Aperçu de la sécurité des informations d'Elastic Cloud

Octobre 2023

elastic.co/fr

TABLE DES MATIÈRES

Services et portée

Avec des solutions pour la recherche, l'observabilité et la sécurité, nous aidons les internautes à trouver plus rapidement ce dont ils ont besoin, nous assurons le bon fonctionnement des applications essentielles et nous les protégeons des cybermenaces. Elastic Cloud est conçu pour vous donner la flexibilité nécessaire pour adapter et gérer les déploiements pour votre cas d'utilisation spécifique, en supprimant la complexité et en gérant la plateforme sous-jacente qui alimente vos expériences de recherche rapidement, à l'échelle et de façon pertinente.

Nous comprenons la responsabilité considérable que nous avons envers vous, nos clients, qui comptez sur nous pour offrir des expériences de recherche de pointe tout en protégeant vos données ; nous travaillons assidûment à gagner votre confiance. La sécurité est essentielle dans tout ce que nous faisons, qu'il s'agisse de la supervision du conseil et de la gouvernance exécutive au sommet de l'organisation ou de la façon dont nous intégrons et formons continuellement chaque Elasticien. Elastic a obtenu un ensemble complet et de pointe de rapports et certifications de conformité pour le service Elastic Cloud et notre système de gestion de la sécurité des informations (ISMS –Information Security Management System). Ces rapports de certification sont la preuve que des pratiques de sécurité efficaces sont inhérentes à toutes nos activités, y compris le développement et le déploiement de produits, la gestion des vulnérabilités, la gestion des incidents et les processus de gestion des menaces.

Ce document souligne les politiques, procédures et contrôles techniques que nous avons mis en place pour vous fournir la confiance que vous méritez pour alimenter vos solutions avec Elastic Cloud. Elastic Cloud et ses solutions logicielles associées peuvent être déployés sur site, dans des clouds privés ou publics, ou dans des environnements hybrides pour répondre aux divers besoins des utilisateurs et des clients ; cependant, les contrôles pour les déploiements autogérés dépassent le cadre de ce document.

Aperçu d'Elastic Cloud

Elastic propose des solutions cloud-native pour la recherche, l'observabilité et la sécurité, afin d'améliorer l'expérience des clients et des employés, d'assurer le bon fonctionnement des applications fondamentales et de les protéger des cybermenaces. Les produits Elastic ingèrent et stockent des données provenant de tous types de sources, quel que soit leur format, pour réaliser des recherches, des analyses et des visualisations.

Elastic Cloud est une famille de produits software-as-a-service (SaaS) qui comprend l'Elasticsearch Service (ESS), Enterprise Search, Observability et Elastic Security. Elastic héberge et gère les composants de la suite Elastic, y compris Elasticsearch et Kibana, sur une infrastructure sélectionnée par le client à partir de plusieurs fournisseurs de cloud public, dont Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure et IBM. Les offres Elastic Cloud comprennent des fonctionnalités avancées de la suite Elastic, comme la sécurité, l'alerting, le monitoring, le reporting, le machine learning et la visualisation.

Vous trouverez davantage d'informations sur les composants d'Elastic Cloud ci-dessous.

Composant d'Elastic Cloud	**Description du composant**
Elasticsearch Service (ESS)	ESS est un moteur de recherche et d'analyse distribué en temps réel ainsi qu'un datastore pour tous les types de données (textuelles, numériques, géospatiales, structurées et non structurées).
Enterprise Search	Elastic Enterprise Search fournit des outils puissants pour délivrer rapidement des expériences de recherche tout en scalant facilement : *Workplace Search* est un outil destiné à unifier les plateformes de contenu d'une organisation(Google Drive, Slack, Salesforce, et bien d'autres) en proposant une expérience de recherche naturelle et personnalisée. *App Search* est une boîte à outils destinée aux développeurs, pour qu'ils puissent exploiter la puissance d'Elasticsearch pour ajouter une fonctionnalité de recherche aux applications mobiles et SaaS, grâce à un produit ultracomplet qui intègre un robot d'indexation, un ensemble d'API avancées, des tableaux de bord intuitifs et des commandes de réglage de la pertinence. *Site Search* permet l'ajout de puissantes fonctionnalités de recherche à un site Web, y compris la zone de recherche si nécessaire.

Observability	Elastic Observability permet une analyse unifiée des informations concernant les logs, les indicateurs, les performances de l'application et le monitoring de la disponibilité. En utilisant Elastic Agent et des connecteurs d'intégration prédéfinis pour la collecte de données, les organisations peuvent faire apparaître les anomalies concernant le machine learning et les règles de détection prêtes à l'emploi dont se servent aussi bien les équipes DevOps que SecOps.
Security	Elastic Security permet la prévention, la détection et la réponse aux menaces, le tout regroupé dans une seule et même interface utilisateur : *Elastic SIEM* fournit une agrégation et une corrélation conventionnelles des logs, qui aident à détecter et à répondre aux menaces, ainsi que des fonctionnalités de sécurité avancée comme l'évaluation des risques avec le machine learning, la gestion intégrée des incidents et le SOAR. *Elastic Agent* offre une polyvalence illimitée avec une empreinte minime, qui fonctionne à peu près n'importe où, y compris dans les environnements hybrides. Il peut empêcher les menaces, transférer des données et être compatible avec plusieurs cas d'utilisation pour enrichir les informations concernant la sécurité ainsi que la protection. *Limitless XDR* modernise les opérations de sécurité en unifiant les capacités de SIEM et de sécurité des points de terminaison, en permettant d'analyser des années de données, en automatisant les processus de détection et de réponse et en appliquant une protection native aux points de terminaison pour chaque hôte.

Programmes de conformité Cloud

La sécurité est intrinsèque à Elastic Cloud. Nous avons obtenu et maintenons des certifications et rapports d'attestation de pointe qui démontrent notre engagement envers la sécurité, la conformité, la confidentialité et la fiabilité.

L'ISMS mondial d'Elastic a obtenu la certification ISO 27001, et le service commercial d'Elastic Cloud a été audité et a obtenu les certifications ISO 27017, ISO 27018, SOC 2 Type 2, Cloud Compliance Matrix (CCM) de la CSA, HIPAA et PCI-DSS. Nous mettons également à disposition des synthèses de tests de pénétration ainsi que des certifications spécifiques aux secteurs d'activité et aux emplacements géographiques. Pour en savoir plus sur les normes de conformité utilisées pour nos évaluations et sur la manière d'obtenir des copies de nos rapports et certifications, consultez la section Normes de conformité de ce document.

Elastic Cloud a également obtenu une certification FedRAMP avec niveau d'impact modéré sur AWS GovCloud. Rendez-vous sur notre page consacrée à l'offre Cloud avec certification FedRAMP pour examiner les détails de la certification. Les clients et prospects fédéraux concernés peuvent bénéficier d'un accès à nos Packs Security FedRAMP via le Marketplace FedRAMP, à l'aide du formulaire de demande d'accès au pack FedRAMP.

