Elastic Cloud Information Security Overview

October 2023

elastic.co

TABLE OF CONTENTS

elastic

Services and Scope

With solutions in Enterprise Search, Observability, and Security, we help people find what they need faster, keep mission-critical applications running smoothly, and protect against cyber threats. Elastic Cloud is designed to give you the flexibility to adapt and manage deployments for your specific use case, removing complexity and managing the underlying platform that powers your search experiences with speed, scale, and relevance.

We understand the significant responsibility we have to you, our customers, who rely on us to deliver leading search experiences while protecting your data – we work diligently to earn your trust. Security – from board oversight and executive governance at the top of the organization to how we onboard and continuously train every Elastician – is critical in everything we do. Elastic has obtained an extensive suite of industry leading compliance reports and certifications for the Elastic Cloud service and our Information Security Management System (ISMS). These reports and certifications serve as evidence that effective security practices are inherent in all of our activities, including product development and deployment, vulnerability management, incident management, and threat handling processes.

This document outlines our policies, procedures, and technical controls in place to give you the confidence that you deserve to power your solutions with Elastic Cloud. Elastic Cloud and its related software solutions can be deployed on-premises, in public or private clouds, or in hybrid environments to satisfy various user and customer needs; however, controls for self-managed deployments are out of scope for this document.

Elastic Cloud Overview

Elastic delivers cloud-native enterprise search, observability, and security solutions that enhance customer and employee search experiences, keep mission-critical applications running smoothly, and protect against cyber threats. Elastic products ingest and store data from any source and in any format to perform search, analysis, and visualization.

Elastic Cloud is a family of software-as-a-service (SaaS) products that includes the Elasticsearch Service (ESS), Enterprise Search, Observability, and Elastic Security. Elastic hosts and manages Elastic Stack components, including Elasticsearch and Kibana, on customer-selected infrastructure from multiple public cloud providers, including Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, and IBM. Elastic Cloud offerings include advanced Elastic Stack features, such as security, alerting, monitoring, reporting, machine learning, and visualization capabilities.

More information on the components of Elastic Cloud is provided below.

Elastic Cloud Component	**Component description**
Elasticsearch Service (ESS)	ESS is a distributed, real-time search and analytics engine and datastore for all data types, including textual, numerical, geospatial, structured, and unstructured data.
Enterprise Search	Elastic Enterprise Search provides powerful tools to deliver search experiences quickly while scaling seamlessly: *Workplace Search* is a tool to unify an organization's content platforms (Google Drive, Slack, Salesforce, and many others) into a personalized, natural search experience. *App Search* is a toolbox for developers to leverage the power of Elasticsearch to add search to mobile and SaaS apps, complete with a web crawler, refined APIs, intuitive dashboards, and tunable relevance controls. *Site Search* enables the addition of powerful search capabilities to a website, including the search box if needed.
Observability	Elastic Observability enables unified analysis across logs, metrics, application performance, and uptime monitoring information. Using Elastic Agent and pre-built integration connectors for data collection, organizations can surface outliers

	with machine learning and out-of-the-box detection rules supporting both DevOps and SecOps teams.
Security	Elastic Security enables threat prevention, detection, and response through a single user interface: *Elastic SIEM* provides conventional log aggregation and correlation, supporting threat detection and response, as well as advanced security features like risk assessment with machine learning, integrated case management, and SOAR. *Elastic Agent* offers limitless versatility with a small footprint that works just about anywhere, including hybrid environments. It can prevent threats, forward data, and support multiple use cases to enrich security information and protection. *Limitless XDR* modernizes security operations, unifying SIEM and endpoint security, enabling analytics across years of data, automating detection and response processes, and bringing native endpoint protection to every host.

Cloud Compliance Programs

Elastic Cloud is designed with security at its core. We have achieved and maintain industry leading certifications and attestation reports that demonstrate our commitment to security, compliance, privacy, and reliability.

Elastic's global ISMS has been certified against ISO 27001 and the Elastic Cloud commercial service has been audited or certified against ISO 27017, ISO 27018, SOC 2 Type 2, CSA Cloud Compliance Matrix (CCM), HIPAA, and PCI-DSS. We also have penetration test executive summaries as well as industry and geographic specific certifications (i.e., TISAX) available. For more information on the Compliance Standards we are evaluated against and how to obtain copies of our reports and certifications, refer to the Compliance Standards section of this document.

Additionally, Elastic Cloud is FedRAMP authorized at the Moderate Impact Level in AWS GovCloud. Please visit our FedRAMP authorized cloud offering page to review certification details. Relevant government customers and prospects can obtain access to our FedRAMP Security Packages though the FedRAMP Marketplace using the FedRAMP Package Access Request Form.

