Visão geral da segurança da informação do Elastic Cloud

Outubro de 2023

elastic.co/pt

ÍNDICE

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Serviços e escopo

Com soluções em busca empresarial, observabilidade e segurança, ajudamos as pessoas a encontrar mais rapidamente o que precisam, manter aplicações de missão crítica funcionando sem problemas e se proteger contra ameaças cibernéticas. O Elastic Cloud foi projetado para oferecer flexibilidade a fim de que você possa adaptar e gerenciar as implantações para seu caso de uso específico, eliminando a complexidade e gerenciando a plataforma que está por trás das suas experiências de busca com velocidade, escala e relevância.

Nós compreendemos a responsabilidade significativa que temos para com vocês, nossos clientes, que confiam em nós para lhes proporcionar as melhores experiências de busca e, ao mesmo tempo, proteger seus dados. Nós trabalhamos incansavelmente para conquistar sua confiança. A segurança — desde a supervisão do conselho e a governança executiva no topo da organização até a forma como integramos e treinamos continuamente cada Elastician — é fundamental em tudo o que fazemos. A Elastic obteve um amplo conjunto de relatórios e certificações de conformidade líderes do setor para o serviço Elastic Cloud e nosso Sistema de Gestão de Segurança da Informação (SGSI). Esses relatórios e certificações servem como prova de que práticas de segurança eficazes são inerentes a todas as nossas atividades, incluindo desenvolvimento e implantação de produtos, gerenciamento de vulnerabilidades, gerenciamento de incidentes e processos de tratamento de ameaças.

Este documento descreve nossas políticas, procedimentos e controles técnicos em vigor para lhe dar a confiança que você merece para aproveitar suas soluções com o Elastic Cloud. O Elastic Cloud e suas soluções de software relacionadas podem ser implantados no local, em nuvens públicas ou privadas, ou em ambientes híbridos para satisfazer diversas necessidades dos usuários e clientes; no entanto, os controles para implantações autogerenciadas estão fora do escopo deste documento.

Visão geral do Elastic Cloud

A Elastic oferece soluções de busca empresarial, observabilidade e segurança nativas da nuvem que aprimoram as experiências de busca de clientes e funcionários, mantêm aplicações de missão crítica funcionando sem problemas e protegem contra ameaças cibernéticas. Os produtos da Elastic ingerem e armazenam dados de qualquer fonte e em qualquer formato para busca, análise e visualização.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

O Elastic Cloud é uma família de produtos de software como serviço (SaaS) que inclui Elasticsearch Service (ESS), Enterprise Search, Observability e Elastic Security. A Elastic hospeda e gerencia componentes do Elastic Stack, incluindo o Elasticsearch e o Kibana, na infraestrutura selecionada pelo cliente de vários provedores de nuvem pública, incluindo Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure e IBM. As soluções do Elastic Cloud incluem recursos avançados do Elastic Stack, como segurança, alerta, monitoramento, relatórios, machine learning e visualização.

Mais informações sobre os componentes do Elastic Cloud são fornecidas abaixo.

Componente do Elastic Cloud	**Descrição do componente**
Elasticsearch Service (ESS)	O ESS é um mecanismo distribuído de análise de dados e busca em tempo real e um datastore para todos os tipos de dados, incluindo textuais, numéricos, geoespaciais, estruturados e não estruturados.
Enterprise Search	O Elastic Enterprise Search fornece ferramentas poderosas para entregar experiências de busca com rapidez e total escalabilidade: O *Workplace Search* é uma ferramenta para unificar as plataformas de conteúdo de uma organização (Google Drive, Slack, Salesforce e muitas outras) em uma experiência de busca personalizada e natural. O *App Search* é uma caixa de ferramentas para os desenvolvedores aproveitarem o poder do Elasticsearch para adicionar busca a seus apps de SaaS e para celular, completa com um rastreador da web, APIs refinadas, dashboards intuitivos e controles de relevância ajustáveis. O *Site Search* permite adicionar poderosos recursos de busca a um site, incluindo a caixa de busca, se necessário.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Observability	O Elastic Observability possibilita análises unificadas de logs, métricas, desempenho de aplicações e informações de monitoramento de tempo de funcionamento. Usando o Elastic Agent e conectores de integração pré-criados para coleta de dados, as organizações podem revelar discrepâncias com machine learning e regras de detecção prontas para uso, apoiando as equipes de DevOps e SecOps.
Security	O Elastic Security proporciona prevenção, detecção e resposta a ameaças por meio de uma única interface de usuário: O *Elastic SIEM* fornece agregação e correlação de logs convencionais, dando suporte à detecção e resposta a ameaças, além de recursos avançados de segurança como avaliação de riscos com machine learning, gerenciamento integrado de casos e SOAR. O *Elastic Agent* oferece versatilidade ilimitada em uma solução compacta que funciona em praticamente qualquer lugar, incluindo ambientes híbridos. Ele pode prevenir ameaças, encaminhar dados e oferecer suporte a vários casos de uso para enriquecer as informações de segurança e a proteção. O *Limitless XDR* moderniza as operações de segurança, unificando o SIEM e a segurança de endpoint, permitindo análises de dados de vários anos, automatizando processos de detecção e resposta, e levando proteção nativa de endpoint para todos os hosts.

Programas de conformidade para nuvem

O Elastic Cloud foi projetado tendo a segurança em sua essência. Alcançamos e mantemos certificações e relatórios de atestado líderes do setor que demonstram nosso compromisso com a segurança, a conformidade, a privacidade e a confiabilidade.

O SGSI global da Elastic foi certificado pela ISO 27001 e o serviço comercial Elastic Cloud foi auditado ou certificado pela ISO 27017, ISO 27018, SOC 2 Tipo 2, CSA Cloud Compliance Matrix (CCM), HIPAA e PCI-DSS. Também temos resumos executivos de testes de penetração, bem como certificações específicas do setor e da região (ou seja, TISAX) disponíveis. Para obter mais informações sobre os padrões de conformidade pelos quais somos avaliados e saber como obter cópias dos nossos relatórios e certificações, consulte a seção Padrões de conformidade deste documento.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Além disso, o Elastic Cloud é autorizado pelo FedRAMP no nível de impacto Moderado no AWS GovCloud. Acesse nossa página Solução de nuvem da Elastic autorizada pelo FedRAMP para saber os detalhes da certificação. Clientes governamentais relevantes e possíveis clientes podem obter acesso aos nossos pacotes de segurança do FedRAMP por meio do FedRAMP Marketplace usando o FedRAMP Package Access Request Form (formulário de solicitação de acesso ao pacote do FedRAMP).

