KuppingerCole Report

MARKET COMPASS

By Graham Williamson

April 21, 2022

Policy Based Access Management

Access control is recognized as the most important component of an organization's cybersecurity protection. For too long access control has been based on static entitlements, but this is changing. Organizations are now increasingly demanding dynamic access control, with decisions made in real-time. They want support for an agile IT approach with dynamic workloads across multiple cloud environments. They want support for their DevOps staff for containerized cloud developments and cloud-native deployments. Course-grained authentication is no longer sufficient, applications and protected resources require fine grained authorization services that can also supply identity attributes and context variables. Policy-based Access Management can satisfy these requirements.

By **Graham Williamson**
gw@kuppingercole.com

Content

1 Management Summary

Much has changed since the last market compass on Dynamic Access Management. Technology is galloping ahead at dizzying rates that many organizations find difficult to assimilate. This is unfortunate because if they can't stay abreast of advances in technology, when new competitors come on the scene, agile and lean competitors without the baggage of more mature enterprises, there is a danger that established companies will find their market-share diminishing. But it does not have to be this way. With a pivot to a unified-services approach, underpinned by consistent policy, mature enterprises can compete with start-ups, leveraging their experience to remain competitive. A unified-services approach is one in which the services a user can access do not vary depending upon the technology on which they are deployed; accessing services will be consistent regardless of whether the applications are on-premises, delivered via cloud infrastructure or via cloud -native deployments.

To achieve this, organizations need to make a strategic decision to unify IT development and operations (DevOps). There must be a shift from a siloed environment to a holistic, integrated approach. Silo's may be functional i.e., staff from the marketing department do not talk to anyone in the production department; or infrastructure siloes may exist i.e., data center operators do not interact with cloud service providers and have nothing to do with SaaS (Software as a Service) applications on public cloud infrastructure. But such practices are detrimental, it must be remembered that all diverse deployments start as a tactical response to a business need. Migration to an 'integrated services' approach, driven by a common strategy is now required.

This strategy should be focused on managing complexity. Over the past few years, organizations have gone from managing their own data centers, to accepting services deployed on vendor-managed clouds, to deploying apps on VMs on public clouds, to allowing business units to engage with SaaS app vendors or cloud platform suppliers, to deploying containerized software, to developing cloud native solutions. Each step along this journey has decreased oversight across the IT environment and increased cybersecurity threats. Access control management of administrative accounts on cloud infrastructure is often inadequate. Nightly transfers of personal identity data to multiple SaaS providers across the internet are not uncommon. APIs in containerized cloud native deployments across disparate cloud environments occur in the absence of mandated management and security settings. The adoption of cloud platforms often abrogates the CIO from the responsibility for administration and governance services. The IT environment has become too broad for many CIOs to effectively manage and too complex to fully understand.

But complexity can be reduced by mandating a service-based approach, rather than a product approach, and by moving to automated, policy-based management across runtime environments. A service-based approach means applications are loosely coupled with the user interface provided to the client, the user no longer needs access to the infrastructure on which the application is running, they only need to access the exposed services. Policy-based access control assists in this decoupling; it allows organizations to enforce

consistent entitlements across multiple applications for multiple business units. 'Where an app is running' becomes less important than the 'availability of the service' that it is providing. The focus is now on the response, resilience and redundancy of an organization's business services.

A four-step process is recommended for the design and deployment of a PBAM environment:

