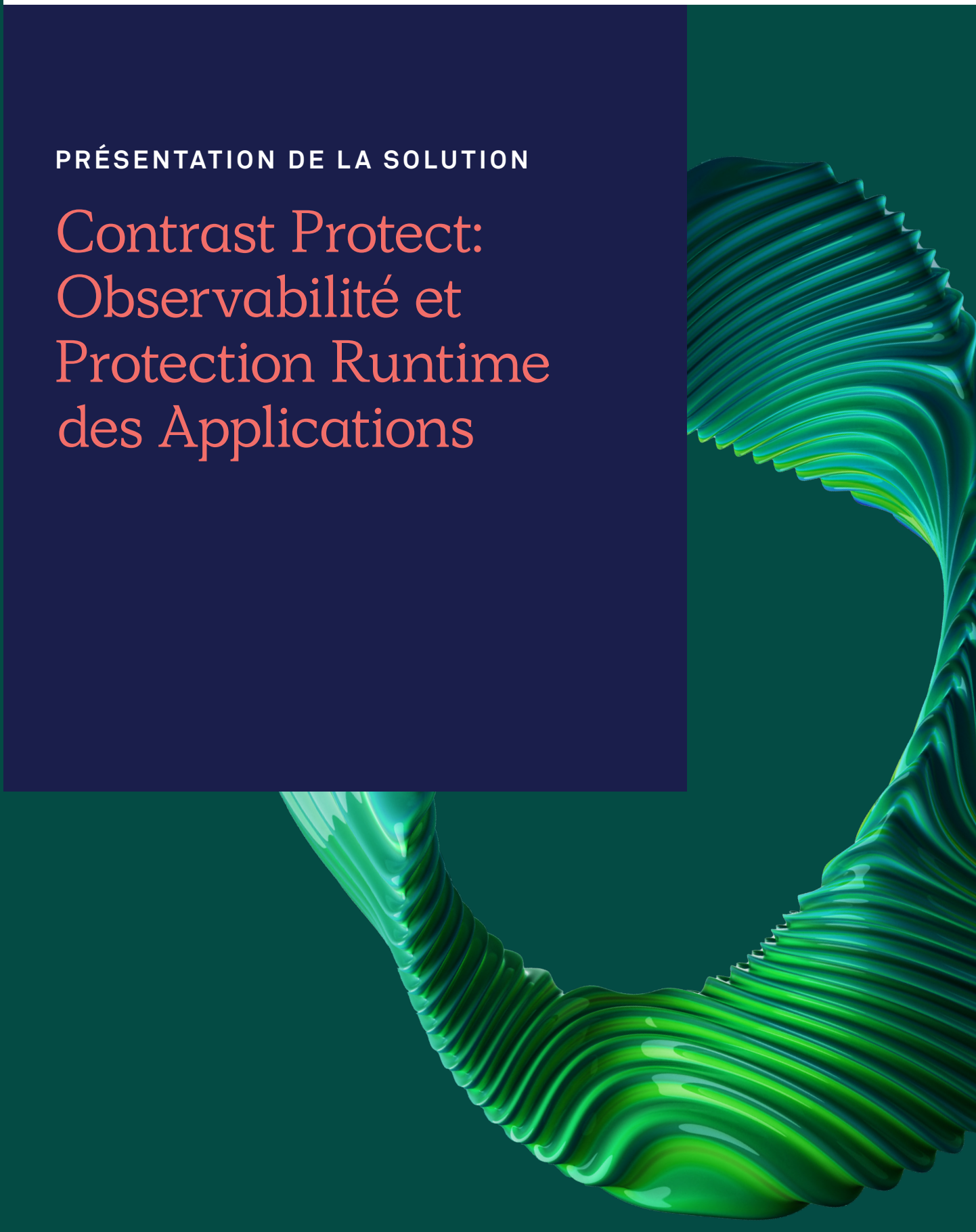
Contrast SECURITY

PRÉSENTATION DE LA SOLUTION

Contrast Protect: Observabilité et Protection Runtime des Applications



Aperçu

Les applications web et les interfaces de programmation d'applications (API) sont toujours une cible de choix pour des intrusions coûteuses et nuisibles à la réputation des entreprises. Les responsables de la sécurité éprouvent des difficultés à mettre en place des protections efficaces contre les menaces connues et inconnues en s'appuyant uniquement sur des solutions de sécurité applicative périmétriques, notamment les pare-feux d'applications web (WAF). Sans compter les coûts humains et financiers, intenables pour les entreprises.

Si les solutions périmétriques fournissent les protections nécessaires au niveau du réseau, les responsables de la sécurité ont également besoin d'une visibilité au niveau des applications pour déterminer comment les vulnérabilités sont impactées quand elles sont exposées aux menaces réelles en production. Seul ce type d'observabilité, dans le contexte de la production, permet de bloquer de manière ciblée les menaces ayant un impact sur les activités de l'entreprise et d'optimiser l'allocation des ressources DevOps pour corriger les vulnérabilités associées.