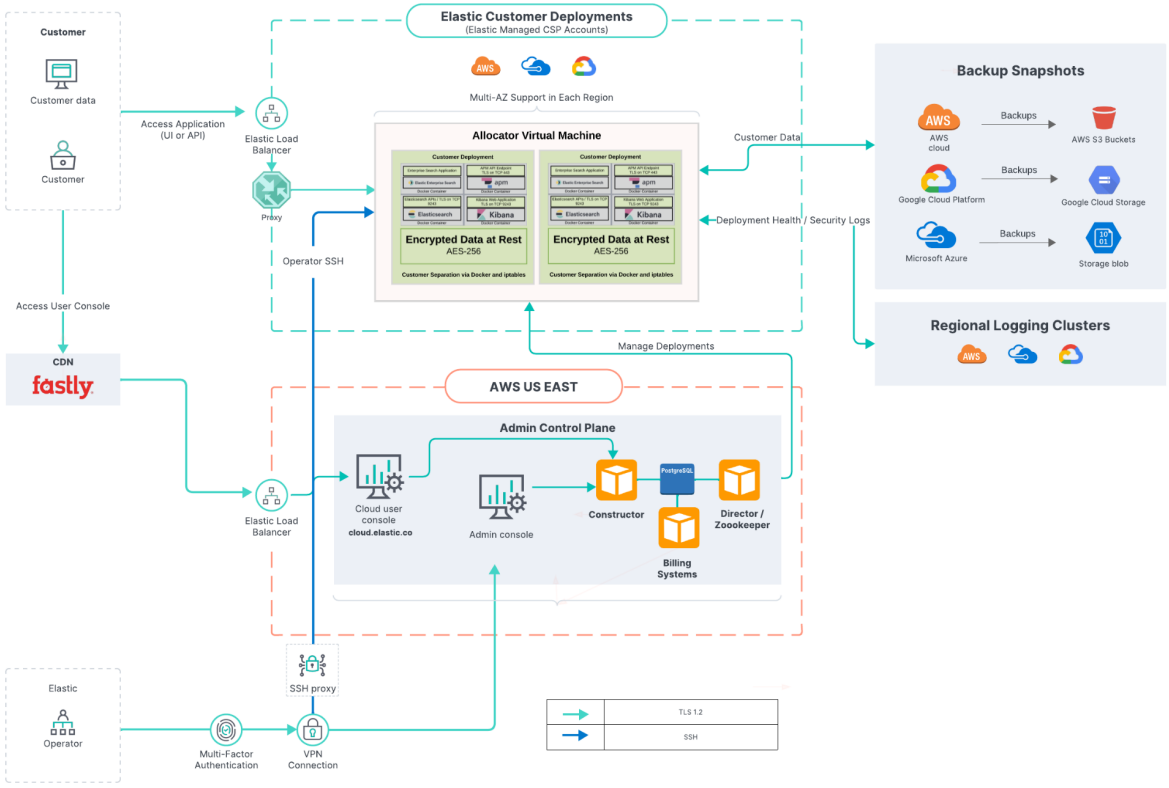
Product Usage Data and Customer Content

We treat our customers' information with the utmost care - the protections described throughout this document are in place to protect Customer Content. The distinction between Product Usage Data versus Customer Content is further explained below.

Product Usage Data: This is the data used by Elastic to facilitate the delivery of our products, manage and monitor infrastructure, provide support, and for product analytics and improvement. Product Usage Data is strictly controlled and protected, and is subject to both internal and external assessments that test the security and integrity of this data. However, this document is focused on how we deploy defense-in-depth to protect Customer Content.

Customer Content: This is the data customers ingest, upload or otherwise submit into Elastic's products and services. Elastic only processes this data as necessary to provide the products or services, and as may be necessary to comply with law. The customer always has full control over what data they ingest into Elastic Cloud.

Elastic Cloud Service Diagram



Elastic Cloud Architecture Description

Control Plane

The Control Plane of Elastic Cloud includes the **ZooKeeper**, **Director**, and **Constructor** management services, explained further below:

- **ZooKeeper** - ZooKeeper is a distributed data store which holds essential information for Elastic Cloud components: Proxy routing tables, memory capacity advertised by the allocators, changes committed through Admin Console, and so on. It acts as a message bus for communication between the services. It also stores the state of the Elastic Cloud installation and the state of all deployments running in Elastic Cloud.

- **Director** - Director manages the ZooKeeper data store and signs the Certificate Signing Requests (CSRs) for internal clients that want to communicate with ZooKeeper. It also

maintains the STunnels ZooKeeper uses for communication and establishes quorum when new ZooKeeper nodes are created.

- **Constructor** - Constructor works like a scheduler that monitors requests from the Admin console. It determines what needs to be changed and writes the changes to ZooKeeper nodes monitored by the allocators. It also assigns cluster nodes to allocators and maximizes the utilization of underlying allocators to reduce the need to spin up extra hardware for new deployments. The Constructor places cluster nodes and instances within different availability zones to ensure that the deployment can withstand any zone failure.

  These placement preferences are customizable for data sovereignty requirements.

- **Cloud UI and API** - These features provide web and API access for administrators to manage and monitor their installation.

Proxies

Proxies handle user requests, mapping deployment IDs that are passed in request URLs for the container to the actual Elasticsearch cluster nodes and other instances. The association of deployment IDs to a container is stored in ZooKeeper, cached by the proxies. In the event of ZooKeeper downtime, the platform can still service the requests to existing deployments using the cache.