Dados de Uso do Produto e Conteúdo do Cliente

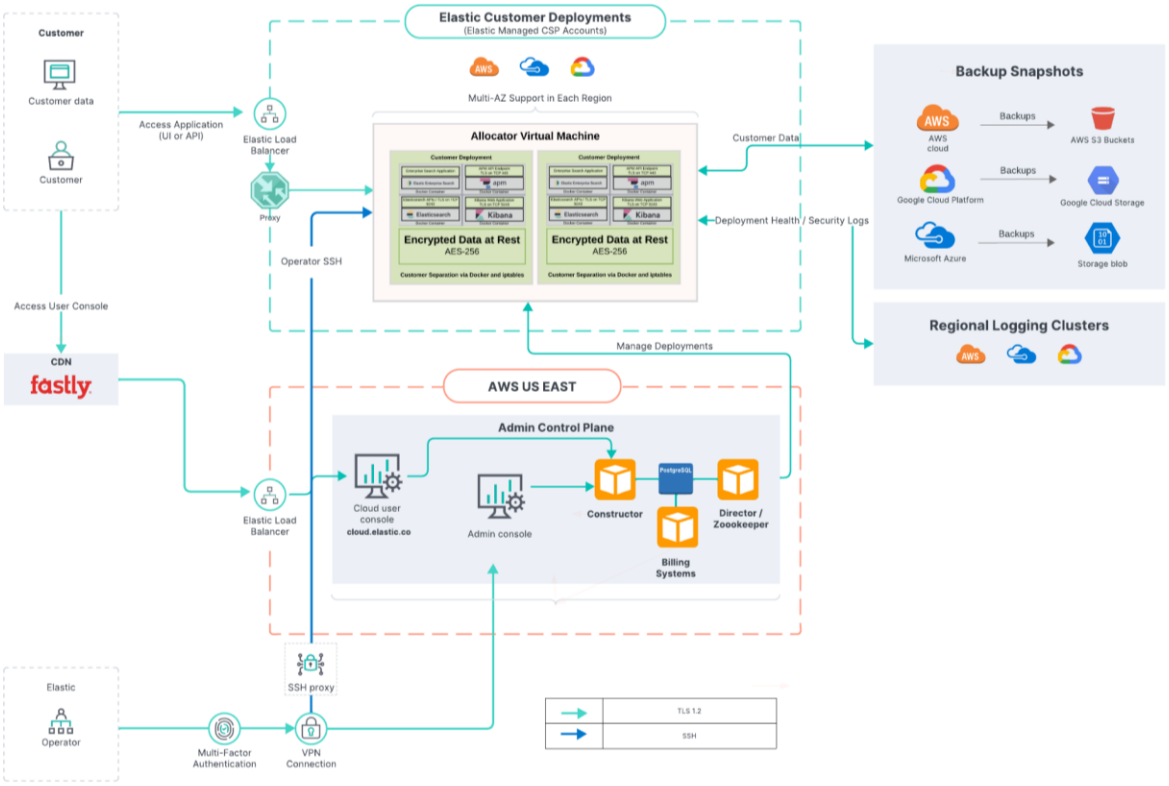
Tratamos as informações dos nossos clientes com o máximo cuidado — as proteções descritas ao longo deste documento existem para proteger o Conteúdo do Cliente. A distinção entre Dados de Uso do Produto e Conteúdo do Cliente é explicada mais detalhadamente abaixo.

Dados de Uso do Produto. São os dados usados pela Elastic para facilitar a entrega dos nossos produtos, gerenciar e monitorar a infraestrutura e fornecer suporte. São também usados na analítica e melhoria dos produtos. Os Dados de Uso do Produto são estritamente controlados e protegidos, e estão sujeitos a avaliações internas e externas que testam a segurança e a integridade desses dados. No entanto, este documento se concentra em como implantamos uma defesa profunda para proteger o Conteúdo do Cliente.

Conteúdo do Cliente. São os dados que os clientes ingerem, carregam ou enviam de outra forma para os produtos e serviços da Elastic. A Elastic somente processa esses dados conforme necessário para fornecer os produtos ou serviços e conforme necessário para cumprir a lei. O cliente sempre tem controle total sobre quais dados ingere no Elastic Cloud.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Diagrama do Serviço Elastic Cloud



Descrição da arquitetura do Elastic Cloud

Control Plane

O Control Plane do Elastic Cloud inclui os serviços de gerenciamento **ZooKeeper**, **Director** e **Constructor**, explicados mais abaixo:

- **ZooKeeper** — O ZooKeeper é um datastore distribuído que guarda informações essenciais para os componentes do Elastic Cloud: tabelas de roteamento de proxy, capacidade de memória anunciada pelos alocadores, alterações confirmadas por meio do Admin Console e assim por diante. Ele atua como um barramento de mensagens para comunicação entre os serviços. Também armazena o estado da instalação do Elastic Cloud e o estado de todas as implantações em execução no Elastic Cloud.

- **Director** — O Director gerencia o datastore do ZooKeeper e assina as solicitações de assinatura de certificado (CSRs) para clientes internos que querem se comunicar com o ZooKeeper. Ele também mantém os STunnels que o ZooKeeper usa para comunicação e estabelece o quórum quando novos nós do ZooKeeper são criados.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

- **Constructor** — O Constructor funciona como um agendador que monitora solicitações do console de administração. Ele determina o que precisa ser alterado e grava as alterações nos nós do ZooKeeper monitorados pelos alocadores. Também atribui nós de cluster a alocadores e maximiza a utilização de alocadores subjacentes para reduzir a necessidade de ativar hardware extra para novas implantações. O Construtor coloca nós e instâncias de cluster em diferentes zonas de disponibilidade para garantir que a implantação possa resistir a qualquer falha em uma zona.

  Essas preferências de posicionamento são customizáveis para requisitos de soberania de dados.

- **Cloud UI e API** — Estes recursos fornecem acesso à web e à API para que os administradores gerenciem e monitorem sua instalação.

Proxies

Os proxies lidam com solicitações de usuários, mapeando IDs de implantação que são passados em URLs de solicitação do container para os nós reais do cluster do Elasticsearch e outras instâncias. A associação de IDs de implantação a um container é armazenada no ZooKeeper e armazenada em cache pelos proxies. Caso haja uma inatividade do ZooKeeper, a plataforma ainda poderá atender às solicitações para implantações existentes usando o cache.

Eles também monitoram o estado e a disponibilidade das zonas se você tem um cluster do Elasticsearch altamente disponível. Se uma das zonas ficar inativa, o proxy não encaminhará nenhuma solicitação para lá. Além disso, eles ajudam no redimensionamento e nas atualizações sem tempo de inatividade. Antes de realizar uma atualização, um snapshot é gerado, e os dados são migrados para os novos nós. Quando a migração é concluída, um proxy alterna o tráfego para os novos nós e desconecta os nós antigos. Normalmente, vários proxies são configurados atrás de um balanceador de carga para garantir que o sistema permaneça disponível.

Alocadores

Os alocadores são executados em todas as máquinas que hospedam nós do Elasticsearch e instâncias do Kibana. Eles controlam o ciclo de vida dos nós do cluster das seguintes formas:

- Criando novos containers e iniciando nós do Elasticsearch quando solicitado
- Reiniciando um nó se ele parar de responder
- Removendo um nó se ele não for mais necessário

Eles também anunciam a capacidade de memória da máquina host subjacente ao ZooKeeper para que o Constructor possa tomar uma decisão informada sobre onde implantar.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Gerenciamento de riscos

A Elastic adotou uma abordagem baseada em risco para segurança e conformidade, utilizando o FAIR — a principal metodologia quantitativa de avaliação e análise de riscos, a fim de identificar e avaliar os riscos para os negócios, bem como priorizar atividades de mitigação de riscos.