Contrast Protect est une solution d'observabilité et de protection des applications en production qui analysent les événements en temps réel pour confirmer l'exploitabilité avant de bloquer une attaque. S'appuyant à la fois sur des capteurs de précision multitechniques et sur un contrôle dynamique de l'exécution, Contrast Protect maximise la détection et la protection contre les menaces connues et inconnues, tout en éliminant pratiquement tout risque de faux positifs. Facile à déployer et fonctionnant en continu dans les applications, quel que soit leur emplacement, Contrast Protect s'aligne sur les processus DevSecOps modernes, facilitant une évolutivité rapide et rentable dans le respect de la sécurité.

Une protection efficace de l'intérieur

Contrast Protect fonctionne au moyen d'une instrumentation logicielle par le biais d'agents, qui introduisent des éléments d'observabilité et de contrôle dans le code binaire (runtime). Ces agents se déploient facilement, en quelques minutes, à partir du tableau de bord web de Contrast, sans que les ressources chargées de la sécurité ou du développement n'aient à modifier le code source.

> ***En vingt ans, le nombre moyen de vulnérabilités de sécurité par application n'a pas changé – 26,7 problèmes graves à chaque version.[1] En 2020, 43 % des violations de données étaient des attaques sur des vulnérabilités applicatives[2], soit plus du double que l'année précédente.[3]***

Contrast SECURITY

Une fois déployé, Contrast Protect assure une protection continue par le biais de sa solution Runtime Exploit Prevention™. Cette approche unique en son genre et multi-étapes analyse les événements d'exécution et confirme l'exploitabilité, améliorant ainsi la probabilité de contrer des attaques zero-day en détectant et en bloquant automatiquement les tentatives d'infraction pendant l'exécution du code en temps réel au sein de l'application. Et tout cela enmoins d'une milliseconde, même pour les attaques les plus violentes.

> *Même en cas d'attaque extrêmement massive, Contrast Protect assure une protection en moins d'une milliseconde. Ou quand sécurité rime avec rapidité.*

Contrast Protect détecte les principales menaces identifiées par l'Open Web Application Security Project (OWASP) ainsi que toutes les autres classes d'attaques courantes. Contrast Protect assure également une observabilité de toute la pile applicative, dont le code binaire, les bibliothèques et les classes personnalisées et open source, ainsi que les API. Grâce à cette visibilité plus profonde, Contrast Protect détecte et bloque les attaques qui échappent souvent aux défenses périmétriques. Par son intégration aux systèmes de gestion des événements et des informations de sécurité (SIEM), Contrast Protect améliore également la précision des analyses de sécurité.

MOINS DE FAUX POSITIFS, MOINS DE BAISSES DE VIGILANCE

Contrast Protect protège efficacement et avec discernement, faisant la distinction entre les attaques réelles et pouvant aboutir et les tentatives d'attaques non nuisibles qui n'atteignent pas une vulnérabilité ciblée. Par exemple, si une attaque par injection SQL modifie la syntaxe attendue d'une requête SQL, Contrast Protect bloque instantanément cet événement d'exécution exploitable sans impact sur l'application, et envoie une alerte au SIEM. À l'inverse, si une attaque par injection SQL n'atteint jamais une requête SQL, Contrast Protect reconnaît qu'il s'agit d'une tentative inoffensive et ne la bloque pas, ce qui élimine les faux positifs dans le SIEM.

> *La baisse de vigilance est l'ennemi de la rétention des talents SecOps. Les effectifs de cybersécurité (y compris de la sécurité des applications) doivent augmenter de 89 % au niveau mondial pour répondre à la demande actuelle de talents qualifiés.*[5]

Puisque les tentatives inoffensives constituent la majorité des attaques visant les applications[4], Contrast Protect peut éviter aux équipes de sécurité et de développement d'avoir à réparer des heures durant des vulnérabilités insignifiantes et de perturber le fonctionnement de l'entreprise par une mise à l'arrêt des applications.

Contrast SECURITY

Par ailleurs, la diminution du nombre de faux positifs réduit sensiblement la perte d'attention des équipes, inquiétude majeure des responsables SecOps. Car en plus des risques d'erreur dus à l'épuisement, la baisse de vigilance entraîne également un surmenage et une rotation élevée dans un secteur qui se caractérise déjà par une pénurie chronique de compétences.

UN DÉPLOIEMENT SIMPLIFIÉ NÉCESSITANT PEU DE PERSONNEL

Les équipes de sécurité qui travaillent avec des WAF et d'autres outils périmétriques sont habituées à déployer des dispositifs matériels ou logiciels, et à modifier la configuration du réseau pour faire transiter les données par le WAF. Les règles périmétriques statiques doivent être ajustées régulièrement en fonction du flux. Ces opérations de configuration, de réglage, de gestion, de maintenance et de dépannage dans les services SecOps, DevOps et réseau coûtent du temps et de l'argent. Une enquête révèle par exemple que 30 % des professionnels de la sécurité estiment qu'il est difficile de modifier les politiques WAF pour se prémunir contre les nouvelles attaques d'applications web.[6]

Contrast Protect présente l'avantage de se déployer durant l'exécution d'une application, et connaît toutes les informations contextuelles de sa configuration et de son déroulement. À peine activée, cette solution peut donc jouer immédiatement son rôle de blocage, au prix d'un effort de déploiement minimal.

