurs modèles de tarification, y compris la tarification basée sur le nombre d'employés supervisés ou la quantité de données ingérées.

Parmi les points forts, les clients interrogés notent la convivialité et la compréhension des comportements individuels des utilisateurs. Ils considèrent également la stratégie de tarification du fournisseur comme une caractéristique attrayante. Les témoignages des clients signalent que la croissance rapide du fournisseur peut nuire à la qualité du support technique et indiquent que les nouvelles fonctionnalités présentent souvent des bogues lors de la première version. Les entreprises de taille moyenne et celles recherchant une plateforme d'analyse de la sécurité modulaire, mais intégrée et axée sur le comportement des utilisateurs, devraient envisager Exabeam.

› **Microsoft s'invente sur le marché de l'analyse de la sécurité.** Microsoft Azure Sentinel, la solution d'analyse de la sécurité du fournisseur, a été annoncée lors de la conférence RSA sur la sécurité de 2019, puis lancée en grande pompe en septembre de la même année. L'entrée du fournisseur dans l'espace de l'analyse de la sécurité a captivé les acheteurs du secteur. La décision audacieuse de Microsoft de permettre l'ingestion gratuite des logs d'activité Microsoft Azure et Microsoft Office 365 dans Sentinel rend la solution attrayante pour les entreprises qui utilisent déjà Azure et Microsoft 365. La tarification des autres sources de données est basée sur la consommation, déterminée par la quantité de données ingérée par la plateforme. En seulement un an, Microsoft a produit un impact significatif sur le marché.

Bien qu'Azure Sentinel soit innovant et tire pleinement parti de l'infrastructure Azure, il s'agit toujours d'une offre très récente. Cette nouveauté se manifeste dans différents domaines et permet notamment d'introduire des logs tiers. Les clients interrogés notent la facilité d'intégration d'autres produits Microsoft (par exemple, Azure, Microsoft 365 et Windows Defender for Endpoint) comme un grand avantage. Selon les témoignages des clients, l'automatisation constitue un autre atout. La poussée de Microsoft dans le secteur pose problème aux professionnels de la sécurité qui ne souhaitent pas qu'un même fournisseur assure la sécurité de différentes couches, dont le cloud, les points de terminaison et la messagerie électronique. Toutefois, ceux qui recherchent une solution chez un fournisseur unique apprécieront les intégrations entre les technologies. Les entreprises de toutes tailles qui se reposent beaucoup sur Microsoft Azure et Microsoft 365 devraient envisager Microsoft.

Acteurs majeurs

› **LogRhythm offre une flexibilité de déploiement pour l'analyse de la sécurité d'entreprise.** LogRhythm, acquis par la société de capital-investissement Thoma Bravo en juillet 2018, est un acteur de longue date sur le marché des SIEM. Connue depuis longtemps comme une solution de milieu de gamme, LogRhythm propose une plateforme d'analyse de la sécurité riche en fonctionnalités et adaptée aux entreprises de toutes tailles. La licence de base du fournisseur inclut les SIEM, l'analyse et l'automatisation. Mais SUBA, fourni via son IA cloud, doit être acheté en complément. LogRhythm propose des appliances sur site, des appliances virtuelles, des logiciels et des solutions SaaS. En 2020, dans le but d'offrir aux clients une tarification flexible, LogRhythm a introduit son forfait de données True Unlimited, un modèle qui promet une utilisation illimitée des données comme alternative à son modèle basé sur la consommation, dont les prix sont déterminés par le nombre de messages par seconde (MPS).

Les clients interrogés font remarquer que la solution est facile à utiliser et s'adapte bien à la croissance. Ils notent également l'assistance client comme un atout. Les témoignages des clients mentionnent que les fonctionnalités d'automatisation et de réponse rapide incluses ne sont pas à la hauteur des solutions autonomes SOAR et que la prise en charge des environnements cloud et SaaS tiers ne répond pas aux attentes. LogRhythm peut convenir aux moyennes et grandes entreprises recherchant une plateforme d'analyse de la sécurité complète avec des options de déploiement flexibles.

