



# Does your Zero Trust strategy have a unified data access layer?

Connecting and operationalizing pillars to speed Zero Trust adoption and lower costs.

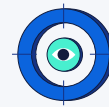
# Table of Contents

<b>Zero Trust requires real-time data</b>	<b>4</b>
<b>3 must-haves for a Zero Trust data layer</b>	<b>5</b>
<b>Elastic unifies data and adds value to each Zero Trust pillar</b>	<b>6</b>
Identity	8
Devices	9
Network & environment	10
Applications & workloads	11
Data	12
<b>Data mesh is key for Zero Trust</b>	<b>13</b>
<b>Data, analytics, and orchestration</b>	<b>14</b>
<b>Real-world applications and success stories</b>	<b>15</b>

With mounting regulatory pressures and increasing cyber threats targeting the public sector, adopting Zero Trust is no longer optional. Regulations such as the CISA Zero Trust Maturity Model (ZTMM), the EU NIS2 Directive, and Australia's Essential Eight are not only recommending but in some cases mandating Zero Trust frameworks for government agencies and organizations.

But can agencies buy their way into a comprehensive Zero Trust strategy with one fell swoop? It's a common misconception. New technology is often needed to fill capability gaps, especially when moving to a new philosophy like Zero Trust. But in most cases, the "one-size-fits-all" or "all-in-one" solutions tend to overcomplicate operations, slow progress, introduce new gaps, add complexity, and increase costs.

Zero Trust is not a single product, but a strategic approach that requires integrating multiple tools, policies, and processes to be truly effective. To make it work, agencies must maximize their existing tools and reduce duplication, improving overall efficiency. A critical first step is data unification. It often becomes the top priority for chief data officers (CDOs) and chief information security officers (CISOs).



**What cyber threats  
should you be on the  
lookout for?**

Find out in the [Elastic  
Global Threat Report](#)

# Zero Trust requires real-time data

A common, unified data layer serves several purposes in a Zero Trust implementation:

- ✓ It makes Zero Trust policy decisions easier by providing a common data layer to integrate with.
- ✓ It allows the centralized monitoring and reporting of events, decisions, and related activities to Zero Trust.
- ✓ The unified data layer can be used to validate and cross-correlate access decisions and activities detected at various layers of the organization.

Without a common shared data layer, each Zero Trust tool effectively creates its own new silo of data that will either force a swivel-chair approach for analysts or introduce fragility through custom tool-to-tool integrations.

Or in other words, this unified data platform can essentially serve as the glue that connects all your systems, making them more integrated, accurate, and trustable because they're all working off "the same sheet of music." Ideally, you'll want a platform that can scale with increasing amounts of data (which is inevitable in Zero Trust architecture) without running up costs. At the same time, you need a solution that's agile enough to adapt to mission variables and strategies.

In order to continually evaluate, or "always verify," your IT ecosystem, it's essential to capture contextual, time-stamped information about user, device, and tool integration activities and have the ability to constantly evaluate this information in near real time. This typically translates to massive amounts of logging and behavioral data being captured, and the traditional big data problems (of data findability vs. scalability vs. cost) will inevitably follow (not to mention the unnecessary costs for duplication of data across teams and tool silos).

# 3 must-haves for a Zero Trust data layer

In order for a unified data layer to be as effective as possible in a Zero Trust context, it must have:



## The ability to ingest everything

Agencies should capture user, device, and tool telemetry from on-premises, hybrid, multi-cloud, or air-gapped environments — performing interactive and automated analyses of all data in context.



## Affordable data storage

Storing massive data volumes is inevitable under Zero Trust. Using tiered storage and capabilities like Elastic's searchable snapshots helps control costs while retaining the ability to query historical data quickly.



## Fast access to all your data

Data must be searchable and correlated in near real time from a single query interface. Fragmented or duplicated data sources risk missing crucial signals.

# Elastic unifies data and adds value to each Zero Trust pillar



Analyze identity events, activities, and behaviors to detect threats or anomalies and enforce Zero Trust automatically.



Dynamic feedback loop continuously collects and analyzes data, using ML to monitor and secure endpoints, even in disconnected environments.



