

Utilizing ABAC to Deliver Purpose-Built, Dynamic Authorization for Asset Sharing

ABAC Trust Controller™ and ABAC Verification Point™

Attribute-Based Access Controls (ABAC) allow organizations to share protected information, collaborate with confidence, and weave existing assets into an orchestrated security architecture. Fornetix's **ABAC Trust Controller** and **ABAC Verification Point** are powerful policy orchestration tools enabling the flexible access controls a true Zero Trust strategy requires.

What Is ABAC?

Traditional access controls have focused primarily on a role-based model (RBAC) for securing sensitive assets. Organizations needed to predefine all potential functions and assign each user a certain level of security privileges, granting or denying access to data based entirely on their role. This rigid, one-size-fits-all method quickly becomes unwieldy and error-prone with significant security risks when deployed at scale.

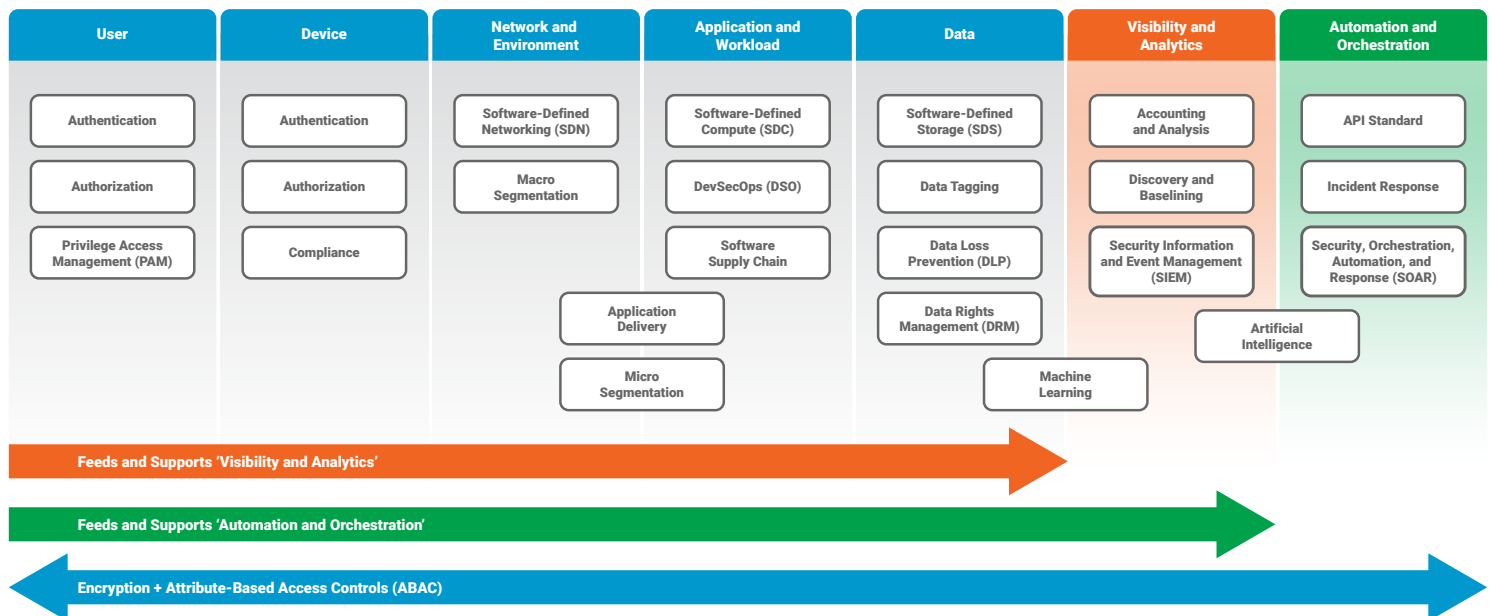
As an attribute-based model, ABAC allows for the use of fine-grained, centralized policies to govern whether a user can access the desired data.

Instead of rigid roles, ABAC leverages a wide variety of attributes as building blocks to construct meaningful policies. For example, a policy might dictate specific locations, approved devices, certain hours of the day, whitelisted IP addresses, security classifications, department membership, and many other contextual details. Access to the resource is denied if the circumstances fail any of the policy's requirements.

In a time of increasing collaboration and sharing between enterprises and partners, dynamic and flexible access controls are a non-negotiable requirement for protecting critical assets.

Strong Foundation for Zero Trust

The concept of "trust nothing and verify everything" has stood the test of time for a reason. And yet, authorization and access controls are frequently relegated to an afterthought when designing enterprise infrastructure. Implementing ABAC principles from the outset allows organizations to weave those powerful security benefits throughout all aspects of a Zero Trust architecture. ABAC can also be easily added to existing infrastructure, enabling these powerful security capabilities.