› **Gurucul propose une analyse des données basée sur le risque.** Gurucul est apparu comme fournisseur d'analyses de sécurité Big Data en 2010 et a évolué en tant que fournisseur de plateforme d'analyse de sécurité couvrant SUBA, SIEM et SOAR. Gurucul propose sa propre architecture de Big Data et prend également en charge les dépôts de données tiers fournis par le client. Le fournisseur permet aux clients de personnaliser ses modèles d'analyse ou de créer leurs propres modèles via Gurucul STUDIO. Gurucul offre des fonctions personnalisables de profilage des comportements de machine learning ainsi que des fonctions de notation prédictive des risques, et des alertes hiérarchisées en fonction du risque. Gurucul se déploie en tant que logiciel pouvant être exécuté sur du matériel ou dans une infrastructure virtuelle fournies par le client, une appliance ou en tant que SaaS. Le fournisseur propose des licences par abonnement, perpétuelles et SaaS. La tarification de la solution est modulaire, avec des modules distincts pour SIEM, SUBA, le stockage personnalisé des logs, SOAR et NAV. Des tarifs d'entreprise sont disponibles. Le prix du monitoring dépend du nombre d'identités/entités surveillées.

  Les commentaires de clients interrogés indiquent que les modèles de machine learning de Gurucul, la notation des risques et la flexibilité sont des points forts. Les faiblesses mentionnées par les clients interrogés incluent la complexité de la solution et les efforts de commercialisation du fournisseur. Les entreprises à la recherche d'un outil d'analyse de la sécurité robuste et personnalisable proposant une hiérarchisation basée sur le risque devraient envisager Gurucul.

› **Micro Focus regroupe les essentiels de la plateforme d'analyse de la sécurité.** Micro Focus a réalisé des acquisitions stratégiques, avec notamment un fournisseur SUBA (Interset) et un fournisseur SOAR (Atar Labs), complétant son SIEM existant ArcSight, en retard sur le reste du marché depuis plusieurs années. ArcSight a longtemps été le fournisseur de prédilection pour certaines des plus grandes entreprises et agences gouvernementales du monde, bien que de nombreux clients de longue date aient abandonné la plateforme. Micro Focus progresse, mais a très tardivement adopté la livraison dans le cloud par rapport aux autres participants de cette évaluation. ArcSight se déploie en tant qu'appliances matérielles, conteneurs ou logiciels pouvant être déployés dans des environnements virtuels et dans le cloud. Micro Focus travaille actuellement à fournir une version SaaS complète. Le prix de la solution est basé sur EPS, et la fonction SUBA est vendue en tant que complément et sous licence selon le nombre d'entités gérées.

  Micro Focus investit dans le secteur d'analyse de la sécurité, ajoutant des fonctionnalités à sa plateforme, ce qui est encourageant. Les clients interrogés ont mentionné l'intégration avec d'autres produits, la corrélation et l'assistance mondiale comme points forts. Concernant les lacunes, ils ont noté la lenteur de la recherche, l'assistance et la console de gestion. Les entreprises qui ont investi dans d'autres éléments du portefeuille Micro Focus et celles qui recherchent un fournisseur doté d'une longue expérience dans le secteur de l'analyse de la sécurité devraient envisager Micro Focus.

› **Rapid7 combine plusieurs fonctionnalités de sécurité dans le cloud.** La plateforme InsightIDR de Rapid7 est entièrement livrée dans le cloud, offrant ainsi une gestion des logs, SIEM, SUBA et SOAR qui s'intègrent à sa plateforme de gestion des vulnérabilités. Le fournisseur propose également des fonctionnalités de visibilité et de détection des points de terminaison, de contrôle de l'intégrité des fichiers et de détection des fraudes. Grâce à l'acquisition de NetFort en 2019, il dispose de fonctionnalités NAV lui permettant de bénéficier d'une visibilité sur le trafic réseau et les comportements, disponibles en complément. Le fournisseur peut ajouter des services afin de partager avec les équipes internes de ses clients son expertise et son assistance. En tant qu'offre SaaS, la licence se présente sous la forme d'un modèle d'abonnement, et la tarification est basée sur le nombre d'actifs surveillés.