SOAR automation and ingestion is enabled, correlating network logs to reduce blind spots, detect threats, and enforce microsegmentation.



Collect real-time logs, metrics, and traces from apps, enforcing Zero Trust to isolate threats and adjust policies.



Universal visibility, analytics, automation & AI. Retain multi-year logs for compliance and forensics while lowering costs.



Unified datastore that integrates all security data, with an API-first design for easy automation and system orchestration.



Supervised and unsupervised machine learning, enabling seamless data access for diverse analytics needs.



## Unified data layer with end-to-end visibility and analytics



### Identity

- Inventory
- User access
- Behavioral & context



### Devices

- Detection and compliance
- Device auth EDR/XDR



### Network & Environment

- SDN event logging
- Firewall/NAC
- Netflow/network audit



### Apps & Workloads

- Application inventory
- SSD/DevOps
- Continuous monitoring



### Data

- Data tagging
- Data monitoring
- Access control



### Automation & Orchestration

- Machine learning/AI
- API integration
- SOC/IR



### Visibility & Analytics

- SIEM
- Log all data
- EUBA/RMF

Data is the link that connects all the pillars of Zero Trust. Unifying data generated by each pillar is key to effective Zero Trust operations.



Elastic is a distributed, search-based platform that allows you to access the information you need faster, wherever it's stored, in whatever format, without requiring centralization. It's scalable, flexible, and cost-effective, making it easy to connect and operationalize data across diverse systems.

Zero Trust isn't just a single solution — it requires a [strategic, collaborative, and vendor-agnostic approach](#) to provide end-to-end security with comprehensive visibility across the entire environment. With Elastic's extensive ecosystem of partners and integrations, you can connect and unify data across all Zero Trust pillars, regardless of current or future toolsets.

# Identity

Challenge/need	Elastic capabilities	Use case example
<p><b>Unified IAM analytics</b></p> <p>Ensure real-time visibility and correlate identity events</p>	<p>Elastic serves as a common data layer that connects all data streams, from endpoints to applications. It centralizes logs from Active Directory, MFA, cloud identity services, and more in one index for high-speed correlation.</p>	<p>A government agency consolidates logs to detect anomalous login activities from different systems instantly.</p>
<p><b>Anomaly detection</b></p> <p>Detect complex security threats across diverse systems</p>	<p>Elastic's machine learning (ML) jobs detect suspicious sign-in activity (e.g., abnormal geolocation, privilege escalation) in near real time, triggering automated Zero Trust enforcement.</p>	<p>A government employee attempts to sign in from two distant locations within minutes; the system automatically flags and restricts access pending verification.</p>

# Devices

Challenge/need	Elastic capabilities	Use case example
<p><b>Centralized endpoint monitoring</b></p> <p>Agencies must scale security monitoring across a large fleet of devices, often distributed geographically</p>	<p>Elastic's <a href="#">single endpoint agent</a> and endpoint security allows you to monitor processes, files, network activity, and runtime anomalies across thousands of endpoints from a single console.</p>	<p>A defense agency tracks endpoint security across hundreds of field offices and mobile devices, detecting abnormal network usage and enforcing security policies to maintain confidentiality.</p>
<p><b>Endpoint protection</b></p> <p>Keep devices secure from threats, even in air-gapped environments</p>	<p>A single endpoint agent not only collects data from devices but also protects against malware, ransomware, and behavioral irregularities using ML algorithms. This signatureless approach keeps devices secure, even in disconnected or intermittent connectivity scenarios.</p>	<p>Customs and border control systems use single endpoint agent to protect sensitive data from cyber attacks while operating in isolated, disconnected environments.</p>
<p><b>Device posture</b></p> <p>Identify and isolate vulnerable or compromised endpoints while allowing security teams to investigate incidents</p>	<p>Visualize patch levels and vulnerabilities at scale, ensuring that compromised endpoints can be rapidly isolated — yet remain queryable for forensics. OSQuery enables real-time and scheduled querying of nearly any device attribute.</p>	<p>A government laptop shows signs of a ransomware infection and is automatically isolated from the network, while still being accessible for forensic analysis via SIEM.</p>