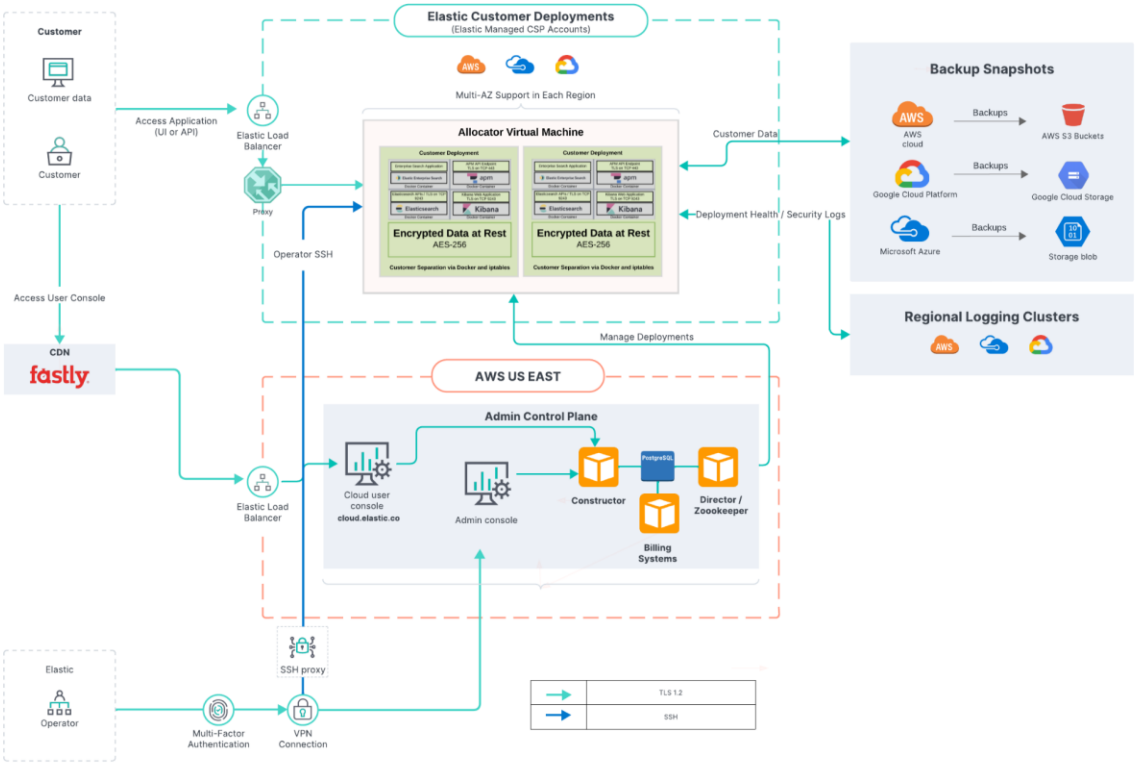
Données d'utilisation du produit et Contenu client

Nous traitons les informations de nos clients avec le plus grand soin : les protections décrites dans ce document sont en place pour protéger le Contenu client. La distinction faite entre Données d'utilisation du produit et Contenu client est expliquée ci-dessous.

Données d'utilisation du produit : il s'agit des données utilisées par Elastic pour faciliter la livraison de nos produits, gérer et monitorer l'infrastructure, fournir un support technique, et analyser et améliorer le produit. Les données d'utilisation du produit sont strictement contrôlées et protégées, et sont sujettes à des évaluations aussi bien internes qu'externes, qui en testent la sécurité et l'intégrité. Cependant, ce document se concentre sur la façon dont nous déployons une défense en profondeur pour protéger le Contenu client.

Contenu client : il s'agit des données que les clients ingèrent, importent ou envoient dans les produits et services d'Elastic. Elastic ne traite ces données qu'en fonction de ce qui est nécessaire pour fournir les produits et services, et de sorte à se conformer à la loi. Le client bénéficie toujours d'un contrôle total sur les données qu'il ingère dans Elastic Cloud.

Diagramme Elastic Cloud



Description de l'architecture d'Elastic Cloud

Plan de commande

Le Plan de commande d'Elastic Cloud comprend les services de gestion **ZooKeeper**, **Director** et **Constructor**, expliqués plus loin :

- **ZooKeeper :** ZooKeeper est un datastore distribué qui contient les informations essentielles concernant les composants d'Elastic Cloud : les tables de routage de proxy, la capacité de mémoire annoncée par les allocators, les modifications engagées via la Console d'administration, etc. Il fait office de bus de messagerie pour communiquer entre les services. Il stocke également l'état de l'installation d'Elastic Cloud et l'état de tous les déploiements exécutés dans Elastic Cloud.

- **Director :** Director gère le datastore ZooKeeper et signe les Demandes de signature de certificat (Certificate Signing Requests – CSR) pour les clients internes qui souhaitent communiquer avec ZooKeeper. Il assure également la maintenance de STunnels que ZooKeeper utilise pour la communication et établit un quorum lorsque de nouveaux nœuds ZooKeeper sont créés.

- **Constructor :** Constructor fonctionne comme un planificateur qui monitore les requêtes de la console d'administration. Il détermine ce qui doit être changé et rédige les modifications apportées aux nœuds ZooKeeper monitorés par les allocators. Il attribue également des nœuds de cluster à des allocators et optimise l'utilisation d'allocators sous-jacents pour réduire la nécessité de lancer du matériel supplémentaire pour de nouveaux déploiements. Le Constructor place des nœuds et des instances de cluster au sens de différentes zones de disponibilité pour garantir que le déploiement peut supporter n'importe quelle défaillance de zone.

  Ces préférences de placement sont personnalisables en fonction des exigences de souveraineté des données.

- **Interface utilisateur Cloud et API :** ces fonctionnalités fournissent un accès Web et API aux administrateurs, qui leur permettent de gérer et de monitorer leur installation.

Proxys

Les proxys gèrent les demandes des utilisateurs, les identifiants de déploiement de mapping transmis dans les URL de demandes pour le conteneur vers les véritables nœuds de cluster Elasticsearch et les autres instances. L'association d'identifiants de déploiement à un conteneur est stockée dans ZooKeeper, mis en cache par les proxys. En cas d'indisponibilité de ZooKeeper, la plateforme peut toujours fournir les demandes aux déploiements existants à l'aide du cache.

Ils aident également à suivre l'état et la disponibilité des zones si vous possédez un cluster Elasticsearch hautement disponible. Si l'une des zones tombe en panne, le proxy n'y acheminera aucune requête. Ils aident également avec les montées en charge et les mises à niveau sans indisponibilité. Avant d'effectuer une mise à niveau, un instantané est pris et les données sont migrées vers les nouveaux nœuds. Une fois la migration terminée, un proxy fait passer le trafic vers les nouveaux nœuds et déconnecte les anciens nœuds. Plusieurs proxys sont généralement configurés derrière un équilibreur de charge pour garantir que le système reste disponible.

Allocators

Les allocators s'exécutent sur toutes les machines qui hébergent des nœuds Elasticsearch et des instances Kibana. Ils contrôlent le cycle de vie des nœuds de cluster par l'intermédiaire de :

- la création de nouveaux conteneurs et le démarrage de nœuds Elasticsearch lorsque c'est nécessaire ;
- le redémarrage d'un nœud s'il ne répond plus ;
- la suppression d'un nœud s'il n'est plus nécessaire.

Ils annoncent également la capacité de mémoire de la machine sous-jacente ZooKeeper, afin que le Constructor puisse prendre une décision éclairée sur l'endroit du déploiement.

Gestion des risques

Elastic a adopté une approche de la sécurité et de la conformité basée sur les risques, qui utilise FAIR, la meilleure méthodologie d'analyse et d'évaluation des risques quantitatifs, pour identifier et évaluer les risques pour votre entreprise, ainsi que pour hiérarchiser les activités de réduction des risques.