They also keep track of the state and availability of zones if you have a highly available Elasticsearch cluster. If one of the zones goes down, the proxy will not route any requests there. Additionally, they help with no-downtime scaling and upgrades. Before performing an upgrade, a snapshot is taken and data is migrated to the new nodes. When the migration is complete, a proxy switches the traffic to the new nodes and disconnects the old nodes. Typically, multiple proxies are configured behind a load balancer to ensure that the system remains available.

Allocators

Allocators run on all the machines that host Elasticsearch nodes and Kibana instances. They control the lifecycle of cluster nodes through:

- Creating new containers and starting Elasticsearch nodes when requested
- Restarting a node if it becomes unresponsive
- Removing a node if it is no longer needed

They also advertise the memory capacity of the underlying host machine to ZooKeeper so that the Constructor can make an informed decision on where to deploy.

Risk Management

Elastic has adopted a risk-based approach to security and compliance, utilizing FAIR - the leading quantitative risk assessment and analysis methodology, to identify and assess risks to the business as well as prioritize risk mitigation activities.

Elastic's risk assessment process identifies and manages risks that could affect our ability to provide trusted and reliable services to our customers. The key risks that we have identified, and are focused on controlling, include:

- Organizational management
- Human resource security
- Asset management
- Access control
- Cryptography
- Secure communications
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management

- Business continuity management

The risk identification process considers both internal and external factors and their impact on the achievement of the objectives.

Identified risks are analyzed through a process that includes an analysis of possible threats and vulnerabilities relative to our business objectives and estimating the potential significance of the risk. The risk assessment process considers how to manage the risk and whether to accept, avoid, mitigate, or transfer the risk. We determine mitigation strategies for the risks that have been identified. The strategies can include designing, developing, and implementing controls, and adopting or revising policies and procedures.

The collective risk identification, analysis and assessment process informs our Risk Register, which are risk scenarios evaluated using the FAIR methodology and ranked based on estimated financial impact to Elastic. The Risk Register is re-evaluated on a semi-annual basis to account for changes to internal and external risk factors, business priorities, and evolving mitigation strategies. This process also drives the risk-based approach in the Information Security Team's reporting to the Audit Committee of the Board of Directors.

Governance

Information Security Management System (ISMS) and Oversight

Elastic has implemented an ISMS which includes policies, procedures, operational structures, and technical controls working in concert to safeguard customer and company data. The ISMS has been certified against ISO 27001 and is organized to comprehensively address all security and compliance domains including Governance, Trust, Risk and Vulnerability Management, Security Architecture and Engineering, Product Security, Threat Detection, and Incident Response.

The Elastic Board of Directors (Audit Committee) provides oversight for the ISMS and regularly meets with the Chief Information Security Officer (CISO) to ensure the Information Security program is operating in alignment with business goals and objectives, adopting industry best practices, and evolving with the dynamic threat landscape.

The Elastic ISMS is reinforced with a dedicated Business Integrity and Privacy Team that closely collaborates with the Information Security Team on organizational solutions that assure adherence to global data laws and regulations.

Information Security Policies

Elastic has developed a comprehensive policy set to govern our Information Security practices, based on industry standards including NIST and ISO 27001, and communicate management expectations across the company. On an annual basis, policy owners review and executive management approves all Information Security policies. Elastic's policies address the following domains:

- Information Security Program
- Acceptable Use
- Risk Management
- Asset Management
- Data Classification
- Record Retention
- Access Control
- Workstation and Server Security
- Security Analysis and Logging
- Vulnerability Management
- Change Management
- Secure Software Development
- Incident Response
- Business Continuity and Disaster Recovery

All Elastic employees are required to attest that they have reviewed and acknowledged the Elastic Code of Conduct as well as Information Security, Privacy and Acceptable Use policies upon hire and annually thereafter.

We do not share the full text of our Information Security Policies externally. However, an Information Security Policies Bundle is available, which includes each policy's Table of Contents and version history to provide clarity on the domains covered in each policy along with evidence of each policy's regular review, update and approval. For a copy of this document, please contact your Elastic Account Representative or Elastic Support.

In addition to formal policies, Elastic maintains playbooks, process documents, and plans for domains that have more specific process requirements or continually evolving best practices such as cloud encryption, certificate and key management, and third party risk management.

Human Resource Management

We recognize that a comprehensive Security program starts with a strong tone at the top and involves every Elastic employee. Our Source Code, Employee Handbook, and Code of Conduct include explicit guidance and ethical standards all Elastic personnel are expected to uphold. Elastic has a zero tolerance policy for anyone found in violation of these commitments, regardless of position, seniority or tenure.

Elastic has also established entity-level security best practices with formal lines of reporting, which facilitate the flow of information to relevant personnel and ensure appropriate accountability and oversight of employee conduct and performance. Roles and responsibilities are segregated based on functional requirements and job roles are explicitly defined.

All hiring and termination is performed in accordance with documented policies and procedures, which includes procedures for safely and promptly onboarding and offboarding employees and contractors.

Other entity level security practices include performing background checks on new hires and contractors prior to onboarding. In addition, all Elastic employees, including executives and senior management, must complete security awareness training and review and acknowledge information security and privacy policies, the Code of Conduct, and the Employee Handbook upon hire and annually thereafter.