## Network & environment

Challenge/need	Elastic capabilities	Use case example
<p><b>Cross-domain visibility</b></p> <p>Centralize view of network security posture, reducing blind spots</p>	<p>Correlate firewall logs, VPC flow data, container orchestrations, and perimeter logs via Elastic cross-cluster search.</p>	<p>A government cloud team monitors VPC flow logs for policy violations. Unauthorized cross-region traffic is detected, triggering an alert for investigation.</p>
<p><b>Automated detection</b></p> <p>Detect the unauthorized access attempts and ensure adherence to microsegmentation policies</p>	<p>ML-based rules identify malicious port scans, exfiltration attempts, or unauthorized segments to ensure microsegmentation is enforced.</p>	<p>A federal agency enforces strict network segmentation for classified data. An unauthorized attempt to access a restricted subnet is detected, triggering an alert.</p>
<p><b>Automating security actions</b></p> <p>Notifications alone aren't sufficient for security events</p>	<p>The Elastic platform's API-first design enables easy integration with other systems, allowing not only alerts but also automated actions across Zero Trust tools. It serves as a unified data layer, allowing users to orchestrate security enforcement through API integrations, ticketing systems, and <a href="#">SOAR</a> applications.</p>	<p>A government office automates incident response, triggering access restrictions and alerts when suspicious activity is detected.</p>

# Applications & workloads

Challenge/need	Elastic capabilities	Use case example
<p><b>Automated data collection and indexing</b></p> <p>Comprehensive visibility across all layers of the operational stack for continuous monitoring</p>	<p>Elastic integrates with hundreds of data sources, including infrastructure, compute resources, network operations, orchestration platforms, service mesh, VMs/containers, operating systems, and applications.</p>	<p>A government agency oversees multiple data centers, collecting and indexing data across servers, containers, and applications to ensure full visibility and proactive monitoring.</p>
<p><b>Integration with existing infrastructure</b></p> <p>Seamless integration with existing infrastructure, ensuring flexibility</p>	<p>Supports diverse environments, from physical and virtual machines to cloud platforms and containerized services.</p>	<p>A state government with a hybrid cloud infrastructure wants to ensure that data from both on-premise and cloud applications is collected and indexed for comprehensive security monitoring.</p>
<p><b>Application performance monitoring and observability</b></p> <p>Ensure no blind spots in monitoring, improving incident response and compliance</p>	<p>Collect real-time logs, metrics, and traces from apps, microservices, and serverless functions, or traditional apps in real time across all layers — network, infrastructure, and services.</p>	<p>A federal agency requires full data visibility for compliance with cybersecurity mandates. Data from all networks, applications, and transactions is ingested to provide a centralized view for auditing and compliance.</p>
<p><b>Real-time alerting</b></p> <p>Automate threat containment, improving response times and reducing the risk of lateral movement</p>	<p>Enforce Zero Trust rules at the application layer, isolating compromised workloads or adjusting policies when threat levels spike.</p>	<p>A government health agency detects abnormal behavior in a healthcare application. An alert is triggered, automatically isolating the compromised service and updating access policies to contain the threat.</p>

# Data

Challenge/need	Elastic capabilities	Use case example
<b>Unified data layer</b> Consolidate data operations for better governance and security	Elastic integrates with existing systems, serving as a unified, scalable data layer for governance, records management, audit, and compliance.	A national security agency connects multiple agencies' data streams to a unified platform, allowing for real-time analysis, efficient data sharing between departments, and automated audit logging for transparency and compliance.
<b>API-driven data service</b> Agencies need fast, scalable data operations with secure access control to sensitive information	Acts as a common service spanning all systems with built-in data security. RBAC & ABAC capabilities control access at multiple layers.	A law enforcement agency shares case data with judicial departments, with access limited based on user roles and clearance levels.
<b>Searchable snapshots</b> Long term data retention with quick search for audits and investigations	Retain multi-year logs for compliance and forensics without compromising search performance.	A government agency retains years of security event logs using searchable snapshots, allowing fast searches for audits and investigations while minimizing storage costs with Elastic's frozen tier.
<b>Data-centric security</b> Detect unauthorized data access, especially during off-hours	Use ML to monitor large data transfers, CSV exports, and off-hours anomalies to detect potential insider threats or external breaches.	A law enforcement agency monitors large data exports during off-hours using machine learning, detecting unusual patterns that may indicate potential data exfiltration or insider threats.

