elastic

Search. Observe. Protect.

Keeping data actionable in a Zero Trust Architecture

Level setting on Zero Trust

It can be difficult to understand how to implement Zero Trust in your ecosystem because it is not a single architecture, but a set of guiding principles for workflow, system design, and operations that can be used to improve security posture — recognizing that threats exist both inside and outside traditional network boundaries. It is based on the premise that trust is never granted implicitly but must be continually evaluated, often coined as “never trust, always verify”. **According to NIST**, the critical action to take with Zero Trust is to establish an end-to-end approach to enterprise resource and data security that emcompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and interconnecting infrastructure.

Continual evaluation that’s cost-effective

In order to continually evaluate or “always verify” your ecosystem, it’s essential to capture contextual, time-stamped information about user, device, and tool integration activities and have the ability to evaluate this information in perpetuity. This translates to massive amounts of data being captured, and traditionally it follows that data storage costs become untenable. Not with Elastic.

Elastic is a search-based platform that helps customers achieve data-dependent use cases like event log management and endpoint security. Here is how we break down continual evaluation:

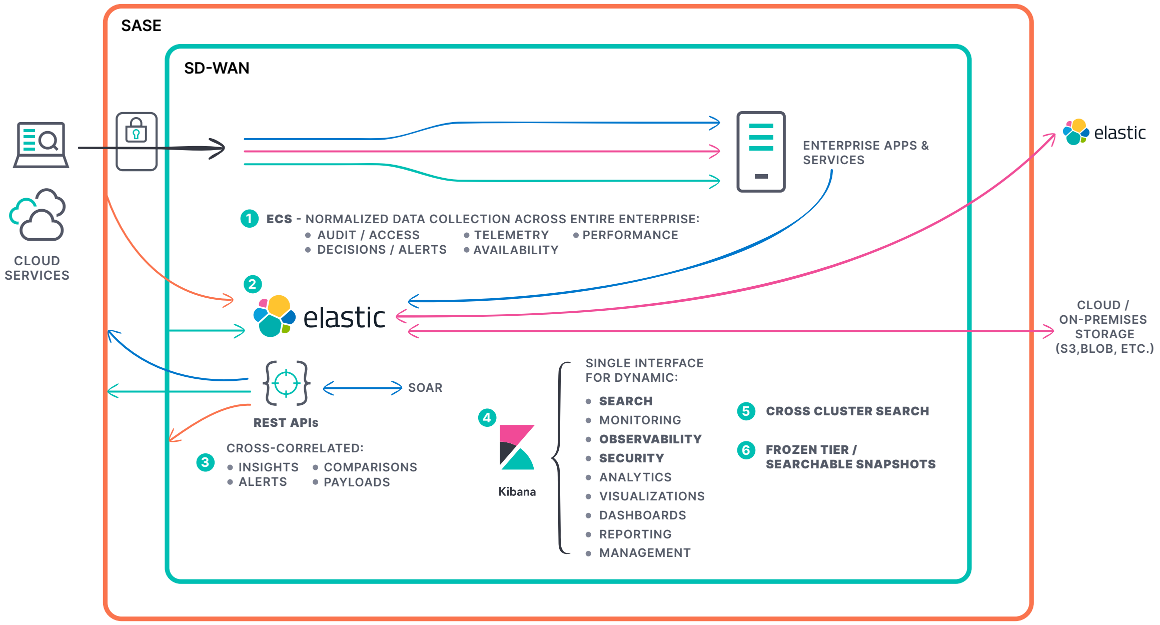
- **Log everything**
  Ingest user, device, and tool integration **telemetry** from your ecosystem — whether you are in a hybrid, multi-cloud, or air-gapped environment— and perform interactive or automated analysis of your data in context to identify correlation and causation.

- **Store data affordably**
  Oversee your data lifecycle management easily with data tiering. Be sure to leverage **frozen tier data storage** to retain older data, where storage costs are 90% less than hot or warm tiers and 80% less than the cold tier.

- **Keep data actionable**
  Use **searchable snapshots** to query frozen-tier data without having to rehydrate it. Query five years worth of data in just seconds. Leverage out-of-the-box features such as machine learning to automate detections so that analysts can focus on mission.

The Elastic Search platform

The diagram below illustrates how Elastic helps you log everything, store data affordably, and keep data actionable in a Zero Trust Architecture.


SASE
SD-WAN
CLOUD SERVICES
ENTERPRISE APPS & SERVICES
elastic
1 ECS - NORMALIZED DATA COLLECTION ACROSS ENTIRE ENTERPRISE:
• AUDIT / ACCESS • TELEMETRY • PERFORMANCE
• DECISIONS / ALERTS • AVAILABILITY
2 elastic
CLOUD / ON-PREMISES STORAGE (S3,BLOB, ETC.)
REST APIs
SOAR
3 CROSS-CORRELATED:
• INSIGHTS • COMPARISONS
• ALERTS • PAYLOADS
4 Kibana
SINGLE INTERFACE FOR DYNAMIC:
• SEARCH
• MONITORING
• OBSERVABILITY
• SECURITY
• ANALYTICS
• VISUALIZATIONS
• DASHBOARDS
• REPORTING
• MANAGEMENT
5 CROSS CLUSTER SEARCH
6 FROZEN TIER / SEARCHABLE SNAPSHOTS

1. **Data collection** of all types from all layers of the enterprise — cloud/infrastructure, network, services, sensors, endpoints, applications — unified via the **Elastic Common Schema.**

2. All data ingested into an exceptionally fast, scalable **search platform** that provides unified multi-modal query, aggregations, and analytics with advanced features like unsupervised machine learning, alerting, and data access management.

3. All data access and analytic functions are available via **REST-based APIs** that can provide cross-correlated, bi-directional insights across layers and systems, and generate automated actions for better programmatic and human-driven decision-making.

4. All data is available to discover, visualize, and analyze through **Kibana**, including several purpose-built solutions for **Search**, **Observability**, and **Security**. Users are not locked into any predetermined workflow and can pivot their inquiry across solutions at the speed of thought. The same data is available (through RBAC/ABAC security controls) as a single source of truth for any use case — the user brings their use case to the data, rather than bringing the data to the use case.

5. Remotely connect to existing enterprise assets running Elastic via **Cross Cluster Search** to provide real-time distributed data access with all the same analytic capabilities everywhere.

6. Store data affordably with **Frozen Tier**, and then query massive amounts of data in just seconds using **Searchable Snapshots**.

Next steps with your Zero Trust use case

As you navigate Zero Trust, our team is here to help. Whether you need to continually evaluate your ecosystem or meet **Executive Order 14028 requirements**, Elastic experts are only a click away. **Get in touch at federal@elastic.co or visit us at elastic.co/industries/public-sector.**