Asset Management

The Asset Management Standard governs the asset management lifecycle, which includes an asset inventory, asset ownership, return and disposal of assets, and audit trail requirements. Asset management processes between fleet management and endpoint management are distinct. Each independent process is explained below:

Fleet

Our partner Cloud Service Providers (CSP), AWS, GCP, Azure, and IBM manage the infrastructure powering Elastic Cloud . Elastic Cloud customers have the flexibility to choose the underlying CSP and geographical region for their data on a per-deployment basis. Physical security, media and hardware controls are the responsibility of the CSP. Elastic reviews the design and operational effectiveness of our partner Cloud Service Providers' media and hardware lifecycle management controls during third party recertifications which are conducted as part of our Third Party Risk Management program.

Elastic Clusters utilize Elastic Observability to track performance and uptime metrics. Critical assets are registered in our asset inventory and the asset inventory is regularly reviewed for completeness and accuracy.

Employee Endpoints

Elastic IT centrally tracks and manages employee endpoints. Device management software is utilized to enforce security settings including encryption, password management, session management and

screen locking, which are enabled by default. These settings cannot be disabled or modified locally. Endpoints are protected with Elastic Security which provides EDR capabilities and real time monitoring and alerting. Refer to the Malware Security section for more information on how we protect employee endpoints from malware.

All Elastic issued devices are handled in accordance with our device management lifecycle. When an Elastic employee is terminated, logical access is disabled and company managed endpoints are sent directly to a third party processor which performs data sanitization and destruction procedures. Our third party partner provides Elastic with certificates of destruction and re-issues or disposes of the machine based on the Elastic Laptop Handling Standard. Elastic IT maintains an audit trail of Elastic managed endpoints to track each device's status within the data destruction lifecycle.

By policy, unmanaged or personal mobile devices cannot store customer data and are not used in the development or support of Elastic Cloud.

Configuration Management

Elastic manages configuration through code, and configuration changes follow the standard change management procedure which includes authorization, peer review and approval, and automated test suites. Elastic monitors for direct changes to production configuration files through File Integrity Monitoring and suspicious activity detections.

Data Protection

Data Classification and Retention

The Elastic Data Classification Standard requires that data is classified based on sensitivity, with access and sharing restrictions defined for each classification. Customer Content and Product Usage Data is classified as restricted - the most sensitive classification - and is subject to the strongest data protection standards designed to preserve the confidentiality, integrity, and availability of this data.

For definitions of Customer Content and Product Usage Data, refer to the Product Usage Data and Customer Data section of this document.

The Elastic Record Retention Standard requires that data is disposed of in accordance with defined retention schedules based on data type and operational, contractual, legal and regulatory requirements. Customers may submit an account deletion request with Elastic Support at any time to have their information deleted. For information on how to submit a Data Access Request, refer to the Data Privacy section of this document.

Data Collection, Handling and Disposal

Data Collection

Elastic only collects the information necessary to provide, support, maintain, secure, and improve our services. This information is never sold to third parties. For more information on the information we collect from customers, refer to our Product Privacy Statement.

Data Ingestion

Elastic does not control or access the data customers choose to store, transmit, or process on their Elastic deployment. Any data ingested by a customer's Elastic deployment is at their sole discretion and under their control at all times.

Data Destruction

The Elastic Record Retention Standard and Asset Management Standard governs data destruction requirements. Our Cloud Service Provider partners manage secure deletion and data destruction for hosting infrastructure. Customers retain full control over the content they store in their Elastic instances and have the right to remove or delete any content from their Elastic instances at any time.

Encryption

Encryption In-Transit

Encryption in-transit for Elastic Cloud is enforced by default through Transport Layer Security (TLS). The minimum accepted cipher strength is TLS 1.2. TLS (HTTPS) connections are displayed in the Elastic Cloud Service Diagram.

Certificates used to support Elastic Cloud are provided by Digicert and utilize RSA public-key authentication with 2048 bit keys. Elastic maintains valid certificates for our Cloud deployments and they are rated A+ by Qualys SSL Labs. These test results can be reproduced by visiting SSL Labs.

Encryption At-Rest

Our Cloud Service Provider partners provide encryption at-rest, which is enabled by default. All of our cloud providers feature minimum key lengths in line with NIST guidelines (256-bit).

Key Management

Encryption Keys never leave the host where they are generated and are considered disposable. They are automatically generated whenever a virtual machine host is created or replaced. They are never backed up, exposed, or leave the host. Key Management for encryption in the underlying IaaS services is automated using the Key Management Service of the provider.

Key Management for Elastic services is maintained as Infrastructure-as-Code and as part of the operational documentation for each applicable component or service.

Network and Device Security Management

Firewalls

Our Cloud Service Provider partners manage the hardware firewalls for production infrastructure. Elastic also maintains software firewalls to filter unauthorized inbound traffic from the internet and deny incoming network connections that are not explicitly authorized (deny-by-default). Further network segmentation and firewalling is in place between logical zones within the environment. Firewall rulesets are reviewed at least semi-annually. Changes to firewall rules follow the standard change management process and are subject to change management controls. In addition, all access to firewalls is implemented using RBAC.