Le processus d'évaluation des risques d'Elastic identifie et gère les risques qui pourraient affecter notre capacité à fournir des services fiables à nos clients. Les risques clés que nous avons identifiés, et que nous faisons en sorte de contrôler, comprennent :

- La gestion organisationnelle
- La sécurité des ressources humaines
- La gestion des actifs
- Le contrôle des accès
- La cryptographie
- Les communications sécurisées
- L'acquisition, le développement et la maintenance du système
- Les relations avec les fournisseurs
- Le système de gestion de la sécurité des informations
- La gestion de la continuité des activités

Le processus d'identification des risques prend en compte les facteurs aussi bien internes qu'externes et leur impact sur la réalisation des objectifs.

Les risques identifiés sont analysés au travers d'un processus incluant une analyse des menaces et vulnérabilités possibles par rapport aux objectifs commerciaux et l'estimation d'une importance potentielle du risque.
Le processus d'évaluation des risques prend en compte la façon dont est géré le risque et s'il faut l'accepter, l'éviter, le réduire ou le transférer. Nous déterminons les stratégies d'atténuation pour les risques ayant été identifiés. Les stratégies peuvent comprendre la conception, le développement et la mise en œuvre de contrôle, ainsi que l'adoption et la révision des politiques et procédures.

Le processus collectif d'identification, d'analyse et d'évaluation des risques renseigne notre Inventaire des risques, c'est-à-dire les scénarios de risques évalués à l'aide de la méthodologie FAIR et classés sur la base de l'impact financier estimé sur Elastic. L'inventaire des risques est réévalué sur une base semestrielle pour tenir compte des modifications apportées aux facteurs de risque internes et externes, aux priorités commerciales et à l'évolution des stratégies d'atténuation. Ce processus pilote également l'approche basée sur les risques dans les rapports qu'envoie l'équipe de sécurité au Comité d'audit du Conseil d'administration.

Gouvernance

"Information Security Management System" (ISMS) et supervision

Elastic a mis en œuvre un ISMS qui comprend des politiques, procédures, structures opérationnelles et contrôles techniques qui œuvrent de concert à sauvegarder les données des clients et de l'entreprise. L'ISMS a obtenu la certification ISO 27001 et est organisée de sorte à répondre totalement à tous les domaines de sécurité et de conformité, y compris la Gouvernance, la Confiance, la Gestion des risques et des vulnérabilités, l'Architecture et ingénierie de la sécurité, la Sécurité des produits, la Détection des menaces et la Réponse aux incidents.

Le Conseil d'administration (Comité d'audit) d'Elastic supervise l'ISMS et rencontre régulièrement le Directeur de la sécurité des systèmes d'information (Chief Information Security Officer – CISO) pour garantir que le programme de sécurité des informations s'aligne sur les buts et objectifs de l'entreprise, adopte les bonnes pratiques du secteur et évolue en parallèle du paysage de menaces dynamique.

L'ISMS d'Elastic est renforcé par une équipe Intégrité et confidentialité professionnelle dédiée, qui collabore étroitement avec l'équipe de sécurité des informations sur des solutions organisationnelles qui garantissent la conformité aux lois et réglementations mondiales sur les données.

Politiques de sécurité des informations

Elastic a développé un ensemble de politiques complet destiné à gouverner nos pratiques de sécurité des informations, basé sur des normes du secteur, y compris les normes NIST et ISO 27001, et à communiquer les attentes en termes de gestion à l'ensemble de l'entreprise. Tous les ans, les détenteurs de la politique examinent toutes les politiques de sécurité des informations et la direction les approuve. Les politiques d'Elastic abordent les domaines suivants :

- Programme de sécurité des informations
- Utilisation acceptable
- Gestion des risques
- Gestion des actifs
- Classification des données

- Conservation des enregistrements
- Contrôle des accès
- Sécurité des postes de travail et des serveurs
- Analyse de la sécurité et logging
- Gestion des vulnérabilités
- Gestion des modifications
- Développement logiciel sûr
- Réponse aux incidents
- Continuité des activités et reprise d'activité après sinistre

Les employés d'Elastic doivent attester avoir examiné et accepté le Code de conduite d'Elastic ainsi que les politiques de sécurité des informations, de confidentialité et d'utilisation acceptable lors de leur embauche, puis tous les ans par la suite.

Nous ne partageons pas le texte intégral de nos politiques de sécurité des informations en externe. Cependant, un fichier groupé des politiques de sécurité des informations est disponible, qui inclut la Table des matières de chaque politique ainsi que l'historique de ses versions, pour clarifier les domaines couverts dans chaque politique et fournir une preuve de l'examen, mise à jour et approbation réguliers de chaque politique. Pour obtenir un exemplaire de ce document, veuillez contacter votre représentant de compte Elastic ou le support technique Elastic.

En plus des politiques officielles, Elastic conserve des playbooks, des documents de processus et des plans pour les domaines ayant des exigences de processus plus spécifiques ou des bonnes pratiques en constante évolution, comme le chiffrement de clouds, la gestion de certificats et de clés, et la gestion de risques tiers.

Gestion des ressources humaines

Nous reconnaissons qu'un programme de sécurité complet commence par le fait que la direction y accorde une forte importance, et implique chaque employé d'Elastic. Notre Code source, notre Manuel de l'employé et notre Code de conduite comprennent des conseils et des normes éthiques explicites que tout le personnel d'Elastic se doit de respecter. Elastic applique une politique de tolérance zéro pour quiconque enfreindrait ces engagements, quels que soient son poste, son ancienneté ou sa fonction.

Elastic a également établi des bonnes pratiques de sécurité au niveau de l'entité avec des modalités de rapport officielles, qui facilitent le flux d'informations vers le personnel concerné et garantit une bonne prise de responsabilité et supervision de la conduite et des performances des employés. Les rôles et responsabilités sont séparés sur la base d'exigences fonctionnelles et les rôles sont définis de façon explicite.

Toutes les embauches et ruptures de contrat se déroulent conformément aux politiques et procédures documentées, ce qui inclut les procédures visant à intégrer et à mettre fin au contrat des employés et prestataires rapidement et en toute sécurité.

Les autres pratiques de sécurité au niveau de l'entité comprennent la vérification des antécédents des nouvelles recrues et prestataires avant leur intégration. De plus, tous les employés d'Elastic, y compris les cadres et la direction, doivent suivre une formation de sensibilisation à la sécurité, ainsi qu'examiner et prendre connaissance des politiques de confidentialité et de sécurité des informations, du Code de conduite et du Manuel de l'employé lors de l'embauche, puis tous les ans par la suite.

Gestion des actifs

La Norme concernant la Gestion des actifs gouverne le cycle de vie de la gestion des actifs, ce qui inclut l'inventaire des actifs, la propriété des actifs, le retour et la suppression des actifs et les exigences des pistes d'audit. Les processus de gestion des actifs entre la gestion de la flotte et la gestion des points de terminaison sont distincts. Chaque processus indépendant est expliqué ci-dessous :

Flotte

Nos partenaires Cloud Service Providers (CSP), AWS, GCP, Azure et IBM gèrent l'infrastructure qui alimente Elastic Cloud. Les clients Elastic Cloud ont la flexibilité de choisir le CSP et la région géographique sous-jacents pour leurs données sur une base par déploiement. Les contrôles de sécurité physique, des médias et du matériel relèvent de la responsabilité du CSP. Elastic examine la conception et l'efficacité opérationnelle des contrôles de gestion du cycle de vie des médias et du matériel de nos fournisseurs de service cloud partenaires lors des recertifications tierces conduites dans le cadre de notre programme de gestion des risques tiers.

