Imprivata Knowledge Hub:

Attribute-Based Access Control (ABAC)

What is Attribute-Based Access Control (ABAC)? Learn about this term and more with our expansive website glossary that explores topics related to cybersecurity and access management.

Video Transcript:

Kayleigh Flemming: Hi, I'm Kayleigh with Imprivata!

Attribute-Based Access Control is a model that uses attributes associated with users, resources, and the environment to determine access rights.

Unlike simpler models like Role-Based Access Control, which relies on predefined roles, Attribute-Based Access Control offers a more granular and flexible approach to managing access. This makes it particularly well-suited for complex and dynamic environments where access decisions need more context.

With Attribute-Based Access Control, attributes can include a wide range of characteristics, such as:

User Role, Job Title, Department Affiliation, Time of Day, Location, and Data Sensitivity.

For example, a user might be granted access to a particular document only if they are a member of the finance department, are accessing the document during business hours, and are located within the company's network. This level of detail allows organizations to implement highly nuanced access policies that, with variable dependencies, can adapt to changing conditions and requirements.

One of the key advantages of this model is the support of fine-grained access controls. This is useful in scenarios where data and resources need to be protected based on multiple, interrelated factors.

For instance, in a healthcare setting, a doctor might be allowed to access patient records only if they are treating the patient and are located within the hospital premises. Similarly, in a financial institution, a trader might be permitted to execute trades only during specific market hours and from approved devices.

Attribute-Based Access Control also enhances security by reducing the risk of unauthorized access and data breaches. By basing access decisions on a combination of attributes, organizations can ensure that only the right individuals have access to the right resources at the right time. This reduces the attack surface and minimizes the potential for insider threats. Additionally, Attribute-Based Access Control can be integrated with other security measures, such as multifactor authentication and encryption for additional layers.

At Imprivata, we deliver simple, secure access for critical workers and third-parties through features and principles like attribute-based access control.

Contact us to learn more.

Thanks for watching!