Elastic Cloud customers can utilize traffic filtering functionality or configure PrivateLink to further restrict traffic to their deployments.
IP traffic filters | Elasticsearch Service Documentation | Elastic
AWS PrivateLink traffic filters | Elasticsearch Service Documentation | Elastic

Malware Security

Anti-malware is enabled on all employee endpoints through centrally managed IT configurations. Local admins cannot disable or modify these settings. Elastic Security Solution provides EDR capabilities and a 24/7 on-call team within Information Security reviews and actions alerts.

Elastic Security is utilized to protect the Elastic Cloud production environment. Signatures and behavior patterns are updated automatically and continuously. Detections can be deployed against emerging threats rapidly and a dedicated Threat Intelligence, Detections and Response team manages detection, analysis, response, and remediation of possible malware infections.

Time Synchronization

Time synchronization is achieved through NTP with a common time source (NIST servers).

Logical Access

Role-Based Access Control

Elastic adheres to the Principle of Least Privilege when provisioning access to internal users. Elastic employees are only granted the level of access that is necessary for their job role. Access rights are regularly reviewed and modified in the event of a job change or other circumstances where a user's access is no longer needed.

Elastic products also feature role-based access control to enable our customers to implement fine-grained access management for users within their Elastic deployments and the Elastic Cloud management platform.

Onboarding and Termination

New hires are automatically provisioned access to corporate cloud-native SaaS applications based on pre-configured rules in our centralized Identity and Access Management (IAM) system. Automatic provisioning rulesets utilize job attributes from our HR system of record, such as supervisory organization, job family, job level, and management structure to grant specific access that is needed for that individual user. Any access beyond this requires a formal request documented in a ticket and is subject to management review and approval.

If an employee transfers to a different job role or organization within Elastic, the changes in their job attributes within the HR system of record will automatically initiate the workflow within the centralized IAM system to re-provision their account with the appropriate access for their new role. The access entitlements from their prior role are de-provisioned and new access is provisioned based on the job attributes of their new role.

Upon termination, access granted through our centralized IAM system is automatically suspended when their employment status changes in our HR management system. This validation check occurs multiple times a day.

Production Access

A limited number of Elastic employees have been granted privileged access to our Elastic Cloud production environment. Elastic maintains this access for platform management, maintenance, and support purposes. The Elastic Data Handling policy expressly prohibits Elastic employees from accessing customer data even in maintenance or troubleshooting scenarios. Customers must give their written consent prior to an Elastic employee viewing any data that has been voluntarily shared for support or troubleshooting purposes. Elastic does not proactively view customer data uploaded to or ingested into Elastic Cloud. Customers can choose to redact or sanitize data prior to sharing with Elastic.

In addition, the Information Security Threat Detection and Response team has developed and implemented detections for suspicious internal account activity and unauthorized access, including file integrity monitoring and indicators of account takeover or data exfiltration. These detections are part of automated workflows which alert the Threat Detection and Response of suspicious activity and trigger analyst investigation.

User Access Reviews

Elastic adheres to the principle of least privilege and only authorizes access that is required for the performance of each job role. System owners and management review and re-cerity user access, including privileged access, during Quarterly User Access Reviews. Access that is no longer required is de-provisioned.

Change Management

The Change Management Standard governs change management processes and establishes requirements designed to control the development and deployment of software and infrastructure changes to the production environment in a safe and managed way.

The change management process ensures that proposed changes are authorized, peer reviewed, tested, implemented, and released in a controlled manner, and that the status of each proposed change is documented and monitored. In the event that an emergency change is necessary, documented approval and automated testing is still required. A manual review of the emergency change is also required, but may occur after implementation.

Supply Chain Security

Software deployments to production environments are managed via automated CI/CD pipelines. Changes are stored in designated branches within each respective repository. Development branches are used for active development and main branches contain production ready code. Changes are version controlled and prior to merging to the main branch, a series of automated tests, including security checks, are performed. Branch Protections are enabled which require test suites to pass before the change is authorized to merge to the main branch. When a change is fully authorized - tests and security checks have passed, peer review and approval is obtained, and integration checks have passed - automated deployment software pushes the change to production without the need for manual intervention.

Our source code is stored in an access controlled and monitored version control system. User activity is captured in audit longs and detections are in place to alert upon unexpected or suspicious modifications and build processes. The ability to modify code within each repository is restricted based on job roles.

Secure Development

SDLC

Security requirements for our Systems Development Life Cycle (SDLC) is maintained in the Secure Software Development Framework. This framework dictates the process to securely design, develop, deploy, track, and maintain all Elastic software. It also includes requirements to protect our build systems and mitigate the risks of build chain compromise. Build systems include software delivery pipelines, package registries, artifact repositories, CI/CD, and source code management systems. The

Secure Software Development Framework prohibits using production data for testing and in non-production systems. It also requires separation of production and non-production environments. Environmental segmentation is assessed during third party penetration testing.

Secure Design and Architecture

Elastic software development follows security best practices in design and architecture to produce software that is “secure by-design” and “secure by-default.”