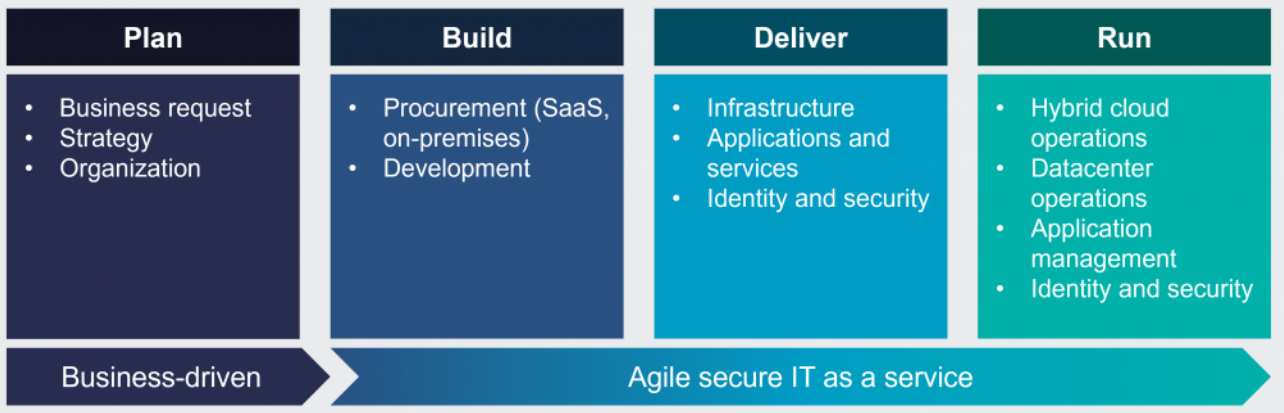


Figure 1: Model for Agile IT Development

Plan	A cross-functional team should be engaged for the project planning to ensure all potential stakeholders have input into the access control strategy for the organization.
Build	A design that satisfies the outcomes of the planning stage is required. A decision on the most appropriate deployment is required, and the most appropriate development environment must be selected. Component and system testing will complete the build stage.
Deliver	Stakeholders should be involved in the acceptance testing as the solution is promoted to production. Most development environments employ Continuous Integration/Continuous Delivery (CI/CD) toolsets that automate much of the deployment activity and keep diverse deployments current.
Run	Operational personnel require tools that provide visibility across hybrid and multi-cloud deployments and a management interface with dashboard features to allow continuous monitoring of the PBAM environment. Connection to the enterprise SOC/SIEM tools is highly advisable.

A dynamic access management environment will reduce complexity by employing a consistent policy across the IT environment, from the on-premises services (legacy line-of-business applications), the IaaS (Infrastructure as a Service) cloud-based apps, and increasingly multi cloud deployments. A consistent set of policies across the entire environment is increasingly important for organizations that are adopting cloud native service deployments where it is no longer a monolithic VM being deployed but containerized services. Such an approach not only leverages benefits of the cloud, such as scaling, but also supports a more agile development environment, an important capability that will reduce 'time to value' and heighten competitiveness.

Cloud-native deployments, which expose services via containers or micro-services, require a new approach for access control. Legacy dynamic access management environments are not able to service multiple APIs in an efficient and agile manner, and typically do not support Cloud Native Computing Foundation (CNCF) protocols. But over the past two years vendors have developed tools to address this market. Cloud-native deployments leverage Open Policy Agent (OPA) protocols and adhere to the CNCF framework.

This Market Compass seeks to cater for both ends of the access control market from traditional PBAC environments, consisting of policy decision points servicing multiple enforcement points, usually adhering to the XACML framework on one end, to cloud-native environments servicing cloud container approaches and microservices platforms, typically adopting the OPA protocol, at the other end.

Key Findings:

- Rapid advances in technology development pose a threat to existing organizations that are typically less agile than their start-up competitors. PBAM solutions can assist by 'building-in' agility with common policies across multiple environments.
- Organizations must seek solutions that reduce complexity and encourage collaboration across the enterprise, a unified approach to providing services that transcend business units can encourage collaboration.
- Access control is increasingly recognized as being essential to cybersecurity, with account take overs responsible for most unauthorized intrusions, PBAM solutions provide access control consistency, reducing vulnerability.
- To fully leverage the benefits of cloud-deployed solutions a cloud-native approach to leverage the scaling capabilities of the cloud and increase agility is required.
- Robust governance strategy requires consistent access control policy across corporate resources. This requires:
    - Centralized policy management
    - Real-time policy decisions
    - Policy lifecycle management and analytics
- To satisfy corporate governance requirements integration between the authorization engine and corporate SOC/SIEM tools is required.