Les clusters Elastic utilisent Elastic Observability pour suivre les performances et les indicateurs de disponibilité. Les actifs sensibles sont enregistrés dans notre inventaire des actifs, et l'inventaire des actifs est régulièrement examiné pour vérifier son exhaustivité et sa précision.

Points de terminaison des employés

Le service informatique d'Elastic centralise le suivi et la gestion des points de terminaison des employés. Un logiciel de gestion des appareils est utilisé pour imposer des paramètres de sécurité, notamment le chiffrement, la gestion des mots de passe, la gestion des sessions et le verrouillage des écrans, qui sont activés par défaut. Ces paramètres ne peuvent pas être désactivés ou modifiés localement. Les points de terminaison sont protégés par Elastic Security, qui fournit des fonctionnalités EDR ainsi qu'un monitoring et un alerting en temps réel. Consultez la section concernant la sécurité vis-à-vis des malwares pour en savoir plus sur la façon dont nous protégeons les points de terminaison des employés des malwares.

Tous les appareils fournis par Elastic sont gérés conformément à notre cycle de vie de gestion des appareils. Lorsque le contrat d'un employé d'Elastic est résilié, l'accès logique est désactivé et les points de terminaison gérés par l'entreprise sont envoyés directement à un processeur tiers qui réalise les procédures d'assainissement et de destruction des données. Notre partenaire tiers fournit à Elastic des certificats de destruction et ré-émet ou supprime la machine sur la base de la norme d'Elastic concernant la gestion des ordinateurs portables. Le service informatique d'Elastic assure la maintenance d'une piste d'audit des points de terminaison gérés par Elastic pour suivre le statut de chaque appareil au sein du cycle de vie de destruction des données.

La politique empêche les appareils mobiles non gérés ou personnels de stocker des données clients ou d'être utilisés pour le développement ou le support technique d'Elastic Cloud.

Gestion de la configuration

Elastic gère la configuration par code, et les modifications de configuration suivent la procédure de gestion des modifications standard qui comprend l'autorisation, l'examen et l'approbation par des paires, et les suites de tests automatisés. Elastic monitore les modifications directes apportées aux fichiers de configuration de production via le Monitoring de l'intégrité des fichiers et la détection d'activités suspectes.

Protection des données

Classification et conservation des données

La norme de classification des données d'Elastic nécessite que les données soient classifiées sur la base de leur sensibilité, avec des restrictions en termes d'accès et de partage définies pour chaque classification. Le Contenu client et les Données d'utilisation du produit sont classifiés comme étant restreints (la classification la plus sensible) et sont soumis aux normes de protection des données les plus strictes, conçues pour préserver la confidentialité, l'intégrité et la disponibilité de ces données. Pour accéder aux définitions du Contenu client et des Données d'utilisation du produit, consultez la section Données d'utilisation du produit et Contenu client de ce document.

La Norme de conservation des enregistrements d'Elastic nécessite que les données soient supprimées conformément au calendrier de conservation défini, sur la base des types de données et des exigences opérationnelles, contractuelles, juridiques et réglementaires. Les clients peuvent envoyer une demande de suppression de compte au support technique Elastic pour que leurs informations soient supprimées. Pour obtenir des informations sur la façon dont envoyer une demande d'accès aux données, consultez la section Confidentialité des données de ce document.

Collecte, gestion et suppression des données

Collecte de données

Elastic ne collecte que les informations nécessaires pour fournir, dépanner, entretenir, sécuriser et améliorer nos services. Ces informations ne sont jamais vendues à des tiers. Pour en savoir plus sur les informations que nous collectons auprès de nos clients, consultez notre Déclaration de confidentialité relative aux produits.

Ingestion des données

Elastic ne contrôle ni n'accède aux données que les clients choisissent de stocker, de transmettre ou de traiter dans leur déploiement d'Elastic. Toute ingestion de données dans le cadre du déploiement Elastic d'un client se fait à son entière discrétion et sous son contrôle à tout moment.

Destruction des données

La Norme de conservation des enregistrements d'Elastic et la Norme de gestion des actifs gouvernent les exigences de destruction. Nos fournisseurs de service cloud partenaires gèrent la suppression et la destruction sécurisée des données pour les infrastructures hôtes. Les clients gardent le contrôle total du contenu qu'ils stockent dans leurs instances Elastic et ont à tout moment le droit de retirer ou de supprimer tout contenu de leurs instances Elastic.

Chiffrement

Chiffrement en transit

Le chiffrement en transit pour Elastic Cloud est appliqué par défaut via le protocole Sécurité de la couche transport (TLS). Le niveau de chiffrement minimum accepté est TLS 1.2. Les connexions TLS (HTTPS) sont affichées dans le Diagramme Elastic Cloud.

Les certificats servant à prendre en charge Elastic Cloud sont fournis par Digicert et utilisent l'authentification de clés publiques RSA avec des clés de 2 048 bits. Elastic assure la maintenance de certificats valides pour nos déploiements Cloud et obtient la note de A+ décernée par Qualys SSL Labs. Ces résultats de tests peuvent être reproduits en vous rendant sur SSL Labs.

Chiffrement au repos

Nos fournisseurs de service cloud partenaires fournissent un chiffrement au repos, activé par défaut. Tous nos fournisseurs cloud comprennent des longueurs de clé minimum conformes aux consignes NIST (256 bits).

Gestion des clés

Les clés de chiffrement ne quittent jamais l'hôte dans lequel elles ont été générées et sont considérées comme jetables. Elles sont générées automatiquement dès qu'un hôte de machine virtuelle est créé ou remplacé. Elles ne sont jamais sauvegardées, exposées, ni ne quittent l'hôte. La gestion des clés pour chiffrement dans les services IaaS sous-jacents est automatisée à l'aide du service de gestion des clés du fournisseur.

La maintenance de la gestion des clés pour les services Elastic est assurée en tant qu'Infrastructure en tant que code et dans le cadre de la documentation opérationnelle pour chaque composant ou service applicable.

Gestion de la sécurité et du réseau des appareils

Pare-feu

Nos fournisseurs de service cloud partenaires gèrent les pare-feu matériels pour l'infrastructure de production. Elastic assure également la maintenance des pare-feu logiciels pour filtrer le trafic entrant non autorisé provenant d'Internet et refuser les connexions réseau entrantes qui ne sont pas explicitement autorisées (refuser par défaut). Davantage de segmentation de réseau et de pare-feu sont en place entre les zones logiques au sein de l'environnement. Les ensembles de règles de pare-feu sont examinés au moins deux fois par an. Les modifications apportées aux règles de pare-feu suivent le processus de gestion des modifications standard et sont soumises à des contrôles de gestion des modifications. De plus, tous les accès au pare-feu sont implémentés à l'aide du RBAC.

Les clients d'Elastic Cloud peuvent utiliser la fonctionnalité de filtrage du trafic ou configurer PrivateLink pour restreindre davantage le trafic vers leurs déploiements.
Filtres de trafic IP | Documentation d'Elasticsearch Service | Elastic
Filtres de trafic AWS PrivateLink | Documentation d'Elasticsearch Service | Elastic

Sécurité vis-à-vis des malwares

La protection contre les malwares est activée sur tous les points de terminaison des employés via des configurations informatiques gérées de façon centrale. Les administrateurs locaux ne peuvent désactiver ni modifier ces paramètres. La solution Elastic Security fournit des fonctionnalités EDR ainsi qu'une équipe d'astreinte 24 h/24 et 7 j/7 dans le cadre d'alertes d'examens et d'actions de sécurité des informations.