O processo de avaliação de riscos da Elastic identifica e gerencia os riscos que podem afetar nossa capacidade de fornecer serviços confiáveis aos nossos clientes. Os principais riscos que identificamos e que nos preocupamos em controlar estão relacionados a:

- Gestão organizacional
- Segurança de recursos humanos
- Gestão de ativos
- Controle de acesso
- Criptografia
- Comunicações seguras
- Aquisição, desenvolvimento e manutenção de sistemas
- Relacionamentos com fornecedores
- Gerenciamento de incidentes de segurança da informação
- Gerenciamento de continuidade de negócios

O processo de identificação de riscos considera fatores internos e externos e seu impacto no alcance dos objetivos.

Os riscos identificados são analisados por meio de um processo que inclui uma análise de possíveis ameaças e vulnerabilidades em relação aos nossos objetivos de negócios e uma estimativa da importância potencial do risco.

O processo de avaliação de riscos leva em consideração como gerenciar o risco e se devemos aceitar, evitar, mitigar ou transferir o risco. Nós determinamos estratégias de mitigação para os riscos identificados. As estratégias podem incluir o projeto, o desenvolvimento e a implementação de controles e a adoção ou revisão de políticas e procedimentos.

O processo coletivo de identificação, análise e avaliação de riscos informa nosso Registro de Riscos, que são cenários de risco avaliados usando a metodologia FAIR e classificados com base no impacto financeiro estimado para a Elastic. O Registro de Riscos é reavaliado semestralmente para levar em conta mudanças nos fatores de risco internos e externos, prioridades de negócios e estratégias de mitigação em evolução. Esse processo também orienta a abordagem baseada no risco no relatório da equipe de segurança da informação ao Comitê de Auditoria do Conselho de Administração.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Governança

Sistema de Gestão de Segurança da Informação (SGSI) e supervisão

A Elastic implementou um SGSI que inclui políticas, procedimentos, estruturas operacionais e controles técnicos trabalhando em conjunto para proteger os dados dos clientes e da empresa. O SGSI foi certificado pela ISO 27001 e está organizado para abordar de forma abrangente todos os domínios de segurança e conformidade, incluindo governança, confiança, gerenciamento de riscos e vulnerabilidades, arquitetura e engenharia de segurança, segurança do produto, detecção de ameaças e resposta a incidentes.

O Conselho de Administração (Comitê de Auditoria) da Elastic supervisiona o SGSI e se reúne regularmente com o Diretor de Segurança da Informação (CISO) para garantir que o programa de segurança da informação esteja operando em alinhamento com as metas e objetivos de negócios, adotando as práticas recomendadas do setor e evoluindo com o cenário dinâmico de ameaças.

O SGSI da Elastic é reforçado com uma equipe dedicada de integridade empresarial e privacidade que colabora estreitamente com a equipe de segurança da informação em soluções organizacionais que garantem a adesão às leis e regulamentações globais de dados.

Políticas de segurança da informação

A Elastic desenvolveu um conjunto abrangente de políticas para reger nossas práticas de segurança da informação, com base em padrões do setor, incluindo NIST e ISO 27001, e comunicar as expectativas da diretoria em toda a empresa. Anualmente, os responsáveis pelas políticas revisam e a diretoria executiva aprova todas as políticas de segurança da informação. As políticas da Elastic abordam os seguintes domínios:

- Programa de segurança da informação
- Uso aceitável
- Gerenciamento de riscos
- Gestão de ativos
- Classificação de dados
- Retenção de registros
- Controle de acesso
- Segurança de estações de trabalho e servidores

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

- Análise de segurança e logging
- Gerenciamento de vulnerabilidades
- Gerenciamento de alterações
- Desenvolvimento de software seguro
- Resposta a incidentes
- Continuidade de negócios e recuperação de desastres

Todos os funcionários da Elastic são obrigados a atestar que leram e reconheceram o Código de Conduta da Elastic, bem como as Políticas de Segurança da Informação, Privacidade e Uso Aceitável no momento da contratação e anualmente a partir de então.

Não compartilhamos externamente o texto completo das nossas Políticas de Segurança da Informação. No entanto, está disponível um pacote de políticas de segurança da informação, que inclui o índice e o histórico de versões de cada política para fornecer clareza sobre os domínios cobertos por cada política, juntamente com evidências da revisão, atualização e aprovação regulares de cada uma. Para obter uma cópia desse documento, entre em contato com seu representante de conta da Elastic ou com o suporte da Elastic.

Além de políticas formais, a Elastic mantém manuais, documentos de processo e planos para domínios que têm requisitos de processo mais específicos ou práticas recomendadas em constante evolução, como criptografia na nuvem, gerenciamento de certificados e chaves e gerenciamento de riscos de terceiros.

Gestão de recursos humanos

Reconhecemos que um programa de segurança abrangente começa com um tom firme na liderança e envolve todos os funcionários da Elastic. Nosso código-fonte, o Manual do Funcionário e o Código de Conduta incluem orientações explícitas e padrões éticos que todos os funcionários da Elastic devem seguir. A Elastic tem uma política de tolerância zero para qualquer pessoa que viole esses compromissos, independentemente de cargo, antiguidade ou mandato.

A Elastic também estabeleceu práticas recomendadas de segurança no nível de entidade com linhas formais de relatórios, que facilitam o fluxo de informações para o pessoal relevante e garantem a responsabilização e a supervisão adequadas da conduta e do desempenho dos funcionários. As funções e responsabilidades são separadas com base nos requisitos funcionais, e as funções do cargo são explicitamente definidas.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Todas as contratações e rescisões são realizadas de acordo com políticas e procedimentos documentados, que incluem procedimentos para integração e desligamento rápidos e seguros de funcionários e contratados.

Outras práticas de segurança no nível de entidade incluem a realização de verificações de antecedentes de novas contratações e contratados antes da integração. Além disso, todos os funcionários da Elastic, incluindo executivos e a alta administração, devem concluir o treinamento de conscientização de segurança e ler e reconhecer as políticas de privacidade e segurança da informação, o Código de Conduta e o Manual do Funcionário no momento da contratação e depois anualmente.

Gestão de ativos

O Padrão para Gestão de Ativos rege o ciclo de vida da gestão de ativos, que inclui inventário de ativos, propriedade de ativos, devolução e alienação de ativos e requisitos de trilha de auditoria. Os processos de gestão de ativos entre gerenciamento de frota e gerenciamento de endpoint são distintos.
Cada processo independente é explicado abaixo:

Frota

Nossos parceiros provedores de serviços em nuvem (CSP), AWS, GCP, Azure e IBM, gerenciam a infraestrutura na qual o Elastic Cloud se baseia. Os clientes do Elastic Cloud têm a flexibilidade de escolher o CSP subjacente e a região geográfica para seus dados a cada implantação. Os controles de segurança física, mídia e hardware são de responsabilidade do CSP. A Elastic analisa o design e a eficácia operacional dos controles de gestão de ciclo de vida de hardware e mídia dos nossos parceiros provedores de serviços em nuvem durante as recertificações de terceiros que são conduzidas como parte do nosso programa de gerenciamento de riscos de terceiros.