  Les commentaires des clients interrogés indiquent la facilité de déploiement et de fonctionnement comme points forts. Les lacunes mentionnées par les clients incluent un manque de personnalisation et des rapports limités. Les petites et moyennes entreprises, ainsi que les grandes sociétés à ressources limitées, qui recherchent une solution d'analyse de la sécurité basée sur le SaaS devraient envisager Rapid7.

› **RSA fournit une plateforme unifiée pour l'analyse de la sécurité.** RSA opère désormais de manière indépendante à la suite d'une sortie de Dell Technologies et d'une acquisition par un consortium d'investisseurs en septembre 2020[1]. L'entreprise fournit des fonctions SIEM, NAV, SUBA et SOAR grâce à son offre de plateforme RSA NetWitness. RSA NetWitness propose une détection et une visibilité des menaces grâce à une combinaison d'analyse des données de log, de point de terminaison et de paquet. La fonction SOAR est livrée via RSA NetWitness Orchestrator, construit via un accord OEM avec Threat Connect, disponible sous forme de licence séparée. La solution est livrée via du matériel ou un logiciel sur site, ou dans le cadre d'un déploiement mixte. La version logicielle peut être hébergée dans des environnements de cloud privé ou public, mais n'est pas disponible en tant qu'offre SaaS, bien qu'une fonctionnalité SaaS complète soit en cours de développement. La tarification est déterminée par les différents composants via une combinaison de tarification basée sur la consommation pour RSA NetWitness Logs et RSA NetWitness Network, et de tarification basée sur l'utilisateur pour RSA NetWitness UEBA, RSA NetWitness Endpoint et RSA NetWitness Orchestrator.

  RSA intègre sa propre fonctionnalité EDR pour la détection et la réponse à RSA NetWitness, en plus de prendre en charge les fournisseurs EDR tiers. Les clients interrogés apprécient la plateforme unifiée et les points forts tels que la combinaison de l'analyse des logs et des paquets. Ils ont noté que la solution est complexe, que l'interface utilisateur n'est pas intuitive et que la courbe d'apprentissage peut être abrupte pour les nouveaux utilisateurs. Les entreprises qui utilisent RSA Archer pour la gouvernance, la gestion du risque et la conformité (GRC) et celles qui recherchent un haut niveau de visibilité sur leur trafic réseau et l'EDR intégrée devraient envisager RSA.

Prétendants

› **FireEye offre une approche intégrée avec Helix.** FireEye combine ses fonctionnalités d'analyse de la sécurité et d'automatisation dans sa plateforme Helix. Helix englobe la rétention des logs, le SIEM, les renseignements sur les menaces (threat intelligence), la recherche de menaces et le SOAR. Le fournisseur propose Helix en tant que solution SaaS autonome ou peut l'intégrer à d'autres solutions FireEye comme la sécurité réseau, la sécurité de la messagerie électronique, la sécurité des points de

terminaison et Cloudvisory. L'acquisition de Verodin en 2019 a permis de visualiser la couverture de la structure MITRE ATT&CK en tant qu'achat complémentaire, bien que Helix permette de rechercher les menaces et de personnaliser les détections à l'aide d'ATT&CK. Les services Mandiant sont également disponibles pour renforcer Helix, en donnant accès à une expertise en matière de sécurité ou pour fournir des services gérés. Le prix du fournisseur est basé sur la consommation, lié aux EPS.