Elastic Security est utilisé pour protéger l'environnement de production d'Elastic Cloud. Les signatures et les modèles de comportement sont mis à jour automatiquement et continuellement. Des détections peuvent être rapidement déployées par rapport aux menaces émergentes et une équipe Threat Intelligence, Détections et Réponse dédiée gère la détection, l'analyse, la réponse est la résolution des possibles infections par malware.

Synchronisation temporelle

La synchronisation temporelle est réalisée via NTP avec une source temporelle commune (serveurs NIST).

Accès logique

Contrôle d'accès basé sur les rôles

Elastic adhère au principe du moindre privilège lorsqu'il s'agit de fournir un accès aux utilisateurs internes. Les employés d'Elastic ne se voient accorder que le niveau d'accès nécessaire à leur rôle. Les droits d'accès sont régulièrement examinés et modifiés en cas de changement d'emploi ou autres circonstances dans lesquelles l'accès d'un utilisateur n'est plus nécessaire.

Les produits Elastic comprennent également un contrôle d'accès basé sur les rôles pour permettre à nos clients de mettre en œuvre une gestion d'accès granulaire pour les utilisateurs au sein de leurs déploiements d'Elastic et de la plateforme de gestion d'Elastic Cloud.

Intégration et fin de contrat

Les nouvelles recrues se voient automatiquement accorder l'accès aux applications SaaS cloud-native professionnelles sur la base de règles pré-configurées dans notre système de Gestion des identités et des accès (IAM) centralisé. Les ensembles de règles de provisionnement automatique utilisent les attributs de fonction de notre système d'enregistrement RH, comme l'organisation de surveillance, la famille de fonctions, le niveau de fonction et la structure de gestion pour accorder un accès spécifique nécessaire à cet utilisateur individuel. Tout accès supplémentaire nécessite une demande officielle documentée dans un ticket, et est soumis à l'examen et à l'approbation de la direction.

Si un employé est muté vers un autre rôle ou une autre organisation au sein d'Elastic, les changements dans les attributs de son rôle au sein du système d'enregistrement RH initieront automatiquement le workflow au sein du système IAM centralisé pour redonner à son compte l'accès approprié à son nouveau rôle. Les droits d'accès de son rôle précédent sont désactivés et un nouvel accès est accordé sur la base des attributs de fonction de son nouveau rôle.

À la fin du contrat, l'accès accordé via notre système IAM centralisé est automatiquement suspendu lorsque sa situation professionnelle est modifiée dans notre système de gestion RH. Le contrôle de validation se déroule plusieurs fois par jour.

Accès à la production

Un nombre limité d'employés d'Elastic se sont vu accorder un accès privilégié à notre environnement de production Elastic Cloud. Elastic conserve cet accès à des fins de gestion, de maintenance et de support de la plateforme. La politique de gestion des données d'Elastic interdit expressément aux employés d'Elastic d'accéder à des données clients, même dans des scénarios de maintenance ou de dépannage. Les clients doivent fournir leur consentement écrit préalable à un employé d'Elastic consultant des données qu'il a volontairement partagées à des fins de support ou de dépannage. Elastic ne consulte pas de façon proactive de données clients chargées ou ingérées dans Elastic Cloud. Les clients peuvent choisir de corriger ou de nettoyer des données avant de les partager avec Elastic.

De plus, l'équipe Sécurité des informations et Détection et réponses aux menaces a développé et mis en œuvre des détections d'activité de compte interne suspectes et d'accès non autorisé, y compris le monitoring de l'intégrité de fichiers et des indicateurs d'usurpation de compte ou d'exfiltration de données. Ces détections font partie des workflows automatiques qui alertent l'équipe de Détection et réponse aux menaces d'une activité suspecte et déclenchent une enquête de l'analyste.

Examens de l'accès utilisateur

Elastic adhère au principe du moindre privilège et autorise uniquement l'accès nécessaire à la réalisation des missions de chaque rôle. Les propriétaires du système et la direction examinent et re-certifient l'accès utilisateur, y compris l'accès privilégié, lors des examens trimestriels de l'accès utilisateur. Un accès qui n'est plus nécessaire est supprimé.

Gestion des modifications

La norme de gestion des modifications gouverne les processus de gestion des modifications et établit des exigences conçues pour contrôler le développement et le déploiement des modifications apportées au logiciel et à l'infrastructure dans l'environnement de production de manière sécurisée et gérée.

Le processus de gestion des modifications garantit que les modifications proposées sont autorisées, examinées par des pairs, testées, mises en œuvre et publiées de façon contrôlée, et que le statut de chaque modification proposée est documenté et monitoré. Dans le cas où une modification d'urgence serait nécessaire, une approbation documentée et des tests automatisés seront toujours nécessaires. Un examen manuel de la modification d'urgence est également requis, mais peut se dérouler après l'implémentation.

Sécurité de la chaîne d'approvisionnement

Les déploiements logiciels vers des environnements de production sont gérés via des pipelines CI/CD automatisés. Les modifications sont stockées dans des branches désignées au sein de chaque référentiel respectif. Des branches de développement sont utilisées pour un développement actif et les branches principales contiennent du code prêt pour la production. Les modifications sont contrôlées par les versions et, avant de les fusionner avec la branche principale, une série de tests automatisés, y compris des vérifications de sécurité, est réalisée. Des protections de branche sont activées et requièrent que des suites de tests soient réalisées avant que la modification ne soit autorisée à fusionner avec la branche principale. Lorsqu'une modification est totalement autorisée (les tests et vérifications de sécurité sont concluants, l'examen et l'approbation par les pairs sont obtenus, et les contrôles d'intégration sont concluants), le logiciel de déploiement automatisé fait passer la modification en production sans avoir besoin d'intervention manuelle.

Notre code source est stocké dans un système de contrôle de version dont l'accès est contrôlé et monitoré. L'activité utilisateur est capturée dans des logs d'audit et des détections sont en place pour alerter en cas de modification inattendue ou suspecte et pour créer des processus. La possibilité de modifier du code au sein de chaque référentiel est restreinte sur la base des rôles.

Développement sécurisé

SDLC

La maintenance des exigences de sécurité pour notre Cycle de vie de développement des systèmes (Systems Development Life Cycle – SDLC) est assurée dans notre Cadre de développement logiciel sécurisé. Ce cadre dicte le processus nécessaire pour concevoir, développer, déployer, suivre et assurer la maintenance de tous les logiciels Elastic en toute sécurité. Il comprend également les exigences pour protéger nos systèmes de version et atténuer les risques de compromission de la chaîne des versions. Les systèmes de version comprennent les pipelines de livraison de logiciels, les registres de package, les référentiels d'éléments, le CIC/CD et les systèmes de gestion du code source. Le Cadre de développement logiciel sécurisé interdit l'utilisation de données de production à des fins de tests et dans des systèmes ne relevant pas de la production. Il nécessite également la séparation des environnements de production et ne relevant pas de la production. La segmentation environnementale est évaluée durant les tests de pénétration tiers.

Architecture et conception sécurisées

Le développement logiciel d'Elastic suit les bonnes pratiques de sécurité en termes de conception et d'architecture afin de produire des logiciels "sécurisés dès la conception" et "sécurisés par défaut."