Os clusters da Elastic utilizam o Elastic Observability para monitorar métricas de desempenho e tempo de atividade. Os ativos críticos são registrados em nosso inventário de ativos, cuja integridade e precisão são verificadas regularmente.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Endpoints de funcionários

O departamento de TI da Elastic monitora e gerencia os endpoints dos funcionários. O software de gerenciamento de dispositivos é utilizado para aplicar configurações de segurança, incluindo criptografia, gerenciamento de senhas, gerenciamento de sessões e bloqueio de tela, que são habilitados por padrão. Essas configurações não podem ser desabilitadas nem modificadas localmente. Os endpoints são protegidos com o Elastic Security, que fornece recursos de EDR e monitoramento e alerta em tempo real. Consulte a seção Segurança contra malware para obter mais informações sobre como protegemos os endpoints dos funcionários contra malware.

Todos os dispositivos emitidos pela Elastic são tratados de acordo com nosso ciclo de vida de gerenciamento de dispositivos. Quando um funcionário da Elastic é demitido, o acesso lógico é desabilitado, e os endpoints gerenciados pela empresa são enviados diretamente para uma empresa terceirizada que executa procedimentos de limpeza e destruição de dados. Nosso parceiro terceirizado fornece à Elastic certificados de destruição e reemite ou descarta a máquina com base no Padrão para Manuseio de Laptop da Elastic. O departamento de TI da Elastic mantém uma trilha de auditoria dos endpoints gerenciados pela Elastic para monitorar o status de cada dispositivo dentro do ciclo de vida de destruição de dados.

Por política, dispositivos móveis pessoais ou não gerenciados não podem armazenar dados de clientes e não são usados no desenvolvimento ou suporte do Elastic Cloud.

Gerenciamento de configuração

A Elastic gerencia a configuração por meio de código, e as alterações de configuração seguem o procedimento padrão de gerenciamento de alterações, que inclui autorização, revisão e aprovação por pares e pacotes de teste automatizados. A Elastic monitora alterações diretas nos arquivos de configuração de produção por meio do monitoramento de integridade de arquivos e detecções de atividades suspeitas.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Proteção dos dados

Classificação e retenção de dados

O Padrão para Classificação de Dados da Elastic exige que os dados sejam classificados com base na sensibilidade, com restrições de acesso e compartilhamento definidas para cada classificação. O Conteúdo do Cliente e os Dados de Uso do Produto são classificados como restritos (a classificação mais sensível) e estão sujeitos aos mais rígidos padrões de proteção de dados, projetados para preservar a confidencialidade, a integridade e a disponibilidade desses dados. Para definições de Conteúdo do Cliente e Dados de Uso do Produto, consulte a seção Dados de Uso do Produto e Dados do Cliente deste documento.

O Padrão para Retenção de Registros da Elastic exige que os dados sejam descartados de acordo com cronogramas de retenção definidos com base no tipo de dados e nos requisitos operacionais, contratuais, legais e regulamentares. Os clientes podem enviar uma solicitação de exclusão de conta ao suporte da Elastic a qualquer momento para que suas informações sejam excluídas. Para obter informações sobre como enviar uma solicitação de acesso a dados, consulte a seção Privacidade de dados deste documento.

Coleta, manuseio e descarte de dados

Coleta de dados

A Elastic coleta apenas as informações necessárias para fornecer, dar suporte a, manter, proteger e melhorar nossos serviços. Essas informações nunca são vendidas a terceiros. Para obter mais informações sobre as informações que coletamos dos clientes, consulte a Product Privacy Statement (Declaração de Privacidade do Produto).

Ingestão de dados

A Elastic não controla nem acessa os dados que os clientes escolhem armazenar, transmitir ou processar em sua implantação da Elastic. Os dados ingeridos pela implantação da Elastic de um cliente ficam a seu exclusivo critério e sob seu controle em todos os momentos.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Destruição de dados

O Padrão para Retenção de Registros e o Padrão para Gestão de Ativos regem os requisitos de destruição de dados. Nossos parceiros provedores de serviços em nuvem gerenciam a exclusão segura e a destruição de dados da infraestrutura de hospedagem. Os clientes mantêm controle total sobre o conteúdo que armazenam em suas instâncias da Elastic e têm o direito de remover ou excluir qualquer conteúdo de suas instâncias da Elastic a qualquer momento.

Criptografia

Criptografia em trânsito

A criptografia em trânsito do Elastic Cloud é aplicada por padrão por meio do Transport Layer Security (TLS). A força de criptografia mínima aceita é TLS 1.2. As conexões TLS (HTTPS) são exibidas no Diagrama do Serviço Elastic Cloud.

Os certificados usados para oferecer suporte ao Elastic Cloud são fornecidos pela Digicert e utilizam autenticação de chave pública RSA com chaves de 2.048 bits. A Elastic mantém certificados válidos para nossas implantações em nuvem, e eles são classificados como A+ pelo Qualys SSL Labs. Os resultados desses testes podem ser reproduzidos acessando o site SSL Labs.

Criptografia em repouso

Nossos parceiros provedores de serviços em nuvem fornecem criptografia em repouso, que é habilitada por padrão. Todos os nossos provedores de serviços em nuvem apresentam comprimentos mínimos de chave de acordo com as diretrizes do NIST (256 bits).

Gerenciamento de chaves

As chaves de criptografia nunca saem do host onde são geradas e são consideradas descartáveis. Elas são geradas automaticamente sempre que um host de máquina virtual é criado ou substituído. Nunca são copiadas em backup, expostas ou saem do host. O gerenciamento de chaves para criptografia nos serviços de IaaS subjacentes é automatizado usando o serviço de gerenciamento de chaves do provedor.

O gerenciamento de chaves para os serviços da Elastic é mantido como infraestrutura como código e parte da documentação operacional de cada componente ou serviço aplicável.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Gerenciamento de segurança de redes e dispositivos

Firewalls

Nossos parceiros provedores de serviços em nuvem gerenciam os firewalls de hardware para a infraestrutura de produção. A Elastic também mantém firewalls de software para filtrar o tráfego de entrada não autorizado da internet e negar conexões de rede de entrada que não sejam explicitamente autorizadas (negação por padrão). Mais segmentação de rede e firewalls estão em vigor entre zonas lógicas dentro do ambiente.
Os conjuntos de regras de firewall são revisados pelo menos semestralmente. As alterações nas regras de firewall seguem o processo padrão de gerenciamento de alterações e estão sujeitas a controles de gerenciamento de alterações. Além disso, todo o acesso aos firewalls é implementado utilizando RBAC.

Os clientes do Elastic Cloud podem utilizar a funcionalidade de filtragem de tráfego ou configurar o PrivateLink para restringir ainda mais o tráfego em suas implantações.
IP traffic filters (Filtros de tráfego IP) | Documentação do Elasticsearch Service |
Elastic AWS PrivateLink traffic filters (Filtros de tráfego do AWS PrivateLink) |
Documentação do Elasticsearch Service | Elastic

Segurança contra malware

O antimalware é habilitado em todos os endpoints de funcionários por meio de configurações de TI gerenciadas centralmente. Os administradores locais não podem desabilitar nem modificar essas configurações. A solução Elastic Security fornece recursos de EDR e uma equipe de plantão 24x7 para análises de segurança da informação e alertas de ações.