The Secure Software Development Framework outlines the data protection requirements and security principles all designs should follow, including:

- Confidentiality - Data is protected from unauthorized observation or disclosure both in-transit and when stored.
- Integrity - Data is protected from unauthorized creation, alteration, or deletion.
- Availability - Data is available to authorized users as required and meets any defined availability SLAs.
- Identification, Authentication, Authorization
- Non-Repudiation
- Auditing and Logging
- Access Control and Principles of Least Privilege
- Secure Communications and Encryption Standards
- Secure Defaults and Fail-Safe / Fail-Secure

Threat modeling and Security Architecture reviews are also part of the software development process to ensure the design has taken account of required security principles.

Secure Coding

As a SaaS provider, we recognize the importance of secure coding practices. Common coding vulnerabilities such as the OWASP Top 10 and CWE Top 25 are addressed in Secure Software Development Training which is issued to relevant teams and individuals on an annual basis. Changes to source code require a review and approval (via merge request) from at least one reviewer, who was

not the author of the change, before merging changes. Changes are reviewed to identify potential security impacts the change may introduce. Additionally, independent penetration testing, which includes secure code review, places added emphasis on common unsafe coding practices. Any issues identified during threat modeling, security review, or source code review are tracked, assessed, and remediated based on assessed risk in accordance with the Vulnerability Management Standard.

Elastic also sponsors a bug bounty program as part of our efforts to maintain secure software and protect our customers from vulnerabilities. For more information, refer to the Vulnerability Disclosure Program in the Vulnerability and Patch Management section.

Open Source and Third Party Software Review

The Secure Software Development Framework requires that code dependencies from open source and third party libraries are identified and tracked. Dependency management software is in place to assist with identification, scanning, and remediation of vulnerable dependencies.

Vulnerability and Patch Management

The Vulnerability Management Standard governs the vulnerability management program and sets requirements for scanning Elastic resources as well as the triage, analysis, remediation, and disclosure of vulnerabilities. Elastic performs vulnerability scans and applies patches to both the infrastructure powering Elastic Cloud as well as Elastic Cloud components themselves. The processes for each are detailed below.

Infrastructure Vulnerability and Patch Management

Elastic utilizes a commercial vulnerability scanner to scan our assets on a continuous basis. All production assets are included in these scans. The third party software vendor updates rulesets on a continuous basis. Severity of vulnerabilities are based on CVSS ratings and patching timelines also correspond with CVSS ratings. Critical and High vulnerabilities are prioritized for patching immediately, or as part of the next scheduled release.

Product Vulnerability and Patch Management

We rigorously test our products for security vulnerabilities through third party penetration testing, automated and manual code scans and reviews, OSS scans, segmentation testing, and through our vulnerability disclosure program. When a vulnerability is discovered in an Elastic product, Elastic will evaluate it in accordance with the Vulnerability Management Standard to determine severity and a remediation plan. If necessary, we will issue an Elastic Security Advisory (ESA.) This is a notice from Elastic to its users of security issues with the Elastic products. Elastic assigns both a CVE and an ESA identifier to each advisory along with a summary and remediation and mitigation details. All new advisories are announced in the Security Announcements forum.

The Vulnerability Management Standard also governs publishing disclosures. The Disclosure process includes releasing a new product version, if necessary, and issuing an announcement on the Advisory page. Depending on the nature of the vulnerability, we will also contact individual customers, publish a blog post, and/or submit the CVE to MITRE.

Customers may track ESAs via an RSS feed.

Vulnerability Disclosure Program

Elastic is proud to sponsor a public Vulnerability Disclosure Program through which security researchers may responsibly submit vulnerabilities for internal review. The Elastic Product Security Team reviews submissions, assesses risk exposure, and remediates based on the assessed risk. Please visit the Elastic Bug Bounty Program on HackerOne for our Bug Bounty Policy or to submit a report.

Third Party Risk Management

Third Party Onboarding

All third parties including sub processors are subjected to a thorough intake and review process. Each vendor's risk profile is evaluated based on the service they are providing, the types of data they will handle, the level of access they will have to internal systems, and other factors that capture the criticality and risk profile of the vendor.

Based on the risk profile of the vendor and the types of services they will provide Elastic, a review workflow is executed. All vendors who will have access to sensitive information, access to internal systems, or provide a critical technology service require additional scrutiny including, but not limited to, Information Security, Legal, and Privacy review. This additional scrutiny includes reviewing the security practices, security certifications, and compliance reporting of third parties. Compliance with laws in the country where the data is processed, stored, and transmitted is taken into account, and where deemed necessary, Elastic may seek additional security requirements in third party agreements.

Elastic also has a published Vendor Code of Conduct which documents the ethical requirements expected of our vendors and partners. It includes, but is not limited to, Ethics and Compliance, Employee Health and Safety, Human and Labor Rights, and Environmental Stewardship requirements.

Third Party Recertification

A continuous Third Party Information Risk Management process is in place to conduct recertification of existing vendors. Third Parties are classified based on risk level and the Elastic Information Security team reviews the security practices of third parties in accordance with the requirements in place for each risk level.