Le Cadre de développement logiciel sécurisé souligne les exigences de protection des données et les principes de sécurité que toutes les conceptions doivent suivre, y compris :

- La confidentialité : les données sont protégées de l'observation et de la divulgation non autorisées aussi bien en transit que lorsqu'elles sont stockées.
- L'intégrité : les données sont protégées de la création, de l'altération ou de la suppression non autorisée.
- La disponibilité : les données sont disponibles aux utilisateurs autorisés autant que nécessaire et satisfont à n'importe quel SLA de disponibilité définie.
- L'identification, l'authentification, l'autorisation
- La non-répudiation
- L'audit et le logging
- Le contrôle d'accès et les principes du moindre privilège
- Les communications sécurisées et les normes de chiffrement
- Les paramètres de sécurité par défaut et les paramètres d'urgence

Les examens de modélisation des menaces et d'architecture de la sécurité font également partie du processus de développement logiciel, pour garantir que la conception a pris en compte les principes de sécurité requis.

Codage sécurisé

En tant que fournisseur SaaS, nous reconnaissons l'importance des pratiques de codage sécurisé. Les vulnérabilités de codage courantes comme le top 10 de l'OWASP et le top 25 du CWE sont abordées dans la Formation concernant le développement sécurisé du logiciel, disponible aux équipes et individus concernés tous les ans. Les modifications au code source nécessitent un examen et une approbation (par le biais d'une demande de fusion) provenant d'au moins un vérificateur, qui n'est pas l'auteur du changement, avant de fusionner les modifications. Les modifications sont examinées dans le but d'identifier de potentiels impacts à la sécurité que la modification pourrait introduire. De plus, des tests de pénétration indépendants, qui comprennent un examen du code sécurisé, soulignent davantage les pratiques courantes de codage non sécurisées. Tout problème identifié lors de la modélisation des menaces, de l'examen de la sécurité ou de l'examen du code source, est suivi, évalué et résolu sur la base du risque évalué, conformément à la Norme concernant la gestion des vulnérabilités.

Elastic sponsorise également un programme de récompense pour les bugs identifiés dans le cadre de ses efforts pour conserver un logiciel sécurisé et protéger ses clients des vulnérabilités. Pour en savoir plus, consultez le Programme de divulgation des vulnérabilités dans la section Gestion des vulnérabilités et des correctifs.

Open source et examen logiciel tiers

Le Cadre de développement logiciel sécurisé nécessite que les dépendances du code à l'open source et aux bibliothèques tierces soient identifiées et suivies. Un logiciel de gestion des dépendances a été mis en place pour aider à identifier, analyser et résoudre les dépendances vulnérables.

Gestion des vulnérabilités et des correctifs

La norme de gestion des vulnérabilités gouverne le programme de gestion des vulnérabilités et définit des exigences pour l'analyse des ressources Elastic ainsi que le tri, l'analyse, la résolution et la divulgation des vulnérabilités. Elastic réalise des analyses de vulnérabilité et applique des correctifs aussi bien à l'infrastructure qui alimente Elastic Cloud qu'aux composants Elastic Cloud eux-même. Les processus de chacun sont détaillés ci-dessous.

Gestion des vulnérabilités de l'infrastructure et des correctifs

Elastic utilise un outil d'analyse des vulnérabilités commerciales pour analyser ses actifs sur une base continue. Tous les actifs de production sont inclus dans ces analyses. Le fournisseur de logiciels tiers met continuellement ces ensembles de règles à jour. La sévérité des vulnérabilités est basée sur des évaluations CVSS et les calendriers d'application de correctifs correspondent également aux évaluations CVSS. Les vulnérabilités critiques et hautes passent en priorité pour l'application de correctifs, ou pour faire partie de la prochaine version planifiée.

Gestion des vulnérabilités du produit et des correctifs

Nous testons régulièrement nos produits à la recherche de vulnérabilités de sécurité via des tests de pénétration tiers, des analyses et examens automatisés et manuels, des analyses OSS, des tests de segmentation et via notre programme de divulgation des vulnérabilités. Lorsqu'une vulnérabilité est

découverte dans un produit Elastic, Elastic l'évaluera conformément à la Norme de gestion des vulnérabilités pour déterminer la sévérité et un plan de résolution. Si nécessaire, nous délivrons une alerte de sécurité Elastic (Elastic Security Advisory – ESA.) Il s'agit d'une notification d'Elastic à ses utilisateurs les informant de problèmes de sécurité avec les produits Elastic. Elastic attribue aussi bien un CVE qu'un identifiant ESA à chaque alerte, ainsi qu'un résumé et des informations concernant la résolution et l'atténuation. Toutes les nouvelles alertes sont annoncées dans le forum Annonces de sécurité.

La Norme de gestion des vulnérabilités gouverne également les divulgations de publication. Le processus de divulgation comprend la publication d'une nouvelle version d'un produit, si nécessaire, et la publication d'une annonce sur la page Alertes. En fonction de la nature de la vulnérabilité, nous contacterons également les clients individuels, publierons un article de blog, et/ou enverrons le CVE à MITRE.

Les clients peuvent suivre les ESA via un flux RSS.

Programme de divulgation des vulnérabilités

Elastic est fier de sponsoriser un programme de divulgation des vulnérabilités public grâce auquel les chercheurs en sécurité peuvent envoyer de façon responsable les vulnérabilités pour examen interne. L'équipe de sécurité produit d'Elastic examine les envois, évalue l'exposition au risque et résout sur la base du risque évalué. Veuillez consulter le programme de récompense pour les bugs identifiés d'Elastic sur HackerOne pour consulter notre politique en la matière ou pour envoyer un rapport.

Gestion des risques tiers

Intégration tierce

Tous les tiers comprenant des sous-processeurs sont soumis à un processus d'entrée et de vérification rigoureux. Le profil de risque de chaque fournisseur est évalué sur la base du service qu'il fournit, des types de données qu'il sera amené à traiter, du niveau d'accès qu'il aura aux systèmes internes et d'autres facteurs qui capturent l'état critique et le profil de risque du fournisseur.

Sur la base du profil de risque du fournisseur et des types de services qu'il fournit à Elastic, un workflow d'examen est exécuté. Tous les fournisseurs qui auront accès à des informations sensibles, à des systèmes internes, ou qui fourniront un service technologique critique nécessitent une surveillance approfondie, notamment, sans s'y limiter, un examen de la sécurité des informations, juridique et de confidentialité. Cette surveillance supplémentaire comprend l'examen des pratiques de sécurité, des certifications de sécurité et des rapports de conformité des tiers. La conformité avec les lois du pays dans lequel les données sont traitées, stockées et transmises est prise en compte, et, là où cela est jugé nécessaire, Elastic se réserve le droit de rechercher des exigences de sécurité supplémentaires dans des accords tiers.

Elastic a également publié un Code de conduite des fournisseurs, qui documente les exigences éthiques attendues des fournisseurs et des partenaires. Il comprend, sans s'y limiter, les exigences relatives à l'éthique et la conformité, la santé et la sécurité des employés, les droits humains et du travail, et la gérance environnementale.

Recertification tierce

Un processus continu de gestion des risques des informations tierces est en place pour réaliser la recertification des fournisseurs existants. Les tiers sont classés sur la base du niveau de risque et l'équipe de sécurité des informations d'Elastic examine les pratiques de sécurité des tiers conformément aux exigences en place pour chaque niveau de risque.

Tous les fournisseurs de service cloud qui fournissent des services d'infrastructure pour Elastic Cloud sont examinés et recertifiés au moins une fois par an. Le processus de recertification implique l'examen du profil de risque d'un fournisseur et l'examen des rapports de sécurité et de conformité des fournisseurs pour garantir que les contrôles de sécurité et de conformité prévus couvrent correctement les services que nous consommons, et que les contrôles sont conçus et fonctionnent efficacement.