Les clients interrogés apprécient l'inclusion d'informations sur les menaces (threat intelligence), la possibilité d'accéder aux experts FireEye et le niveau d'intégration avec d'autres outils de sécurité FireEye. Même si la solution est bien intégrée à l'ensemble de la gamme FireEye, il n'existe pas de console d'administration centrale ni de tableau de bord pour tous les produits FireEye, ce que les clients considèrent comme une faiblesse. Les clients interrogés ont également mentionné l'absence de documentation pour le composant SOAR d'Helix et le manque de ressources qualifiées pour gérer la plateforme. Les entreprises qui font appel au fournisseur pour d'autres éléments de leur infrastructure de sécurité devraient envisager FireEye.

Vue d'ensemble de l'évaluation

Nous avons évalué les fournisseurs selon 27 critères, regroupés en trois catégories de haut niveau :

- **Offre actuelle.** La position de chaque fournisseur sur l'axe vertical du graphique Forrester Wave indique la solidité de son offre actuelle. Les critères clés de ces solutions incluent le déploiement et l'architecture de données, la visibilité, les fonctionnalités de corrélation, la détection des menaces, le mappage ATT&CK, les détections personnalisées, l'orchestration de la sécurité, la conformité, l'expérience de la plateforme, l'analyse, ainsi que l'évaluation et la hiérarchisation des risques.
- **Stratégie.** Le positionnement sur l'axe horizontal indique la solidité de la stratégie des fournisseurs. Nous avons évalué la vision du produit, les améliorations prévues, les performances, le modèle commercial et les partenaires technologiques.
- **Présence sur le marché.** Représentés par la taille des marqueurs sur le graphique, nos scores de présence sur le marché reflètent l'adoption de chaque solution par les entreprises et la taille moyenne de leurs transactions.

Critères d'inclusion des fournisseurs

Forrester a inclus 11 fournisseurs dans l'évaluation : Exabeam, FireEye, Gurucul, IBM Security, LogRhythm, Micro Focus, Microsoft, Rapid7, RSA, Securonix et Splunk. Eléments communs à tous les fournisseurs :

- **Revenus liés au produit.** Le fournisseur doit réaliser un chiffre d'affaires de 50 millions de dollars sur sa gamme de produits pour sa plateforme d'analyse de la sécurité.
- **Fonctionnalités de base.** Le fournisseur doit disposer d'une plateforme d'analyse de la sécurité comprenant des fonctionnalités SIEM et SOAR matures. Les fonctionnalités SOAR fournies peuvent être proposées en tant qu'élément propriétaire ou en marque blanche de la solution.
- **Notoriété pour Forrester.** Les clients de Forrester discutent souvent des fournisseurs participants au cours des enquêtes et des entretiens. Pour garantir la pertinence des participants pour les clients Forrester et la qualité des références fournies, il faut que le produit ait été publiquement disponible et n'ait pas subi de modifications importantes au cours des six derniers mois.

Collaborez avec un analyste

Prenez des décisions avisées en collaborant avec les leaders d'opinion de Forrester afin d'appliquer nos recherches à vos initiatives commerciales et technologiques spécifiques.

Enquête d'analyste

Pour vous aider à mettre en pratique vos recherches, contactez un analyste pour lui poser vos questions lors d'une séance téléphonique de 30 minutes ou demandez une réponse par e-mail.

En savoir plus.

Conseil d'analyste

Traduisez la recherche en action en travaillant avec un analyste sur un engagement spécifique sous forme de réunions sur la stratégie, d'ateliers ou de discours personnalisés.

En savoir plus.

Webinaire

Participez à nos sessions en ligne sur les dernières recherches concernant votre entreprise. Chaque session présente les questions-réponses des analystes et les diapositives, et est disponible à la demande.

En savoir plus.

Applications de recherche de Forrester pour iOS et Android.
Gardez une longueur d'avance sur vos concurrents, où que vous soyez.

Autres ressources

Ressource en ligne

Nous publions tous nos résultats et pondérations Forrester Wave dans un fichier Excel qui indique des évaluations détaillées des produits et des classements personnalisables. Vous pouvez télécharger cet outil en cliquant sur le lien Forrester.com qui se trouve au début de ce rapport. Ces résultats et ces pondérations par défaut ne sont qu'un point de départ et nous incitons les lecteurs à adapter les pondérations en fonction de leurs besoins individuels.