O Elastic Security é utilizado para proteger o ambiente de produção do Elastic Cloud. Assinaturas e padrões de comportamento são atualizados automática e continuamente. As detecções podem ser implantadas rapidamente contra ameaças emergentes, e uma equipe dedicada de inteligência, detecções e resposta a ameaças gerencia a detecção, análise, resposta e correção de possíveis infecções por malware.

Sincronização de horário

A sincronização de horário é obtida por meio de NTP com uma fonte de horário comum (servidores NIST).

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Acesso lógico

Controle de acesso por função

A Elastic adere ao princípio do menor privilégio ao provisionar o acesso aos usuários internos. Os funcionários da Elastic recebem apenas o nível de acesso necessário para sua função. Os direitos de acesso são revisados e modificados regularmente caso haja uma mudança de emprego ou outras circunstâncias em que o acesso do usuário não seja mais necessário.

Os produtos da Elastic também apresentam controle de acesso por função para permitir que nossos clientes implementem gerenciamento de acesso refinado para os usuários em suas implantações da Elastic e na plataforma de gerenciamento do Elastic Cloud.

Integração e rescisão

Os novos contratados recebem automaticamente acesso a aplicações corporativas de SaaS nativas da nuvem com base em regras pré-configuradas em nosso sistema centralizado de gerenciamento de identidade e acesso (IAM, pelas iniciais em inglês). Os conjuntos de regras de provisionamento automático utilizam atributos do cargo do nosso sistema de registro de RH, como organização de supervisão, família de cargos, nível de cargo e estrutura gerencial para conceder o acesso específico necessário para aquele usuário individual. Qualquer acesso além desse requer uma solicitação formal documentada em um tíquete e está sujeito a análise e aprovação gerencial.

Se um funcionário for transferido para uma função ou organização diferente na Elastic, as alterações nos atributos do cargo no sistema de registro de RH iniciarão automaticamente o fluxo de trabalho no sistema centralizado de IAM para reprovisionar sua conta com o acesso apropriado para sua nova função. As autorizações de acesso da sua função anterior serão desprovisionadas, e o novo acesso será provisionado com base nos atributos do cargo da nova função.

Após a rescisão, o acesso concedido por meio do nosso sistema centralizado de IAM é automaticamente suspenso quando a situação laboral muda no nosso sistema de gestão de RH. Essa verificação de validação ocorre várias vezes ao dia.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Acesso à produção

Um número limitado de funcionários da Elastic recebeu acesso privilegiado ao nosso ambiente de produção do Elastic Cloud. A Elastic mantém esse acesso para fins de gerenciamento, manutenção e suporte da plataforma. A Política de Manuseio de Dados da Elastic proíbe expressamente que os funcionários da Elastic acessem os dados dos clientes, mesmo em cenários de manutenção ou solução de problemas. Os clientes devem dar seu consentimento por escrito antes que um funcionário da Elastic visualize quaisquer dados que tenham sido compartilhados voluntariamente para fins de suporte ou solução de problemas. A Elastic não visualiza proativamente os dados do cliente carregados ou ingeridos no Elastic Cloud. Os clientes podem optar por editar ou limpar os dados antes do compartilhamento com a Elastic.

Além disso, a equipe de detecção e resposta a ameaças à segurança da informação desenvolveu e implementou detecções para atividades suspeitas de contas internas e acesso não autorizado, incluindo monitoramento de integridade de arquivos e indicadores de controle de contas ou exfiltração de dados. Essas detecções fazem parte de fluxos de trabalho automatizados que alertam a equipe de detecção e resposta a ameaças sobre atividades suspeitas e disparam a investigação do analista.

Revisões de acesso do usuário

A Elastic segue o princípio do menor privilégio e autoriza apenas o acesso necessário para o desempenho de cada função. Os responsáveis pelo sistema e a gerência analisam e recertificam o acesso do usuário, incluindo o acesso privilegiado, durante as revisões trimestrais de acesso do usuário. O acesso que não é mais necessário é desprovisionado.

Gerenciamento de alterações

O Padrão para Gerenciamento de Alterações rege os processos de gerenciamento de alterações e estabelece requisitos projetados para controlar o desenvolvimento e a implantação de alterações de software e infraestrutura no ambiente de produção de maneira segura e gerenciada.

O processo de gestão de alterações garante que as alterações propostas sejam autorizadas, revisadas por pares, testadas, implementadas e liberadas de maneira controlada, e que o status de cada alteração proposta seja documentado e monitorado. Caso seja necessária uma alteração emergencial, a aprovação documentada e os testes automatizados ainda serão necessários. Uma revisão manual da alteração emergencial também é necessária, mas pode ocorrer após a implementação.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Segurança da cadeia de suprimentos

As implantações de software em ambientes de produção são gerenciadas por meio de pipelines automatizados de CI/CD. As alterações são armazenadas em ramificações designadas em cada repositório respectivo. As ramificações de desenvolvimento são usadas para desenvolvimento ativo, e as ramificações principais contêm código pronto para produção. As alterações têm controle de versão e, antes da mesclagem com a ramificação principal, uma série de testes automatizados, incluindo verificações de segurança, são realizados. As proteções de ramificação estão habilitadas, o que exige que os conjuntos de testes sejam aprovados antes que a alteração seja autorizada para ser mesclada à ramificação principal. Quando uma alteração é totalmente autorizada (ela passa nos testes e verificações de segurança, a revisão e a aprovação dos pares são obtidas e a alteração passa nas verificações de integração), o software de implantação automatizado envia a alteração para a produção sem necessidade de intervenção manual.

Nosso código-fonte é armazenado em um sistema de controle de versão monitorado e com acesso controlado. A atividade do usuário é capturada em logs de auditoria, e detecções estão em vigor para alertar sobre modificações e processos de compilação inesperados ou suspeitos. A capacidade de modificar o código em cada repositório é restrita com base nas funções do cargo.

Desenvolvimento seguro

SDLC

Os requisitos de segurança para nosso ciclo de vida de desenvolvimento de sistemas (SDLC, pelas iniciais em inglês) são mantidos no Framework de Desenvolvimento Seguro de Software. Esse framework determina o processo para projetar, desenvolver, implantar, monitorar e manter com segurança todo o software da Elastic. Também inclui requisitos para proteger nossos sistemas de compilação e mitigar os riscos de comprometimento da cadeia de compilação. Os sistemas de compilação incluem pipelines de entrega de software, registros de pacotes, repositórios de artefatos, CI/CD e sistemas de gerenciamento de código-fonte. O Framework de Desenvolvimento Seguro de Software proíbe o uso de dados de produção para testes e em sistemas que não sejam de produção. Também requer a separação entre ambientes de produção e não de produção. A segmentação ambiental é avaliada durante testes de penetração de terceiros.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Design e arquitetura seguros

O desenvolvimento de software da Elastic segue as práticas recomendadas de segurança em design e arquitetura para produzir software “seguro por design” e “seguro por padrão”.

