

Achieving Zero Trust in Export Control and Compliance Initiatives with TC Engine and Axiomatics

Understanding Export Control and ITAR

For more than three decades, state-sponsored cyber espionage targeting NATO and Defense Industrial Base (DIB) Intellectual Property (IP) has been a persistent threat. In addition to the advances in this area, the DIB faces petabytes-upon-petabytes of data compliance risk every day. Regulations such as the International Traffic in Arms Regulations (ITAR) require specific handling of Export Controlled Information (ECI). Increasingly, export regulators are doling out fines and penalties for [ECI compliance failures stemming from failing to safeguard US military IP](#).

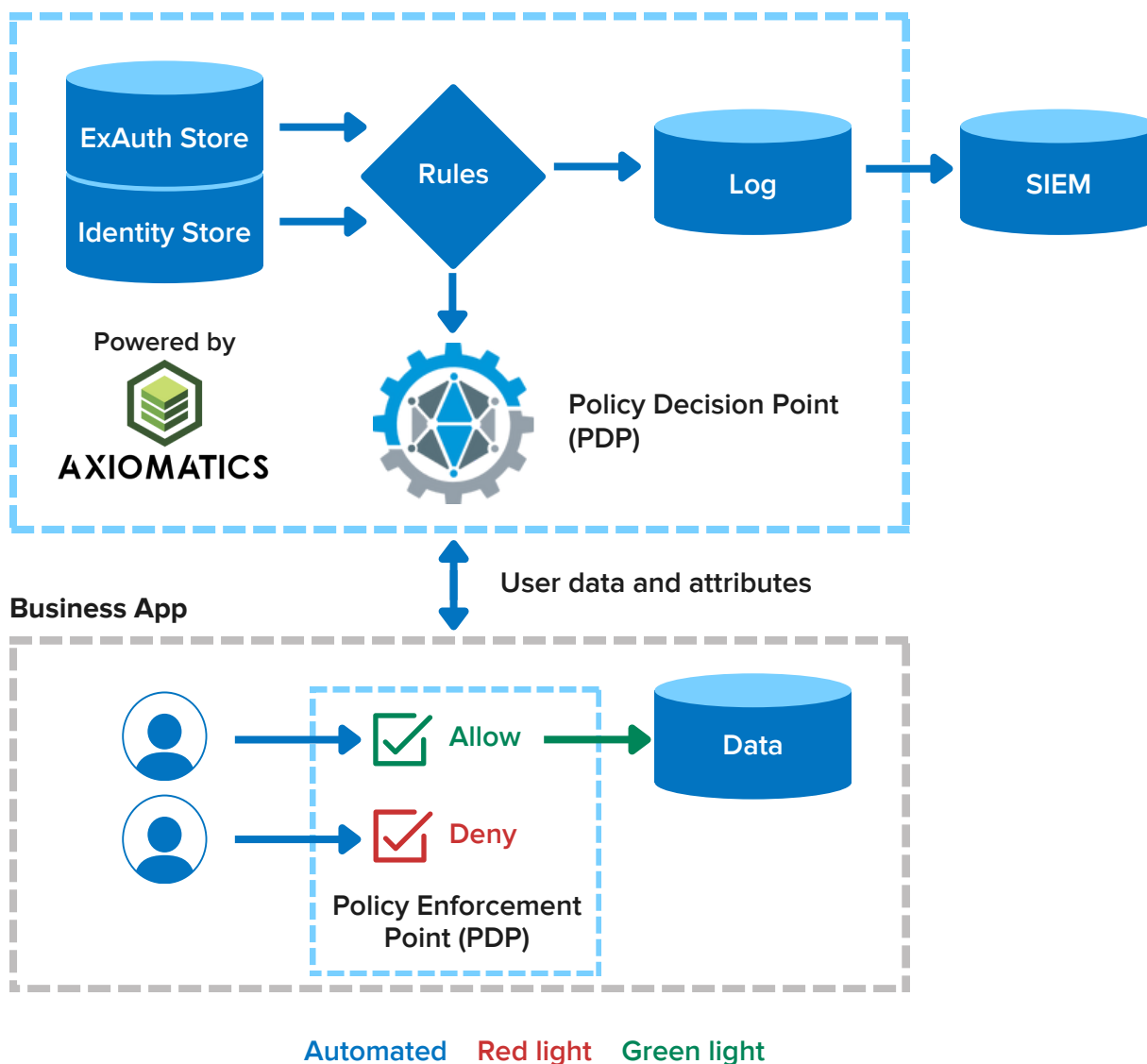
The result of this challenge is that any organization involved in the manufacture, sale or distribution of defense-related items or services supporting any arm of the United States military (or one of their suppliers) knows they must adhere to compliance requirements established by ITAR. ITAR's mandate is to ensure that access to physical materials or technical data related to defense and military technologies is restricted to U.S. citizens and not used for any criminal or terrorist activities.