La méthodologie Forrester Wave

Un rapport Forrester Wave est un guide destiné aux acheteurs qui étudient les options d'achat disponibles sur un marché technologique. Pour offrir un processus équitable à tous les participants, Forrester suit le guide Forrester Wave™ Methodology Guide afin d'évaluer les fournisseurs participants.

Dans le cadre de notre étude, nous menons une recherche préliminaire afin de dresser une liste de fournisseurs à prendre en compte lors de l'évaluation. A partir de ce groupe initial de fournisseurs, nous élaguons cette liste en fonction des critères d'inclusion. Nous recueillons ensuite les détails du produit et de la stratégie à l'aide d'un questionnaire détaillé, de démonstrations/réunions d'information et d'enquêtes/entretiens de référence client. Nous utilisons ces données, ainsi que l'expérience et l'expertise de l'analyste sur le marché, pour évaluer les fournisseurs à l'aide d'un système d'évaluation relatif qui compare les participants les uns aux autres.

Nous incluons clairement la date de publication de Forrester Wave (trimestre et année) dans le titre de chaque rapport Forrester Wave. Nous avons évalué les fournisseurs participant à ce rapport Forrester Wave à l'aide des documents qu'ils nous avaient fournis avant le mardi 18 août 2020 et n'avons pas accepté d'informations supplémentaires après cette date. Nous encourageons les lecteurs à prendre en compte l'évolution du marché et des offres des fournisseurs au fil du temps.

Conformément à la politique relative à l'évaluation des fournisseurs (Forrester Wave™ Vendor Review Policy), Forrester demande aux fournisseurs d'examiner nos résultats avant leur publication afin de vérifier leur exactitude. Les fournisseurs qualifiés comme non participant dans le graphique Forrester Wave correspondent aux critères d'inclusion définis, mais ont souhaité ne pas participer à l'évaluation ou y ont contribué de manière partielle. Nous évaluons ces fournisseurs conformément à la politique des fournisseurs non participants ou n'ayant contribué que partiellement à l'enquête (The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor Policy). Leur classement est publié au côté de celui des fournisseurs participants.

Politique de déontologie

Nous menons toutes nos recherches, notamment les évaluations Forrester Wave conformément à notre politique de déontologie (Integrity Policy) publiée sur notre site Web.

Notes de fin

[1] Source : « RSA® Emerges as Independent Company Following Completion of Acquisition by Symphony Technology Group », communiqué de presse de RSA, 1er septembre 2020 (https://www.rsa.com/en-us/company/news/rsa--emerges-as-independent-company).

Nous travaillons avec des leaders technologiques et métier afin d'instaurer une vision, une stratégie et une mise en œuvre centrées sur le client, afin d'accélérer la croissance.

PRODUITS ET SERVICES

- Recherche et outils
- Mission des analystes
- Données et analyses
- Collaboration entre pairs
- Conseil
- Evénements
- Programmes de certification

Les recherches et les analyses de Forrester sont adaptées à votre rôle et aux initiatives stratégiques de l'entreprise.

LES RÔLES AUXQUELS NOUS RÉPONDONS

Professionnels du marketing et de la stratégie

Directeur marketing (CMO)

Marketing B2B

Marketing B2C

Expérience client

Informations client

Stratégie de eBusiness et de distribution

Professionnels de la gestion des technologies

DSI

Développement et distribution d'applications

Architecture d'entreprise

Infrastructure et opérations

- Sécurité et gestion des risques

Gestion de l'approvisionnement et des fournisseurs

Professionnels de l'industrie technologique

Relations avec les analystes

SUPPORT CLIENT

Pour plus d'informations sur les réimpressions papier ou électroniques, veuillez contacter le support client au +1 866-367-7378, au +1 617-613-5730 ou à l'adresse clientsupport@forrester.com. Nous proposons des remises sur volume et des tarifs spéciaux aux établissements d'enseignement et aux organismes à but non lucratif.