2 Market Segment

The focus of this Market Compass is Policy-Based Access Management (PBAM); a segment of the access control market that employs policies, evaluated in real-time, to provide access decisions to user requests for access to protected resources such as a computer application or sensitive database.

The solutions presented all have at their core a policy-based approach. There are at least two benefits to this: access control is consistent across the organization, no longer characterized by different practices between workgroups, and it improves efficiency with a single place to manage access control strategy. It also improves visibility, there are no longer disparate groups with their own access control environments.

Due to the rapid change that is occurring in cloud environments the PBAM sector covers a range of solutions. At one end of the continuum are the traditional dynamic access management offerings, at the other end are the cloud-native solutions:

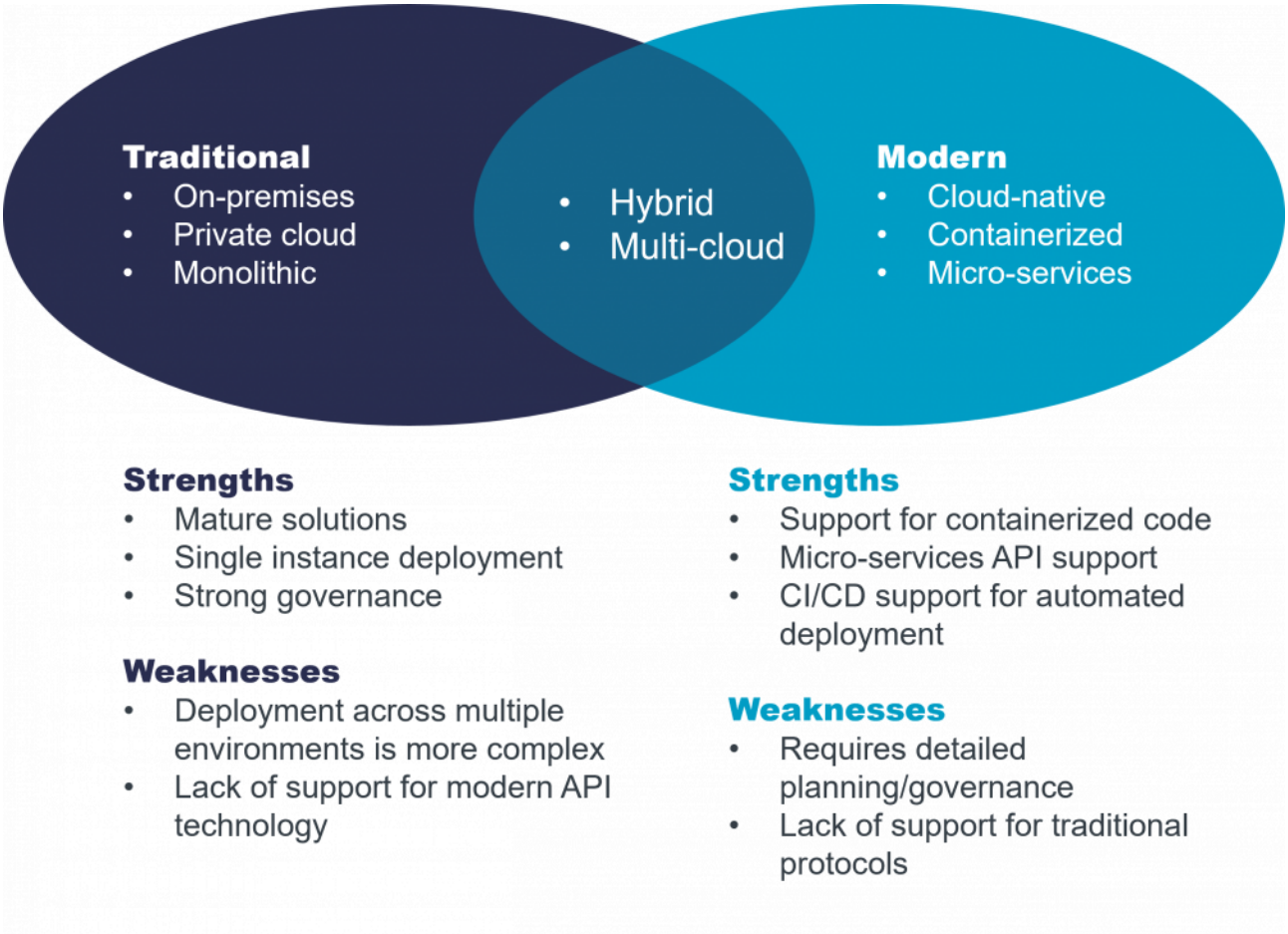


Figure 2: PBAM Contiuum

In reality most organization are somewhere between these two extremes. There will be legacy client-server applications, often fiscal management and ERP solutions that will remain monolithic applications, but most new application deployments will be web-based, typically on containerized cloud platforms. Start-up companies may be completely cloud-based, increasingly adopting cloud-native deployments in order to leverage the benefits of the cloud more fully. For organizations heavily involved in software development PBAM takes on an additional role of managing access to multiple containers or micro-service components that comprise a cloud-native application.