Détection des menaces

Monitoring et Alerting

Nous utilisons Elastic Security comme solution SIEM, ce qui nous permet de développer et déployer rapidement des détections pour des menaces et des schémas d'attaque émergents, ainsi que des détections de comportements suspects, des détections de monitoring d'intégrité de fichiers et des schémas de comportement de malware courants. Nous réalisons le monitoring de nos environnements en temps réel, par le biais de nos détections automatiques. Des workflows d'alerting pré-configurés ont été mis en place pour informer le personnel Elastic approprié en cas d'indicateurs suspects. Notre équipe de Détections et réponses aux menaces, d'astreinte 24 h/24 et 7 j/7, enquête sur ces alertes et les traite.

Du personnel certifié et continuellement formé gère les événements de sécurité et les incidents conformément à notre Norme relative aux réponses aux incidents et notre plan de réponse aux incidents. Pour en savoir plus sur le processus de gestion des incidents, consulter la section Réponse aux incidents de ce document.

Gestion et conservation des logs

Nous utilisons Elasticsearch comme solution de gestion des logs. Nous sommes capables d'ingérer et de centraliser des logs provenant de plusieurs sources, notamment des moteurs de détection, nos fournisseurs d'IaaS, des outils de gestion de la vulnérabilité, la console d'administration cloud et plus encore pour développer des capacités scientifiques, de logging et d'audit. L'accès à nos logs est contrôlé pour éviter la falsification, et l'accès en édition est restreint à l'ingénierie de sécurité sur la base du moindre privilège. De plus, la détection et l'alerting automatisés, y compris le monitoring de l'intégrité des fichiers, protège le système de logging et informe l'équipe en charge de la détection des menaces et de la réponse d'activités suspectes quasiment en temps réel.

Les logs sont conservés conformément à notre Norme de conservation des données, sur la base d'exigences commerciales, juridiques et contractuelles. Les clients qui souhaitent envoyer une demande d'accès aux données peuvent consulter la section Confidentialité des données de ce document.

Réponse aux incidents

La sécurité des informations d'Elastic possède une équipe en charge de la détection des menaces et de la réponse opérant 24 /24 et 7 j/7, dédiée à la gestion d'événements et d'incident de sécurité. La norme relative aux réponses aux incidents gouverne la fonction de réponse aux incidents et dicte les exigences d'identification des événements, de gestion des événements, de création de rapports et de formation. Le plan de réponse aux incidents séparé détaille comment se préparer à, détecter, analyser, contenir, éradiquer, récupérer de et créer des rapports sur les incidents de sécurité. Les intervenants formés aux accidents, qui entraînent et testent régulièrement le plan de réponse aux incidents, gèrent tous les incidents. Les incidents nécessitent également un rapport post-actions et un exercice des leçons apprises.

Dans le cas où nous détecterions une violation ou serions mis au courant d'un accès non autorisé aux systèmes ou données, l'équipe Sécurité juridique des informations d'Elastic émettra des communications client comme requis par la loi ou conformément aux termes du contrat, et ce sans délai.

Si un incident de sécurité nécessite d'établir un rapport auprès d'une entité réglementaire du secteur ou externe, le plan de réponse aux incidents d'Elastic comprend des instructions concernant nos obligations en termes de rapports, sur la base du scénario fourni. Le plan désigne également une équipe officielle en charge de la réponse aux incidents de sécurité informatiques (Computer Security Incident Response Team – CSIRT) ayant des rôles et des responsabilités documentés, pour garantir une bonne communication entre les individus appropriés.

Fiabilité

Disponibilité et état

Une architecture de haute disponibilité est disponible et recommandée sur Elastic Cloud avec un SLA amélioré. Veuillez discuter de cette option avec l'équipe chargée de votre compte si vous pensez qu'elle pourrait vous être bénéfique. Les données historiques et en temps réel concernant les performances du service Elastic Cloud sont disponibles sur Elastic.

Continuité des activités et reprise d'activité après sinistre

Elastic assure la maintenance de plans de continuité des activités et de reprise d'activité après sinistre exhaustifs, en plus d'une norme relative à la continuité des activités et à la reprise d'activité après sinistre, pour se préparer à, répondre à et récupérer après un sinistre.

Elastic est, depuis ses origines, une entreprise distribuée au niveau mondial. Les employés sont totalement équipés pour travailler à distance et la redondance des zones géographiques est prise en compte dans le personnel attribué aux équipes distribuées. Les bureaux d'Elastic ne contiennent aucune infrastructure ni aucun système informatique nécessaire à la connectivité des employés, ou à la fourniture des services ou du support technique d'Elastic à nos clients.

Elastic assure la maintenance des plans de reprise d'activité après sinistre pour Elastic Cloud, qui sont testés au moins une fois par an. Les tests sont uniques et se concentrent chaque année sur un domaine défini, pour identifier les lacunes de connaissance et les faiblesses de nos fonctionnalités de reprise techniques. La durée maximale d'interruption admissible et la perte de données maximale admissible sont suivies et documentées pour chaque test, afin de garantir que notre reprise est capable de répondre aux critères de définition internes. Des tests de reprise après sinistre sont minutieusement documentés avec les détails du scénario, le calendrier des événements et des éléments d'action pour l'amélioration.

Évaluations indépendantes

Test de pénétration

Elastic reconnaît la force et l'importance de la défense en profondeur, et prend en considération la sécurité du personnel, les mouvements latéraux, l'escalade des privilèges et les menaces persistantes. Dans cette optique, Elastic collabore avec plusieurs fournisseurs de services de tests de pénétration indépendants pour réaliser des tests de pénétration de la couche d'application et du réseau, des tests de segmentation et des examens de code sécurisé. Des tests de pénétration sont réalisés au moins tous les ans. Des résolutions sont apportées aux conclusions des tests de pénétration sur la base de l'état critique. Les résultats des tests de pénétration sont également signalés à la direction, pour faciliter l'alignement et la responsabilité interfonctionnels lorsqu'il s'agit d'apporter une résolution aux conclusions et de mettre en œuvre les autres contrôles préventifs et de détection lorsque c'est nécessaire. Les rapports de tests succincts et les rapports des états de la résolution sont disponibles sur demande des clients.

En plus des tests de pénétration indépendants, Elastic sponsorise et soutient un Programme de divulgation des vulnérabilités (récompense pour les bugs identifiés). Les chercheurs en sécurité sont encouragés à signaler les vulnérabilités via notre Programme de divulgation des vulnérabilités. L'équipe de sécurité produit d'Elastic trie et résout les envois sur la base de l'état critique. Pour en savoir plus sur notre politique de récompense pour les bugs identifiés ou pour envoyer un rapport, veuillez consulter le programme de récompense pour les bugs identifiés sur HackerOne.

Normes de conformité

Elastic s'engage à poursuivre et à maintenir les certifications et attestations de sécurité et de conformité qui fournissent le plus de valeur à ses clients. Nous prenons au sérieux la confiance que nos clients nous accordent pour alimenter leurs besoins en recherche, en observabilité et en sécurité dans des secteurs d'activité et régions du monde hautement réglementés. Pour obtenir une liste complète des certifications et attestations que propose Elastic Cloud, rendez-vous sur Sécurité et conformité d'Elastic.

Confidentialité des données

Chez Elastic, la confidentialité des données joue un rôle critique pour gagner et garder la confiance du client. Nous nous engageons à être transparents avec nos clients en ce qui concerne le traitement et la sécurisation de vos données dans Elastic Cloud.