# Data mesh is key for Zero Trust

Elastic's platform offers unified visibility across all Zero Trust pillars through a unified data layer, powered by advanced data analytics and machine learning for scalable threat detection. It integrates with security orchestration systems for automated responses, processes large volumes of data, and correlates events for comprehensive security insights.

In addition to integrating the Zero Trust pillars, Elastic allows a query speed layer for all Zero Trust data flowing between them.



## Unified data layer eliminating silos

Elastic consolidates all data streams, such as logs, metrics, and traces, from a wide range of sources: identity systems, endpoints, network devices, cloud environments, and applications.



## Dashboards

Elastic's intuitive dashboards allow you to track, visualize, and report on Zero Trust status by combining user behavior, device posture, network flows, and other security insights across multiple pillars.



## Events correlation

A unified telemetry repository, fast search, and distributed architecture enable rapid event correlation across all pillars, which allows quick threat detection, investigation, and response without switching between tools.



## Real-time search

Elastic's distributed architecture and high-performance search capabilities enable teams to run sub-second queries — even against massive data volumes.



## Machine learning

Elastic's built-in machine learning proactively detects unusual patterns (such as odd login times or data transfers) without requiring custom code, delivering faster, more accurate threat identification.



## Scalability

Elastic's horizontally scalable design and tiered data storage with searchable snapshots accommodate growing data demands while keeping performance high and costs manageable.

# Data, analytics, and orchestration

With Elastic, data is unified for real-time monitoring and investigation, automating insights and seamlessly integrating with existing tools. Its built-in analytics, filtering, querying, and integrated security drive efficient orchestration, reducing noise and enabling automated actions across systems.



## Flexible rules and alerting

Elastic's detection engine comes with prebuilt detection rules, which agencies can customize or extend. When these rules fire — detecting abnormal credential usage or identifying indicators of compromise, for example — Elastic generates structured alerts that can feed directly into orchestration workflows.



## Dynamic remediation and policy enforcement

By unifying all relevant data, Elastic gives agencies the insight to confidently automate Zero Trust actions. Whether forcing MFA for suspicious accounts, isolating compromised endpoints, or updating network segmentation in real time, Elastic ensures swift, precise threat containment.



## Seamless integration and open APIs

Elastic's well-documented APIs simplify connections to [SIEM](#), [SOAR](#), and ticketing systems. Alignment with ECS (Elastic Common Schema) and OpenTelemetry ensures seamless data interchange across diverse security and operational platforms without cumbersome custom integrations.



## Continuous monitoring and compliance

Elastic's centralized logs and real-time analytics enable agencies to maintain ongoing visibility and respond adaptively to new threats or policy changes. This "always verify" approach is key to meeting federal mandates.

# Real-world applications and success stories

## Data mesh for US federal agencies

For US federal agencies, the Elastic data mesh powers the Continuous Diagnostics and Mitigation (CDM) dashboard, enabling multiple US federal agencies to obtain a unified view of security threats and patterns without transferring data ownership to a central repository. This capability is vital for projects where data visibility is necessary but ownership is distributed.

## Unified view across multiple data centers

One public sector customer needed a unified view across two data centers, each generating 2.5 terabytes of security data per day. Their initial plan was to replicate all data, doubling storage costs. However, with Elastic's cross-cluster search, they eliminated the need for replication, drastically reducing infrastructure complexity and costs. Now, they can access a single pane of glass view from either data center — without duplicating data.



Zero Trust is the top security model for public sector organizations dealing with complex threats. Elastic's platform connects security data from all Zero Trust pillars, offering the visibility and tools needed for effective protection. By aligning with global frameworks, Elastic helps public sector agencies worldwide accelerate their Zero Trust adoption, ensure compliance, and strengthen their security posture.

To set up some time to discuss your specific Zero Trust strategy, contact one of our government specialists at [www.elastic.co/contact/public-sector](http://www.elastic.co/contact/public-sector)

[Get in touch](#)

[elastic.co](http://elastic.co)