All of the Cloud Service Providers who provide infrastructure services for Elastic Cloud are reviewed and recertified at least annually. The recertification process involves reviewing a vendor's risk profile

and examining vendor security and compliance reporting to ensure expected security and compliance controls adequately cover the services we consume and that the controls are designed and operating effectively.

Threat Detection

Monitoring and Alerting

We utilize Elastic Security as our SIEM solution, which enables us to rapidly develop and deploy detections for emerging threats and attack patterns, as well as suspicious behavior detections, file integrity monitoring detections, and common malware behavior patterns. Monitoring of our environments is conducted on a real time basis through our automated detections. Pre-configured altering workflows are in place to notify the appropriate Elastic personnel in the event of suspicious indicators. Our 24/7 on-call Threat Detections and Response Team investigates and actions these alerts.

Certified and continuously trained staff handle security events and incidents in accordance with our Incident Response Standard and Incident Response plan. For more details on the incident management process, refer to the Incident Response section of this document.

Log Management and Retention

We utilize Elasticsearch as our log management solution. We are able to ingest and centralize logs from various sources including detection engines, our IaaS providers, vulnerability management tooling, cloud admin console, and more, to develop robust logging, auditing, and forensic abilities. Our logs are access controlled to prevent tampering and edit access is restricted to Security Engineering based on least privilege. In addition, automated detection and alerting, including file integrity monitoring, protects our logging systems and notifies the Threat Detection and Response Team of suspicious activity in near real time.

Logs are retained in accordance with our Data Retention Standard based on business, legal, and contractual requirements. Customers interested in submitting a Data Access Request can refer to the Data Privacy section of this document.

Incident Response

Elastic Information Security has a 24/7 Threat Detection and Response Team dedicated to managing security events and incidents. The Incident Response Standard governs the incident response function and dictates event identification, event handling, reporting, and training requirements. The separate Incident Response Plan details how to prepare for, detect, analyze, contain, eradicate, recover from, and report on security incidents. Trained incident responders, who regularly exercise and test the Incident Response Plan, handle all incidents. Incidents also require a documented after actions report and lessons learned exercise.

In the event that we detect a breach or become aware of unauthorized access to systems or data, Elastic Legal and Information Security will issue customer communications as required by law or in accordance with contract terms and without undue delay.

If a security incident requires reporting to an external regulatory or industry entity, the Elastic Incident Response Plan includes detailed instructions on our reporting obligations, based on the scenario at hand. The Plan also designates a formal Computer Security Incident Response Team (CSIRT) with documented roles and responsibilities to ensure proper communication to and from appropriate individuals.

Reliability

Availability and Status

High Availability architecture is available and recommended on Elastic Cloud with an enhanced SLA. Please discuss this option with your Account Team if this is something you would benefit from. Real-time and historical data on Elastic Cloud service performance is available at Elastic.

Business Continuity and Disaster Recovery

Elastic maintains comprehensive Business Continuity and Disaster Recovery plans, in addition to the Business Continuity and Disaster Recovery Standard, to prepare for, respond to, and recover from disasters.

Elastic is a globally distributed company and has been since our inception. Employees are fully equipped to work remotely and globally distributed teams are staffed with geographic redundancy in mind. Elastic offices do not contain any infrastructure or IT systems that are required for employee connectivity or for providing Elastic services and support to our customers.

Elastic maintains Disaster Recovery plans for Elastic Cloud, which are tested on at least an annual basis. Tests are unique with a defined focus area each year to identify knowledge gaps and weaknesses in our technical recovery capabilities. RTO and RPO are tracked and documented for each test to ensure our recovery is able to meet internally definition criteria. Disaster Recovery tests are thoroughly documented with scenario details, a timeline of events, and action items for improvement.

Independent Assessments

Penetration Testing

Elastic recognizes the strength and importance of defense in depth, taking into consideration personnel security, lateral movement, privilege escalation, and persistent threats. With this in mind, Elastic engages with multiple independent penetration testing service providers to perform network and application layer penetration testing, segmentation testing, and secure code review. Penetration testing is performed at least annually. Findings from penetration tests are remediated based on criticality. Penetration test results are also reported to senior management to facilitate cross-functional alignment and accountability in remediating findings and implementing additional preventative and detective controls where necessary. Penetration test summary reports and remediation status reports are available to customers upon request.

In addition to independent penetration testing, Elastic sponsors and maintains a formal Vulnerability Disclosure (Bug Bounty) Program. Security researchers are encouraged to report vulnerabilities through our Vulnerability Disclosure Program. The Elastic Product Security Team triages and remediates submissions based on criticality. For more information on our Bug Bounty Policy or to submit a report, visit our Bug Bounty Program on HackerOne.

Compliance Standards

Elastic is committed to pursuing and maintaining security and compliance certifications and attestations that provide the most value to our customers. We take seriously the trust our customers put in us to power their search, observability, and security needs in highly regulated industries and regions around the world. For the full list of certifications and attestations Elastic Cloud offers, please visit Elastic Security and Compliance.

Data Privacy

At Elastic, data privacy plays a critical role in earning and maintaining customer trust. We're committed to providing our customers with transparency about how we process and secure your data in Elastic Cloud.