2.1 Traditional Dynamic Access Control

Traditional PBAC environments consist of several discrete components. While vendors will achieve a solution in diverse ways, a generic depiction showing the components of a dynamic authorization service is shown in Figure 3 -- Traditional Authorization Service.

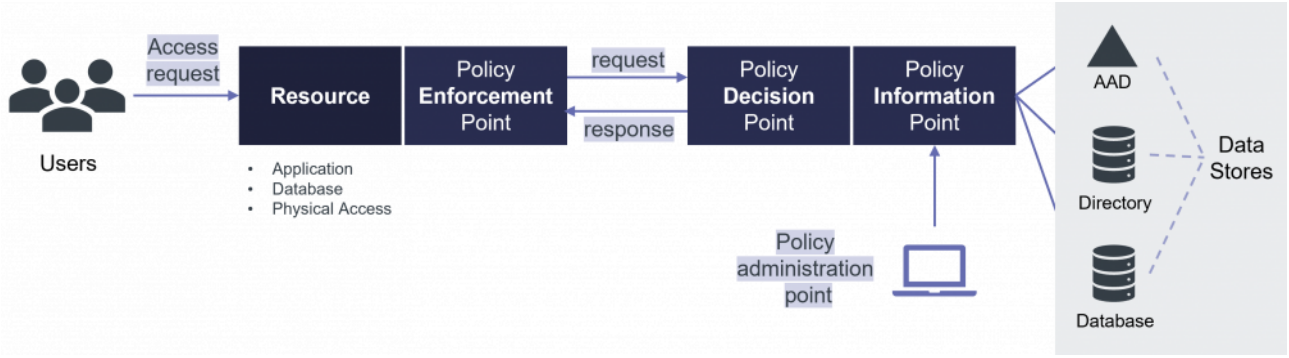


Figure 3: Traditional Authorization Service

The Decision Point will use data from the Information Point, typically identity attributes and context variables, to render decisions to an Enforcement Point integrated with the resource being protected. A Policy Administration tool will provide the interface for policy creation and modification.

2.2 Cloud Native Authorization

A cloud native environment is one in which applications are split up into their component parts typically via a containerized approach that optimizes cloud scaling and results in a more agile codebase. It also requires a more versatile access control solution that can support the authorization requirements of the various components, typically containers or micro-services.

One method to support access control in a cloud-native environment is the OPA model that uses service level policies to authorize users, devices, and other services, rather than an application-centric access control mechanism. Access control logic should never be hard-coded (even for devices); it should be removed from business logic in order to be agile and responsive to changes in user's characteristics, group memberships and device/service entitlements.