O Framework de Desenvolvimento Seguro de Software descreve os requisitos de proteção de dados e os princípios de segurança que todos os projetos devem seguir, incluindo:

- Confidencialidade — Os dados são protegidos contra observação ou divulgação não autorizadas, tanto em trânsito quanto quando armazenados.
- Integridade — Os dados são protegidos contra criação, alteração ou exclusão não autorizadas.
- Disponibilidade — Os dados estão disponíveis para usuários autorizados conforme necessário e atendem a SLAs de disponibilidade definidos.
- Identificação, autenticação, autorização
- Não repúdio
- Auditoria e logging
- Controle de acesso e princípios de menor privilégio
- Comunicações seguras e padrões de criptografia
- Padrões seguros e à prova de falhas/proteção contra falhas

A modelagem de ameaças e as revisões da arquitetura de segurança também fazem parte do processo de desenvolvimento de software para garantir que o design leve em consideração os princípios de segurança exigidos.

Codificação segura

Como fornecedor de SaaS, reconhecemos a importância de práticas de codificação seguras. Vulnerabilidades de codificação comuns, como OWASP Top 10 e CWE Top 25, são abordadas no Treinamento de Desenvolvimento Seguro de Software, que é lançado anualmente para equipes e indivíduos relevantes. As alterações no código-fonte exigem revisão e aprovação (por meio de uma solicitação de mesclagem) de pelo menos um revisor (que não tenha sido o autor da alteração) antes de mesclar as alterações. As alterações são revisadas para identificar possíveis impactos de segurança que a alteração possa introduzir. Além disso, os testes de penetração independentes, que incluem revisão segura do código, dão ênfase adicional às práticas comuns de codificação não segura. Os problemas identificados durante a modelagem de ameaças, a revisão de segurança ou a revisão do código-fonte são monitorados, avaliados e corrigidos com base no risco avaliado de acordo com o Padrão para Gerenciamento de Vulnerabilidades.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

A Elastic também patrocina um programa de recompensas por bugs como parte de nossos esforços para manter o software seguro e proteger nossos clientes contra vulnerabilidades. Para obter mais informações, consulte o Programa de Divulgação de Vulnerabilidades na seção Gerenciamento de vulnerabilidades e patches.

Análise de software open source e de terceiros

O Framework de Desenvolvimento Seguro de Software exige que as dependências de código de bibliotecas open source e de terceiros sejam identificadas e monitoradas. O software de gerenciamento de dependências está disponível para ajudar na identificação, verificação e correção de dependências vulneráveis.

Gerenciamento de vulnerabilidades e patches

O Padrão para Gerenciamento de Vulnerabilidades rege o programa de gerenciamento de vulnerabilidades e define requisitos para verificação de recursos da Elastic, bem como triagem, análise, correção e divulgação de vulnerabilidades. A Elastic realiza verificações de vulnerabilidades e aplica patches tanto à infraestrutura na qual o Elastic Cloud se baseia quanto aos próprios componentes do Elastic Cloud. Os processos para cada um são detalhados abaixo.

Vulnerabilidade da infraestrutura e gerenciamento de patches

A Elastic utiliza um scanner de vulnerabilidade comercial para verificar nossos ativos continuamente. Todos os ativos de produção são incluídos nessas verificações. O fornecedor de software terceirizado atualiza os conjuntos de regras continuamente. A gravidade das vulnerabilidades é baseada nas classificações do CVSS, e os cronogramas de aplicação de patches também correspondem às classificações do CVSS. Vulnerabilidades críticas e altas são priorizadas para correção imediata ou como parte da próxima versão agendada.

Vulnerabilidade de produtos e gerenciamento de patches

Testamos rigorosamente nossos produtos em busca de vulnerabilidades de segurança por meio de testes de penetração de terceiros, verificações e análises de código automatizadas e manuais, verificações de OSS, testes de segmentação e por meio de nosso programa de divulgação de vulnerabilidades. Quando uma vulnerabilidade é descoberta em um produto da Elastic, a Elastic a avalia de acordo com o Padrão para Gerenciamento de Vulnerabilidades com o objetivo de determinar a gravidade e um plano de correção. Se necessário, emitiremos um Elastic Security Advisory (ESA).

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Esse é um aviso da Elastic a seus usuários sobre problemas de segurança com os produtos da Elastic. A Elastic atribui um identificador CVE e um identificador ESA a cada aviso, juntamente com um resumo e detalhes de correção e mitigação. Todos os novos avisos são anunciados no fórum Security announcements (Comunicados de segurança).

O Padrão para Gerenciamento de Vulnerabilidades também rege a publicação de divulgações. O processo de divulgação inclui o lançamento de uma nova versão do produto, se necessário, e a emissão de um comunicado na página de avisos. Dependendo da natureza da vulnerabilidade, também entraremos em contato com clientes individuais, publicaremos um post no blog e/ou enviaremos o CVE ao MITRE.

Os clientes podem acompanhar os ESAs por meio de um feed RSS.

Programa de Divulgação de Vulnerabilidades

A Elastic tem orgulho de patrocinar um Programa de Divulgação de Vulnerabilidades por meio do qual os pesquisadores de segurança podem enviar vulnerabilidades de forma responsável para análise interna. A equipe de segurança do produto da Elastic analisa os envios, avalia a exposição ao risco e corrige com base no risco avaliado. Acesse o Elastic Bug Bounty Program no HackerOne para ver nossa Política de Recompensas por Bugs ou para enviar um relatório.

Gerenciamento de riscos de terceiros

Integração de terceiros

Todos os terceiros, incluindo subprocessadores, estão sujeitos a um processo completo de admissão e análise. O perfil de risco de cada fornecedor é avaliado com base no serviço que ele fornece, nos tipos de dados que manipulará, no nível de acesso que terá aos sistemas internos e em outros fatores que capturam a criticidade e o perfil de risco do fornecedor.

Com base no perfil de risco do fornecedor e nos tipos de serviços que ele fornecerá à Elastic, um fluxo de trabalho de análise é executado. Todos os fornecedores que terão acesso a informações sensíveis, acesso a sistemas internos ou fornecerão um serviço de tecnologia crítico precisam passar por um escrutínio adicional, incluindo, entre outros, análise de segurança da informação, jurídica e de privacidade. Esse escrutínio adicional inclui a análise das práticas de segurança, das certificações

de segurança e dos relatórios de conformidade de terceiros. A conformidade com as leis do país onde os dados são processados, armazenados e transmitidos é levada em consideração e, quando considerado necessário, a Elastic poderá buscar requisitos de segurança adicionais em acordos com terceiros.

A Elastic também publicou um Código de Conduta do Fornecedor que documenta os requisitos éticos esperados dos nossos fornecedores e parceiros. Inclui, entre outros, requisitos de ética e conformidade, saúde e segurança dos funcionários, direitos humanos e trabalhistas, e gestão ambiental.

Recertificação de terceiros

Um processo contínuo de gerenciamento de riscos de informações de terceiros está em vigor para conduzir a recertificação dos fornecedores existentes. Os terceiros são classificados com base no nível de risco, e a equipe de segurança da informação da Elastic analisa as práticas de segurança de terceiros de acordo com os requisitos em vigor para cada nível de risco.

Todos os provedores de serviços em nuvem que fornecem serviços de infraestrutura para o Elastic Cloud são analisados e recertificados pelo menos uma vez por ano. O processo de recertificação envolve a análise do perfil de risco e o exame dos relatórios de segurança e conformidade do fornecedor para garantir que os controles de segurança e conformidade esperados cubram adequadamente os serviços que consumimos e que os controles sejam projetados e operem de forma eficaz.