Due to advances in file sharing technology, there has been a fundamental shift in export compliance risk, from the physical to the cyber domain. Before any business can be conducted, suppliers must obtain an Export Authorization Certificate. Once received, the challenge with the certificate is understanding the detailed legal text and directives to ensure your organization complies with the strict requirements and has initiated sufficient controls among employees and the supply chain to ensure continuous compliance. Additionally, if you are audited or impacted by any sort of breach, you must prove to auditors that you took these steps to maintain compliance. An ITAR violation can result in a hefty fine, severely impact your business and in some cases, mean up to ten years in prison.

Easy Interpretation of Export Authorization

Export Control requirements are complex and can be confusing to understand. To address this and other ITAR compliance-related challenges, TC Engine and Axiomatics have partnered, creating an Authorization Engine that automates transactional compliance through electronic policy enforcement to ensure continuous compliance. This solution combines TC Engine’s AI capabilities to convert export authorizations into the machine-actionable attributes required for compliant exports with Axiomatics’ capabilities to automate complex red-light/green-light decisions. The result is a series of fine-grained access control (FGAC) policies that must be followed to comply with ECI and ITAR regulations - in other words, a Zero Trust solution for ECI.

Zero Trust for ECI (A Simplified Architecture)



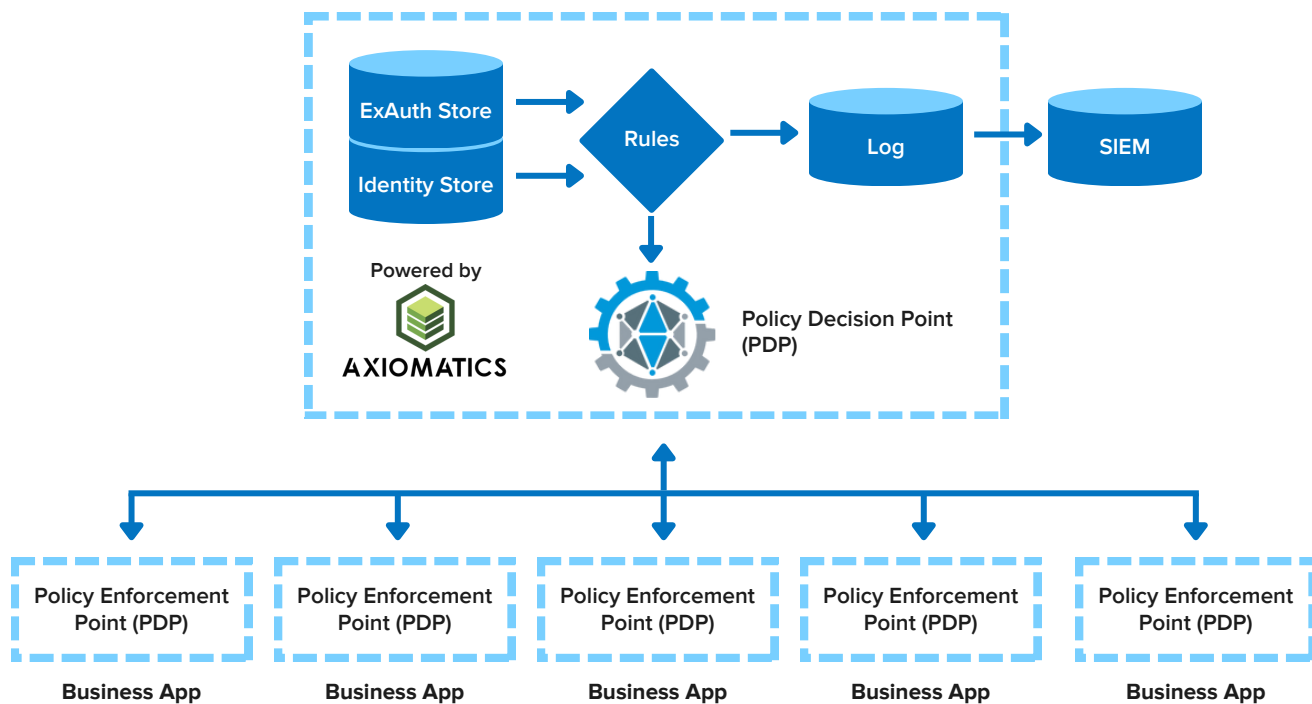
SOLUTION BENEFITS

- 1** Mitigate export-controlled information (ECI) risks and threats through Zero Trust.
- 2** Reduce process debt and resource burden (e.g., queues, cycle time, touch time, etc.).
- 3** Convert export authorization into machine actionable attributes used for automated compliance decision making.
- 4** Standardize and centralize electronic policies for export compliance management.
- 5** Distribute and scale electronic export policy enforcement.
- 6** Centralize electronic export record keeping.
- 7** Enable automated compliance decisions with a country-and regime-agnostic platform.
- 8** Maximize compliant global trade while satisfying safeguarding requirements.

How does it work?

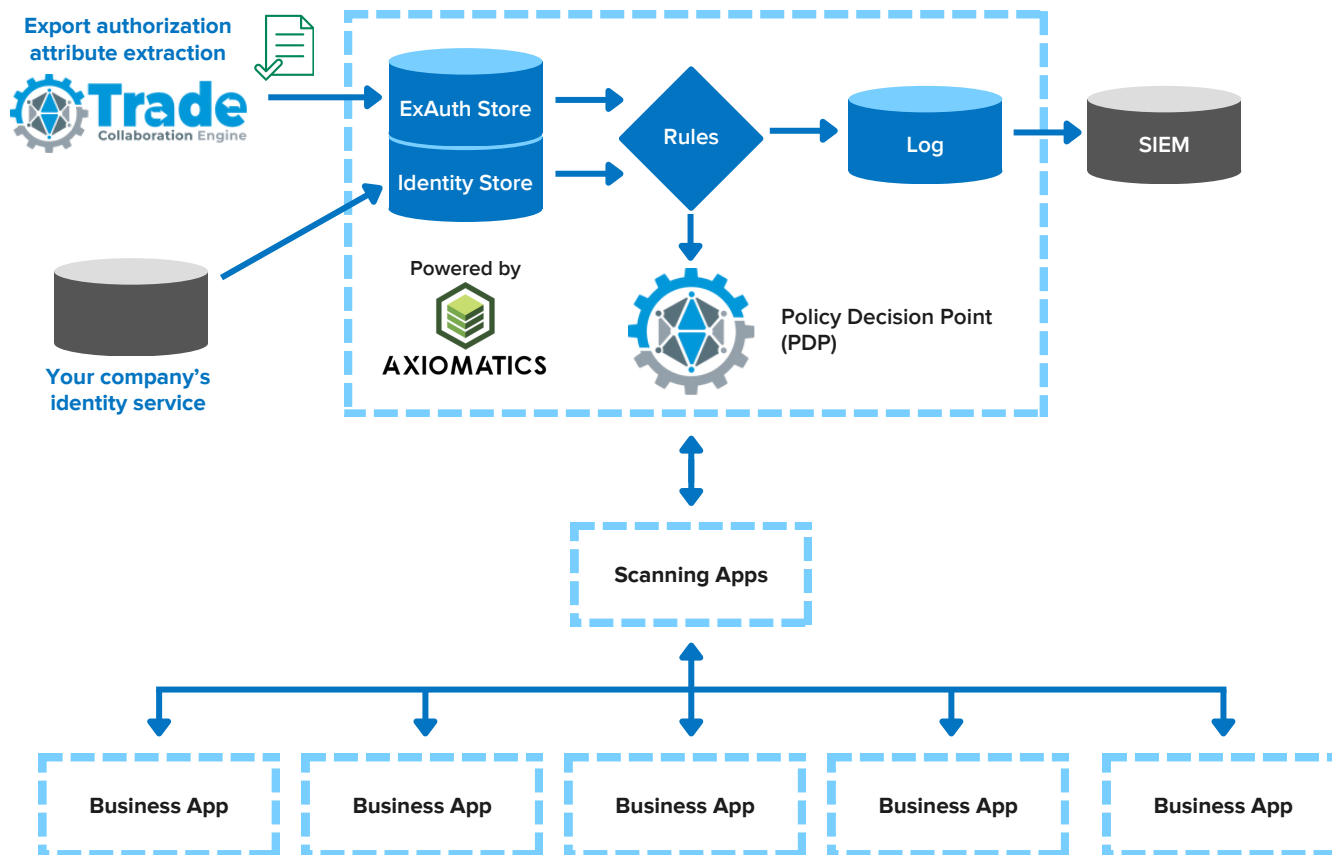
Simply put, Authorization Engine matches an object, entity, and individual, (i.e. user) attributes to export authorization attributes to determine if the export transaction is authorized. A compliant release decision depends upon a three-way match between the transaction object, entity and individual attributes and the export authorization object, entity and individual attributes. When the attributes align, the transaction is approved. From a single platform, companies can define, automatically enforce, record, and monitor export transaction compliance.