Data Hosting

Elastic uses Cloud Service Providers, such as Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) to provide Elastic Cloud. We support hosting options globally through each of our Cloud Service Providers. Customers are able to select the region where they would like to host their Elastic Cloud deployment to best meet their data sovereignty needs. Backups are also configured to retain customer backups in their selected region.

Contractual Commitments

Elastic has built processes, organizational structures, and technical measures throughout our company to ensure we meet global privacy principles. These commitments are backed by the

contractual privacy terms we make available to you in our Customer Data Processing Amendment ("DPA") for Elastic Cloud.

Elastic regularly reviews and updates our DPA to reflect applicable data privacy requirements, including the following provisions:

- You own your data. Our processing of personal data is only carried out on your instruction.
- The data that we process is subject to applicable legal data protection requirements.
- We have implemented and are contractually committed to appropriate technical and organizational measures, which include the standard contractual clauses pursuant to European Commission Decision 2021/914/EU ("SCCs") when applicable.
- All personnel authorized to process personal data are subject to stringent confidentiality policies and procedures.
- Customers are notified of requests from data subjects. Elastic will not respond without customer consent, and will assist customers in meeting their requirements in responding to such requests.
- Elastic is obligated under the SCCs to notify its customers in the event it is made subject to a request for access to customer personal data from a government authority. In the event that Elastic is legally prohibited from making such a disclosure, Elastic is contractually obligated under the SCCs to challenge such prohibition and seek a waiver.
- Elastic utilizes confidentiality agreements and employee training programs to ensure any personnel involved in processing personal data maintain confidentiality. These agreements extend beyond the conclusion of an employee's tenure with Elastic.
- Elastic's sub-processors are subject to the same standards and organizational requirements. Elastic is liable for the acts and omissions of its sub-processors to the same extent if we were performing the services ourselves.

Sub-Processors

Elastic uses certain external service providers and internal affiliates to provide Elastic Cloud which may require processing customer personal data (as sub-processors) strictly as necessary to provide services to you.

The external sub-processors currently engaged by Elastic are as set forth at https://www.elastic.co/agreements/external_subprocessors and the internal sub-processors are as set forth at https://www.elastic.co/agreements/internal_subprocessors.

International Data Transfers and Schrems II

Elastic is a global company and may transfer data from the EEA and UK to third countries to Elastic's non-European personnel, as well as to those third-party organizations that are necessary to provide our services. These locations are set forth in the sub-Processors section above. In such cases, Elastic relies on the SCCs including the controller-processor module with its customers and the processor-processor module with its sub-processors, in addition to robust supplementary measures. Elastic has reviewed the EDPB guidance regarding supplementary measures for international data transfers post-Schrems II. Taking into account Elastic's practical experience, the low likelihood of government interest in the personal data Elastic processes, as well as the safeguards Elastic puts in place to protect customer personal data, Elastic does not consider that its processing of customer personal data outside of Europe presents a risk to individuals' rights preventing Elastic from fulfilling its obligations as the "data importer" under the SCCs.

- Internal analysis and external counsel review has concluded that Elastic data transfers do not fall within the typical focus of surveillance laws. We also offer to provide supplementary measures to protect any data transferred.
- Based on the nature of our services and data processing activities, public authority requests are extremely unlikely. Elastic has never received a FISA, EO12333, or CLOUD Act request.
- The SCCs are applied to protect applicable customer data transfers. Where personal data originating in Europe is (i) directly transferred to Elastic by its customers, (ii) is transferred by Elastic on an intragroup basis between Elastic group entities, or (iii) is transferred by Elastic to external sub-processors, Elastic enters into SCCs with such parties.
- Data is encrypted in-transit and at-rest.
- Customers have the option to select EU servers for our service applications.
- Elastic continually assesses and develops its contractual, technical, and organizational safeguards to protect data transfers.

Public Authority Access Requests

Elastic has established policies and processes for responding to public authority access requests for Customer Content. Such policies and processes adhere to applicable data protection laws and your customer agreement.

Elastic is not aware of any applicable law that would impinge on its ability to comply with its commitments relating to public authority access requests and required disclosures. In no event will Elastic disclose any personal data in a massive, disproportionate, or indiscriminate manner that goes beyond what is necessary in a democratic society.

Notwithstanding the above, Elastic has never received any requests from public authorities for access to Customer Content, including under Section 702 FISA. We are also not aware of any direct access to Customer Content under EO 12333. Elastic has never created a backdoor or master key for any of our products or services and have never allowed any government authority unfettered or direct access to our servers.

Protecting Personal Data as a Business

Privacy Notices

For more information on how Elastic collects, uses, discloses, transfers, and stores personal information in Elastic Cloud, please refer to our Product Privacy Statement.

Global Privacy Regulations

Elastic is committed to adhering to global privacy regulations, including GDPR and CCPA. To submit a Data Subject Request, please view the How to Contact Us section of the General Privacy Statement. For more information on how to ensure your Elastic deployments are GDPR compliant, visit Elasticsearch GDPR and Elastic Stack GDPR Compliance.