Detecção de ameaças

Monitoramento e alerta

Utilizamos o Elastic Security como nossa solução de SIEM, o que nos permite desenvolver e implantar rapidamente detecções para ameaças emergentes e padrões de ataque, bem como detecções de comportamento suspeito, detecções de monitoramento de integridade de arquivos e padrões comuns de comportamento de malware. O monitoramento dos nossos ambientes é realizado em tempo real por meio de nossas detecções automatizadas. Fluxos de trabalho de alerta pré-configurados estão em vigor para notificar o pessoal apropriado da Elastic em caso de indicadores suspeitos. Nossa equipe de detecção e resposta a ameaças investiga e aciona esses alertas 24 horas por dia, 7 dias por semana.

Um pessoal certificado e continuamente treinado lida com eventos e incidentes de segurança de acordo com nosso Padrão de Resposta a Incidentes e com o plano de Resposta a Incidentes. Para obter mais detalhes sobre o processo de gerenciamento de incidentes, consulte a seção Resposta a incidentes deste documento.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Gerenciamento e retenção de logs

Utilizamos o Elasticsearch como nossa solução de gerenciamento de logs. Somos capazes de ingerir e centralizar logs de diversas fontes, incluindo mecanismos de detecção, nossos provedores de IaaS, ferramentas de gerenciamento de vulnerabilidades, console de administração em nuvem e muito mais, para desenvolver habilidades robustas de logging, auditoria e análise forense. Nossos logs têm acesso controlado para evitar adulterações, e o acesso de edição é restrito ao pessoal de engenharia de segurança com base no menor privilégio. Além disso, a detecção e os alertas automatizados, incluindo o monitoramento da integridade de arquivos, protegem nossos sistemas de logging e notificam a equipe de detecção e resposta a ameaças sobre atividades suspeitas quase em tempo real.

Os logs são retidos de acordo com nosso Padrão de Retenção de Dados com base em requisitos comerciais, legais e contratuais. Os clientes interessados em enviar uma solicitação de acesso a dados podem consultar a seção Privacidade de dados deste documento.

Resposta a incidentes

A segurança da informação da Elastic tem uma equipe de detecção e resposta a ameaças que atua em esquema 24x7, dedicada ao gerenciamento de eventos e incidentes de segurança. O Padrão de Resposta a Incidentes rege a função de resposta a incidentes e determina como deve ser a identificação de eventos, o tratamento de eventos, a geração de relatórios e os requisitos de treinamento. O Plano de Resposta a Incidentes separado apresenta diretrizes detalhadas para incidentes de segurança quanto a preparação, detecção, análise, contenção, erradicação, recuperação e geração de relatórios. Equipes treinadas que exercitam e testam regularmente o Plano de Resposta a Incidentes lidam com todos os incidentes. Os incidentes também exigem um relatório documentado após as ações e um exercício de lições aprendidas.

Caso detectemos uma violação ou tomemos conhecimento de acesso não autorizado a sistemas ou dados, a equipe jurídica e de segurança da informação da Elastic emitirá comunicações ao cliente conforme exigido por lei ou de acordo com os termos do contrato e sem demora injustificada.

Se um incidente de segurança exige um relatório a uma entidade reguladora externa ou do setor, o Plano de Resposta a Incidentes da Elastic inclui instruções detalhadas sobre nossas obrigações para a geração de relatórios, com base no cenário em questão. O Plano também designa uma equipe formal de resposta a incidentes de segurança informática (CSIRT, pelas iniciais em inglês) com funções e responsabilidades documentadas para garantir a comunicação adequada de e para os indivíduos apropriados.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Confiabilidade

Disponibilidade e status

A arquitetura de alta disponibilidade está disponível e é recomendada no Elastic Cloud com um SLA aprimorado. Discuta essa opção com sua equipe de conta se você acha que pode lhe trazer benefícios. Dados históricos e em tempo real sobre o desempenho do serviço Elastic Cloud estão disponíveis nesta página de status da Elastic.

Continuidade de negócios e recuperação de desastres

A Elastic mantém planos abrangentes de continuidade de negócios e recuperação de desastres, além do Padrão para Continuidade de Negócios e Recuperação de Desastres, para se preparar, responder e se recuperar de desastres.

A Elastic é uma empresa distribuída globalmente desde a criação. Os funcionários estão totalmente equipados para trabalhar remotamente, e as equipes distribuídas globalmente são compostas tendo em mente a redundância geográfica. Os escritórios da Elastic não contêm nenhuma infraestrutura ou sistema de TI necessários para a conectividade dos funcionários ou para fornecer serviços e suporte da Elastic aos nossos clientes.

A Elastic mantém planos de recuperação de desastres para o Elastic Cloud, que são testados pelo menos anualmente. Os testes são únicos, com uma área de foco definida a cada ano, para identificar lacunas de conhecimento e pontos fracos em nossas capacidades de recuperação técnica. O RTO e o RPO são monitorados e documentados para cada teste para garantir que nossa recuperação seja capaz de atender aos critérios de definição interna. Os testes de recuperação de desastres são minuciosamente documentados com detalhes do cenário, um cronograma de eventos e itens de ação para melhoria.

Avaliações independentes

Teste de penetração

A Elastic reconhece a força e a importância da defesa em profundidade, levando em consideração a segurança do pessoal, o movimento lateral, a escalada de privilégios e as ameaças persistentes. Com isso em mente, a Elastic trabalha com vários provedores independentes para realizar testes de penetração de rede e de camada de aplicação, testes de segmentação e revisão segura do código.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

O teste de penetração é realizado pelo menos anualmente. As descobertas dos testes de penetração são corrigidas com base na criticidade. Os resultados dos testes de penetração também são relatados à alta administração para facilitar o alinhamento multifuncional e a responsabilização na correção de descobertas e na implementação de controles preventivos e de detecção adicionais, quando necessário. Relatórios resumidos de testes de penetração e relatórios de status de correção estão disponíveis aos clientes mediante solicitação.

Além dos testes de penetração independentes, a Elastic patrocina e mantém um Programa de Divulgação de Vulnerabilidades (Bug Bounty) formal. Os pesquisadores de segurança são incentivados a relatar vulnerabilidades por meio do nosso Programa de Divulgação de Vulnerabilidades. A equipe de segurança do produto da Elastic faz a triagem e corrige os envios com base na criticidade. Para obter mais informações sobre nossa Política de Recompensas por Bugs ou para enviar um relatório, acesse nosso Bug Bounty Program no HackerOne.

Padrões de conformidade

A Elastic tem o compromisso de buscar e manter certificações e atestados de segurança e conformidade que forneçam o máximo valor aos nossos clientes. Levamos a sério a confiança que nossos clientes depositam em nós para atender a suas necessidades de busca, observabilidade e segurança em setores e regiões altamente regulamentados em todo o mundo. Para ver a lista completa de certificações e atestados que o Elastic Cloud oferece, acesse a página de segurança e conformidade da Elastic.

Privacidade dos dados

Na Elastic, a privacidade dos dados desempenha um papel fundamental para conquistar e manter a confiança do cliente. Temos o compromisso de fornecer aos nossos clientes transparência sobre como processamos e protegemos seus dados no Elastic Cloud.