Powerful Policy Engine

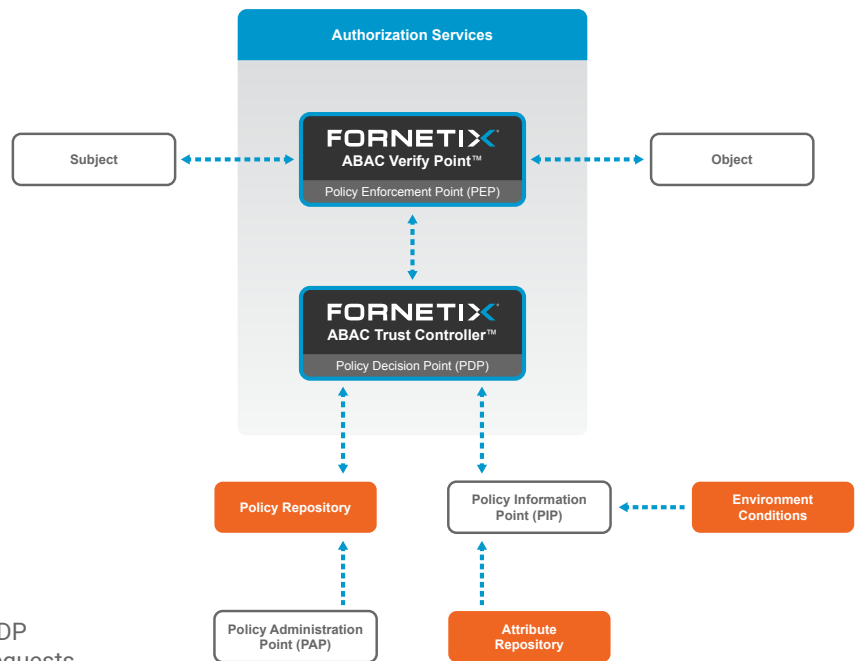
The NIST SP 800-162 document lays out requirements for ABAC access control mechanisms. It states “By evaluating each policy element against the available information, the access control mechanism often employs a **Policy Decision Point (PDP)** to render a decision, a **Policy Enforcement Point (PEP)** to enforce the decision, and some sort of context handler or workflow coordinator to manage the collection of attributes required for the decision.”

In the ABAC framework, attributes are generally grouped into four categories:

- Subject** — The user requesting access
- Action** — The operation being attempted
- Object** — The resource being accessed
- Environment** — Variables such as time, location, or other dynamic characteristics

 The Foretix **ABAC Trust Controller** acts as a PDP within an attribute-based model evaluating all requests against the security policies currently in place. It quickly propagates policies that apply across multiple devices while still allowing granular policies at the node level.

 The Foretix **ABAC Verification Point** acts as a PEP utilizing standards-based APIs to support enforcement of policy decisions across applications and services. Use cases include collaboration tools, databases, custom applications, messaging, PKI, and more.



The approach Foretix has taken to ABAC, allowing you to put these capabilities inside a FIPS 140-2 cryptographic boundary, is unique in the industry. This approach ensures you are able to take advantage of the security benefits of ABAC while maintaining regulatory compliance in many uses you are struggling with today.

ABAC in the Real World

Government Use Case

Deploying Zero Trust architecture in a federal/military environment affords great flexibility to data security for onboarding partners, creating unified environments, secure collaboration, and policy enforcement. Here are two real-world use cases that are currently putting ABAC into practice:

Secure Chat — Foretix has developed chat services in tactical environments for information sharing using industry-standard XMPP chat service. It leverages **ABAC Trust Controller** to make decisions based on user, message, and chat target. **ABAC Verification Point** is embedded into XMPP server allowing for secure API calls into **ABAC Trust Controller**. Policy checks occur on every chat message. Policy decision and enforcement components are kept in core trusted infrastructure. Chat clients do not require modification.

Governance Policy for Bilateral Network — Provides authorization control point when integrating coalition and partner systems into a shared network. Speeds onboarding of secure sharing environments. **ABAC Trust Controller** acts as a PDP and is employed as a repository of authorization attributes for bilateral network services and applications. **ABAC Verification Points** are implemented across targeted applications to enable a Zero Trust PEP.

Healthcare Use Case

A Zero Trust architecture applied to patient privacy would involve layers of security that integrate with health records, billing services, and third-party providers. Health organizations would be able to:

- Securely share PHI health records
- Implement control of external partners via centralized policies
- Enforce policy based on attributes such as login times, specific ID10 codes, and network location
- Conduct authorization with no perceptible impact on performance
- Maintain regulatory compliance
- Reduce costs by reducing IT complexity