Avec Contrast Protect, la sécurité fait partie intégrante du processus classique de déploiement des applications, sans étapes supplémentaires ni interruption des activités. Contrast Protect fonctionne partout où l'application s'exécute – dans le centre de données ou sur le cloud, sur des serveurs physiques, des machines virtuelles ou des conteneurs. Cette simplicité intégrée et continue réduit considérablement les processus et coûts d'installation – ce qui permet aux équipes de développement d'intervenir plus rapidement et de réparer sans compromettre la sécurité.

INTÉGRATION DE LA SÉCURITÉ DES APPLICATIONS SUR L'ENSEMBLE DU PORTEFEUILLE

Étant intégré au code d'exécution, Contrast Protect l'accompagne lors des mises à jour de version, des portages vers d'autres systèmes d'exploitation, des migrations de et vers des environnements clouds, et autres changements.

Par exemple, si une application crée des copies d'elle-même sur de multiples instances de serveur pour servirune base d'utilisateurs distribuée, Contrast Protect s'adaptera en parallèle et en toute fluidité – sans configuration ni réglage, quel que soit le lieu de déploiement. De plus, si on l'installe sur des serveurs virtuels ou en cloud, Contrast Protect peut tirer parti de ces ressources CPU et mémoire supplémentaires, en parallèle de l'application.

> *Quel que soit le niveau de sécurité de votre code, vous pouvez compter sur Contrast. Contrast Protect supporte Java, .NET, Python, Ruby, Node, NGINX et Golang.*

Contrast SECURITY

CONFORMITÉ AUX NORMES RECONNUES

En se conformant aux dernières normes et réglementations en vigueur, les entreprises s'adaptent à l'évolution incessante du paysage des cybermenaces, et appliquent les meilleures pratiques en termes de sécurité et d'infrastructure réseau, notamment en protégeant leurs applications.

Solution de protection et d'observabilité en cours d'exécution basée sur l'instrumentation, Contrast Protect aide les entreprises à se conformer aux normes générales propres à chaque secteur d'activité, comme celles de l'Institut national des normes et de la technologie (NIST) et de l'industrie des cartes de paiement (PCI DSS). Les dernières versions de ces normes exigent une instrumentation de sécurité de pointe pour assurer l'autoprotection des applications en production, afin de réduire les vulnérabilités des logiciels en surveillant les entrées et en bloquant celles propices aux attaques.[7]

Contrast protège là où les applications en ont le plus besoin

En complément des WAF et des autres défenses périmétriques traditionnelles, Contrast Protect et son instrumentation de protection et d'observabilité des applications en cours d'exécution garantissent visibilité, précision, facilité de déploiement et évolutivité instantanée. Contrast Protect aide les entreprises à protéger leurs applications contre les attaques internes et externes en temps réel et élimine les faux positifs qui font perdre leur temps aux analystes sécurité, en plus de garantir la conformité aux nouvelles normes garantes d'une protection efficace et moderne.

> ***Les publications SP 800-53B du NIST contiennent une norme de sauvegarde SI-7 (17), nécessitant une autoprotection de pointe des applications lors de l'exécution.[8]***

Contrast SECURITY

[1] "Malware and ransomware attack volume down due to more targeted attacks," Help Net Security, 5 février 2020.
[2] "2020 Data Breach Investigations Report," Verizon, mai 2020.
[3] "2019 Data Breach Investigations Report," Verizon, avril 2019.
[4] "Contrast Labs Application Security Intelligence Report: January-February 2020," Contrast Security, mars 2020.
[5] "Cybersecurity Professionals Stand Up to a Pandemic: (ISC)2 Cybersecurity Workforce Study 2020," (ISC)2, 2020.
[6] "International Cyber Benchmarks Index, May 2020 Survey Results," Neustar International Security Council, mai 2020.
[7] "AppSec Solution Guide for Complying with New NIST SP 800-53 IAST and RASP Requirements," Contrast Security, mars 2020.
[8] "Control Baselines for Information Systems and Organizations," NIST, octobre 2020.

Contrast Security est leader du marché de sécurité des applications grâce à une approche moderne qui intègre l'analyse du code et la prévention des attaques au cœur même des applications. Sa technologie d'instrumentation brevetée Deep Security bouscule totalement les approches traditionnelles par son observabilité intégrée et complète en fournissant une évaluation très précise et en assurant une protection continue du portefeuille d'applications tout entier. Ainsi, plus besoin de disposer d'infrastructures gourmandes en performances et d'experts spécialisés en sécurité. La plateforme de sécurité des applications Contrast accélère les cycles de développement, augmente l'efficacité et réduit les coûts, et permet un déploiement rapide tout en protégeant les applications contre les menaces connues et inconnues.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast SECURITY

contrastsecurity.com