Hospedagem dos dados

A Elastic usa provedores de serviços em nuvem, como Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP), para fornecer o Elastic Cloud. Oferecemos suporte para opções de hospedagem globalmente por meio de cada um de nossos provedores de serviços em nuvem.
Os clientes podem selecionar a região onde gostariam de hospedar sua implantação do Elastic Cloud para melhor atender às suas necessidades de soberania de dados. Os backups também são configurados para reter backups de clientes na região selecionada.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Compromissos contratuais

A Elastic criou processos, estruturas organizacionais e medidas técnicas em toda a empresa para garantir o cumprimento dos princípios globais de privacidade. Esses compromissos são respaldados pelos termos contratuais de privacidade que disponibilizamos a você em nossa Emenda sobre Processamento de Dados do Cliente ("DPA", pelas iniciais em inglês) para o Elastic Cloud.

A Elastic revisa e atualiza regularmente a DPA para refletir os requisitos de privacidade de dados aplicáveis, incluindo as seguintes disposições:

- Seus dados pertencem a você. Nosso tratamento de dados pessoais é realizado apenas sob sua instrução.
- Os dados que tratamos estão sujeitos aos requisitos legais de proteção de dados aplicáveis.
- Implementamos e estamos contratualmente comprometidos com as medidas técnicas e organizacionais adequadas, que incluem as cláusulas contratuais padrão de acordo com a Decisão 2021/914/UE da Comissão Europeia ("SCCs"), quando aplicáveis
- Todo o pessoal autorizado a processar dados pessoais está sujeito a políticas e procedimentos de confidencialidade rigorosos.
- Os clientes são notificados sobre solicitações dos titulares dos dados. A Elastic não responderá sem o consentimento do cliente e ajudará os clientes a atender a seus requisitos na resposta a tais solicitações.
- A Elastic é obrigada, de acordo com as SCCs, a notificar seus clientes caso seja submetida a uma solicitação de acesso aos dados pessoais do cliente por parte de uma autoridade governamental. Caso a Elastic seja legalmente proibida de fazer tal divulgação, a Elastic será contratualmente obrigada, de acordo com as SCCs, a contestar tal proibição e buscar uma renúncia.
- A Elastic utiliza acordos de confidencialidade e programas de treinamento de funcionários para garantir que qualquer pessoal envolvido no tratamento de dados pessoais mantenha a confidencialidade. Esses acordos vão além da conclusão do mandato de um funcionário na Elastic.
- Os subprocessadores da Elastic estão sujeitos aos mesmos padrões e requisitos organizacionais. A Elastic é responsável pelos atos e omissões de seus subprocessadores tanto quanto se nós mesmos estivéssemos prestando os serviços.

Subprocessadores

A Elastic usa determinados provedores de serviços externos e afiliados internos para fornecer o Elastic Cloud, o que pode exigir o tratamento de dados pessoais do cliente (como subprocessadores) estritamente conforme necessário para fornecer serviços a você.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Os subprocessadores externos atualmente contratados pela Elastic estão definidos em https://www.elastic.co/pt/agreements/external_subprocessors, e os subprocessadores internos estão definidos em https://www.elastic.co/pt/agreements/internal_subprocessors.

Transferências internacionais de dados e Schrems II

A Elastic é uma empresa global e pode transferir dados do EEE e do Reino Unido para países terceiros, para funcionários não europeus da Elastic, bem como para organizações terceirizadas que sejam necessárias para fornecer nossos serviços. Esses locais são definidos na seção Subprocessadores acima. Nesses casos, a Elastic conta com as SCCs, incluindo o módulo controlador-processador com seus clientes e o módulo processador-processador com seus subprocessadores, além de medidas complementares robustas.
A Elastic revisou as orientações do Comitê Europeu para a Proteção de Dados (CEPD) sobre medidas suplementares para transferências internacionais de dados pós-Schrems II. Levando em consideração a experiência prática da Elastic, a baixa probabilidade de interesse do governo nos processos de dados pessoais da Elastic, bem como as salvaguardas que a Elastic implementa para proteger os dados pessoais dos clientes, a Elastic não considera que seu tratamento de dados pessoais dos clientes fora da Europa apresente um risco para os direitos dos indivíduos, impedindo a Elastic de cumprir suas obrigações como "importador de dados" nos termos das SCCs.

- A análise interna e a revisão do conselho externo concluíram que as transferências de dados da Elastic não se enquadram no foco típico das leis de vigilância. Também oferecemos medidas suplementares para proteger os dados transferidos.
- Com base na natureza dos nossos serviços e nas atividades de tratamento de dados, as solicitações das autoridades públicas são extremamente improváveis. A Elastic nunca recebeu uma solicitação da FISA, EO12333 ou Lei CLOUD.
- As SCCs são aplicadas para proteger as transferências de dados de clientes aplicáveis. Quando os dados pessoais originados na Europa são (i) transferidos diretamente para a Elastic por seus clientes, (ii) são transferidos pela Elastic intragrupo entre entidades do grupo Elastic ou (iii) são transferidos pela Elastic para subprocessadores externos, a Elastic entra nas SCCs com essas partes.
- Os dados são criptografados em trânsito e em repouso.
- Os clientes têm a opção de selecionar servidores da UE para nossas aplicações de serviço.
- A Elastic avalia e desenvolve continuamente suas salvaguardas contratuais, técnicas e organizacionais para proteger as transferências de dados.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.

Solicitações de acesso de autoridades públicas

A Elastic estabeleceu políticas e processos para responder às solicitações de acesso de autoridades públicas ao Conteúdo do Cliente. Tais políticas e processos obedecem às leis de proteção de dados aplicáveis e ao seu contrato de cliente.

A Elastic não tem conhecimento de nenhuma lei aplicável que possa afetar sua capacidade de cumprir seus compromissos relativos a solicitações de acesso de autoridades públicas e divulgações exigidas. Em nenhuma hipótese a Elastic divulgará quaisquer dados pessoais de maneira maciça, desproporcional ou indiscriminada que vá além do necessário em uma sociedade democrática.

Não obstante o acima exposto, a Elastic nunca recebeu nenhuma solicitação de autoridades públicas para acesso ao Conteúdo do Cliente, inclusive sob a Seção 702 da FISA. Também não temos conhecimento de qualquer acesso direto ao Conteúdo do Cliente sob a Ordem Executiva 12333.
A Elastic nunca criou um backdoor ou uma chave mestra para nenhum de nossos produtos ou serviços e nunca permitiu que qualquer autoridade governamental tivesse acesso irrestrito ou direto aos nossos servidores.

Proteção de dados pessoais como empresa

Avisos de privacidade

Para obter mais informações sobre como a Elastic coleta, usa, divulga, transfere e armazena informações pessoais no Elastic Cloud, consulte a Elastic Product Privacy Statement (Declaração de Privacidade do Produto da Elastic).

Regulamentações globais de privacidade

A Elastic tem o compromisso de aderir às regulamentações globais de privacidade, incluindo GDPR e CCPA. Para enviar uma solicitação de titular de dados, consulte a seção Como entrar em contato conosco da Declaração Geral de Privacidade. Para obter mais informações sobre como garantir que suas implantações da Elastic sejam compatíveis com o GDPR, acesse A conformidade com o GDPR e o Elasticsearch.

 © 2023 Elasticsearch B.V. Todos os direitos reservados.