Zero Trust for ECI = Scalable ECI Compliance



The role of the Authorization Engine in this process is to validate export authorization coverage to determine if the export transaction is authorized thereby executing a compliant release decision. The Authorization Engine can also integrate with centralized user access provisioning systems to render the process across the enterprise mistake-proof. The attribute-based monitoring aspect is a powerful use case. For example, one of the leading causes of ITAR violations is users introducing unauthorized ECI into the wrong storage container. The power of attribute-based transaction monitoring provides capabilities to quickly identify mistakes and mitigate risk consequences.

Zero Trust for ECI = Scalable ECI Compliance



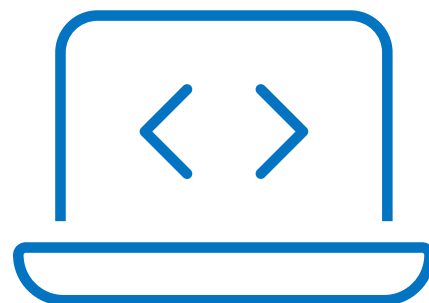
Efficiency and Automation

The solution is designed with automation in mind at every step. Your employees aren't export control regulators or experts and are focused on driving your business forward. At the same time, your security and compliance team can't physically be involved in every decision each time an end user shares a file. This solution helps automate the necessary steps for all key stakeholders involved and ensures productivity is maintained with compliance and security in mind.

Take the next steps

For more information on our solution, [watch our prerecorded webinar](#) and [read our blog post](#).

Meet with our solution experts for [a demo of our Orchestrated Authorization solution](#) and discuss how our approach can save your organization time and money.



Stay connected and informed

Get the latest insights, announcements, and assets from our thought leaders and customer success team:



[Blog articles](#)



[Join us on LinkedIn](#)



[Press releases and announcements](#)



[Subscribe to our YouTube channel](#)



[Resources, solution briefs, and tools](#)

Axiomatics is the originator and leading provider of runtime, fine-grained authorization delivered with attribute-based access control (ABAC) for applications, data, APIs, and microservices.

The company's Orchestrated Authorization strategy enables enterprises to effectively and efficiently connect Axiomatics' award-winning authorization platform to critical security implementations, such as Zero Trust or identity-first security. The world's largest enterprises and government agencies continually depend on Axiomatics' award-winning authorization platform to share sensitive, valuable, and regulated digital assets – but only to authorized users and in the right context

Follow us on LinkedIn: <https://www.linkedin.com/company/axiomatics>

Join us on YouTube: <https://www.youtube.com/@axiomatics>

Learn more or request a demo of our solution:

axiomatics.com

info@axiomatics.com

US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240



AXIOMATIC