Hébergement des données

Elastic utilise des fournisseurs de services Cloud, comme Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP) pour fournir Elastic Cloud. Nous prenons en charge les options d'hébergement de façon mondiale grâce à chacun de nos fournisseurs de service cloud. Les clients ont la possibilité de sélectionner la région dans laquelle ils souhaitent héberger leur déploiement Elastic Cloud, de sorte à répondre au mieux à leurs besoins de souveraineté des données. Des sauvegardes sont également configurées pour conserver les sauvegardes du client dans la région qu'il a sélectionnée.

Engagements contractuels

Elastic a créé des processus, des structures organisationnelles et des mesures techniques dans l'ensemble de l'entreprise pour garantir de respecter les principes de confidentialité mondiaux. Ces engagements sont soutenus par les accords de confidentialité contractuels que nous mettons à votre disposition dans notre Avenant relatif au traitement des données clients (Data Processing Amendment –"DPA") pour Elastic Cloud.

Elastic examine et met à jour régulièrement notre DPA pour qu'il reflète les exigences de confidentialité des données applicables, notamment les dispositions suivantes :

- Vous possédez vos données. Nous traitons vos données personnelles uniquement de la façon dont vous nous le demandez.
- Les données que nous traitons sont sujettes aux exigences de protection des données légales applicables.
- Nous avons mis en œuvre et nous sommes contractuellement engagés à des mesures techniques et organisationnelles appropriées, qui comprennent les clauses contractuelles standard, conformément à la décision de la Commission européenne 2021/914/EU ("SCC"), le cas échéant.
- Tout le personnel autorisé à traiter des données personnelles est soumis à des politiques et procédures de confidentialité strictes.
- Les clients sont informés des demandes de la part des personnes concernées. Elastic ne répondra pas sans le consentement du client, et aidera les clients à répondre à leurs exigences concernant la réponse à ces requêtes.
- Elastic a l'obligation, en vertu des SCC, d'informer ses clients au cas où une instance gouvernementale lui demanderait d'accéder aux données personnelles d'un client. Dans le cas où Elastic aurait l'interdiction légale de procéder à une telle divulgation, Elastic a l'obligation contractuelle, conformément aux SCC, de contester cette interdiction et de chercher à obtenir une dispense.
- Elastic utilise les accords de confidentialité et les programmes de formation des employés pour garantir que tout personnel impliqué dans le traitement de données personnelles en assure la confidentialité. Ces accords restent en vigueur, même une fois qu'un employé a quitté sa fonction au sein d'Elastic.
- Les sous-processeurs d'Elastic sont soumis aux mêmes normes et exigences organisationnelles. Elastic peut être tenu pour responsable des actes et oublis de ses sous-processeurs, au même titre que s'il fournissait lui-même ce service.

Sous-processeurs

Elastic utilise certains fournisseurs de services externes et affiliés internes pour fournir Elastic Cloud, ce qui peut nécessiter le traitement de données personnelles des utilisateurs (en tant que sous-processeur), strictement lorsque cela est nécessaire pour vous fournir les services.

Les sous-processeurs externes actuellement engagés par Elastic sont présentés sur https://www.elastic.co/fr/agreements/external_subprocessors et les sous-processeurs internes sont présentés sur https://www.elastic.co/fr/agreements/internal_subprocessors.

Transferts de données internationaux et Schrems II

Elastic est une entreprise mondiale et peut être amené à transférer des données depuis l'EEE et le Royaume-Uni vers des pays tiers à du personnel non européen d'Elastic, ainsi qu'aux organisations tierces nécessaires pour fournir les services. Ces lieux sont présentés dans la section sous-processeurs ci-dessus. Dans ces cas-là, Elastic se fie aux SCC, y compris le module contrôleur–processeur pour ses clients et le module processeur–processeur avec ses sous-processeurs, en plus de mesures supplémentaires solides.

Elastic a examiné les conseils EDPB concernant les mesures supplémentaires pour les transferts de données internationaux post-Schrems II. En prenant en compte l'expérience pratique d'Elastic, la faible susceptibilité d'un intérêt gouvernemental dans les données personnelles que traite Elastic, ainsi que les précautions qu'Elastic met en place pour protéger les données personnelles des clients, Elastic ne considère pas que son traitement des données personnelles des clients en dehors de l'Europe présente un risque vis-à-vis des droits des individus, et empêche Elastic de remplir ses obligations en tant qu'importateur de données conformément aux SCC.

- Une analyse interne et un examen externe ont conclu que les transferts de données d'Elastic ne s'inscrivaient pas dans les centres d'intérêt typiques des lois sur la surveillance. Nous proposons également de fournir des mesures supplémentaires pour protéger toutes données transférées.
- Sur la base de la nature de nos services et de nos activités de traitement de données, les demandes émanant des pouvoirs publics sont très improbables. Elastic n'a jamais reçu de demande FISA, EO12333 ou CLOUD Act.
- Les SCC sont appliquées pour protéger les transferts de données clients applicables. Lorsque des données personnelles originaires d'Europe sont (i) directement transférées vers Elastic par ses clients, (ii) transférées par Elastic sur une base d'intragroupe entre des entités du groupe Elastic ou (iii) transférées par Elastic vers des sous-processeurs externes, Elastic contracte des SCC avec ces parties.
- Les données sont chiffrées en transit et au repos.
- Les clients ont la possibilité de sélectionner des serveurs européens pour nos applications de service.
- Elastic évalue et développe continuellement ses dispositifs de protection contractuels, techniques et organisationnels afin de protéger les transferts de données.

Demande d’accès pour les pouvoirs publics

Elastic a établi des politiques et processus pour répondre aux demandes d’accès au Contenu client des pouvoirs publics. Ces politiques et processus adhèrent aux lois applicables en matière de protection des données ainsi qu’à votre contrat client.

Elastic n’a connaissance d’aucune loi applicable qui empiéterait sur sa capacité à respecter ses engagements concernant les demandes d’accès des pouvoirs publics et les divulgations requises. En aucun cas Elastic ne dévoilera d’informations personnelles massivement, de façon disproportionnée ou au hasard, qui irait au-delà de ce qui est nécessaire dans une société démocratique.

Nonobstant ce qui précède, Elastic n’a jamais reçu aucune demande émanant des pouvoirs publics d’accéder à du Contenu client, y compris en vertu de la Section 702 FISA. Nous n’avons également connaissance d’aucun accès direct au Contenu client, conformément à l’ordre exécutif EO 12333. Elastic n’a jamais créé de porte dérobée ou de passe-partout pour aucun de ses produits ou services, et n’a jamais autorisé aucune instance gouvernementale à accéder directement ou en toute liberté à ses serveurs.

Protéger les données personnelles en tant qu’entreprise

Notifications de confidentialité

Pour en savoir plus sur la façon dont Elastic collecte, utilise, divulgue, transfère ou stocke des informations personnelles dans Elastic Cloud, veuillez consulter notre Déclaration de confidentialité relative aux produits.

Réglementations mondiales concernant la confidentialité

Elastic s’engage à adhérer aux réglementations mondiales concernant la confidentialité, y compris le RGPD et le CCPA. Pour envoyer une Demande de personne concernée, veuillez consulter la section Nous contacter de la Déclaration générale de confidentialité. Pour en savoir plus sur la façon dont nous garantissons la conformité au RGPD de vos déploiements Elastic, rendez-vous sur Conformité d’Elasticsearch et de la Suite Elastic avec le RGPD.