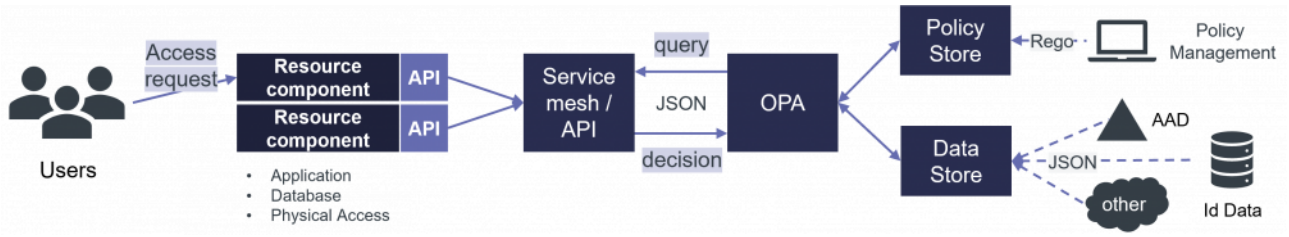


Figure 4: Cloud-native Authorization using OPA

In a cloud-native environment policy management is usually achieved via APIs, typically via JSON files over

HTTP. Policies and associated data are deployed via a library file, daemon or container sidecar on the application host or cloud infrastructure to ensure low latency in responses to access requests.

In cloud native-environments platforms are increasingly being adopted to abstract the application or resource from the underlying infrastructure. These platforms typically employ the OPA model for authorization services.

OPA can extend the Kubernetes access control capability so that each container can use the OPA APIs that expose the corporate access policies. In many cases cloud native environments employ a service-mesh architecture, to provide a consistent approach to access control across multiple applications. The OPA query language is Rego. It allows for the definition of assertions and communication of a binary decision. Data for OPA decisions is provided via JSON files.

Recently 'Kyverno' has been adopted for some Kubernetes deployments. It acts as an admission controller responding to webhook events in simple authorization environments. It is proprietary to Kubernetes environments and might be too limiting for enterprise deployments.

2.3 Market Direction

Identity data is becoming increasingly important within organizations. Historically the main reason for deploying an identity management solution was to provide access control to corporate resources, but the reliance on identity data goes beyond access control. It is now necessary to be able to support corporate applications with identity data to allow them to provide sophisticated services to staff, business partners and customers. Fine-grained access to identity attributes provides the ability for applications to optimize the user experience. Staff in the marketing department have different needs to finance department personnel, business partners must be restricted to the on-line order entry module, technical support personnel should only access the HVAC service functions, customers will receive a different user experience depending on their category. What is now required is an 'Identity Fabric' that allows organizations to leverage the trends in the marketplace:

- Migration to cloud services adds a level of complexity to the deployment of an externalized authorization service that must support on-premise applications, SaaS apps and multiple cloud environments. This means that PEP support for distributed applications is a requirement. Some vendors support a distributed PDP model where the decision point code is embedded in applications i.e., the PEP does not need to "call out to" an external PDP.
- Rapid containerization of cloud services presents a further complication. If PDP code is to be deployed on cloud infrastructure the PBAM solution must support distributed APIs and should ideally support a micro-services approach.
- Multi-factor authentication is now expected. Smartphones are ubiquitous and rapidly becoming the

enabling device for multi-factor deployments to significantly raise the assurance level associated with a user login event.

- At the network level, monitoring and control has significantly improved, resulting in reduced cybersecurity vulnerability, but this requires access to more fine-grained identity data such as security clearance level or subnet entitlements. Authorization servers provide real-time access to identity attributes to support network tools.
- User behavioral analytic tools are becoming more prevalent and require identity data and access to end-point device detail for corporate staff and business partners.
- AI is another trend that impacts PBAM and requires support from an organization's Identity Fabric. Access to a user's role within an organization, the department they're working in, their normal entitlements, any temporary assignments and date range for their validity, are common identity attributes that an AI engine must typically access in order to advise on, and provide governance over, policy-driven entitlements.

While the PBAM market sector is well established now, solution vendors are continually evolving and developing their products to accommodate these market trends; the IAM (Identity and Access Management) industry sector is expected to be increasingly flexible in its support for technology development and in leveraging the opportunities that arise. With the accelerating interest in cybersecurity issues these opportunities are expected to significantly increase over the next 2-3 years.

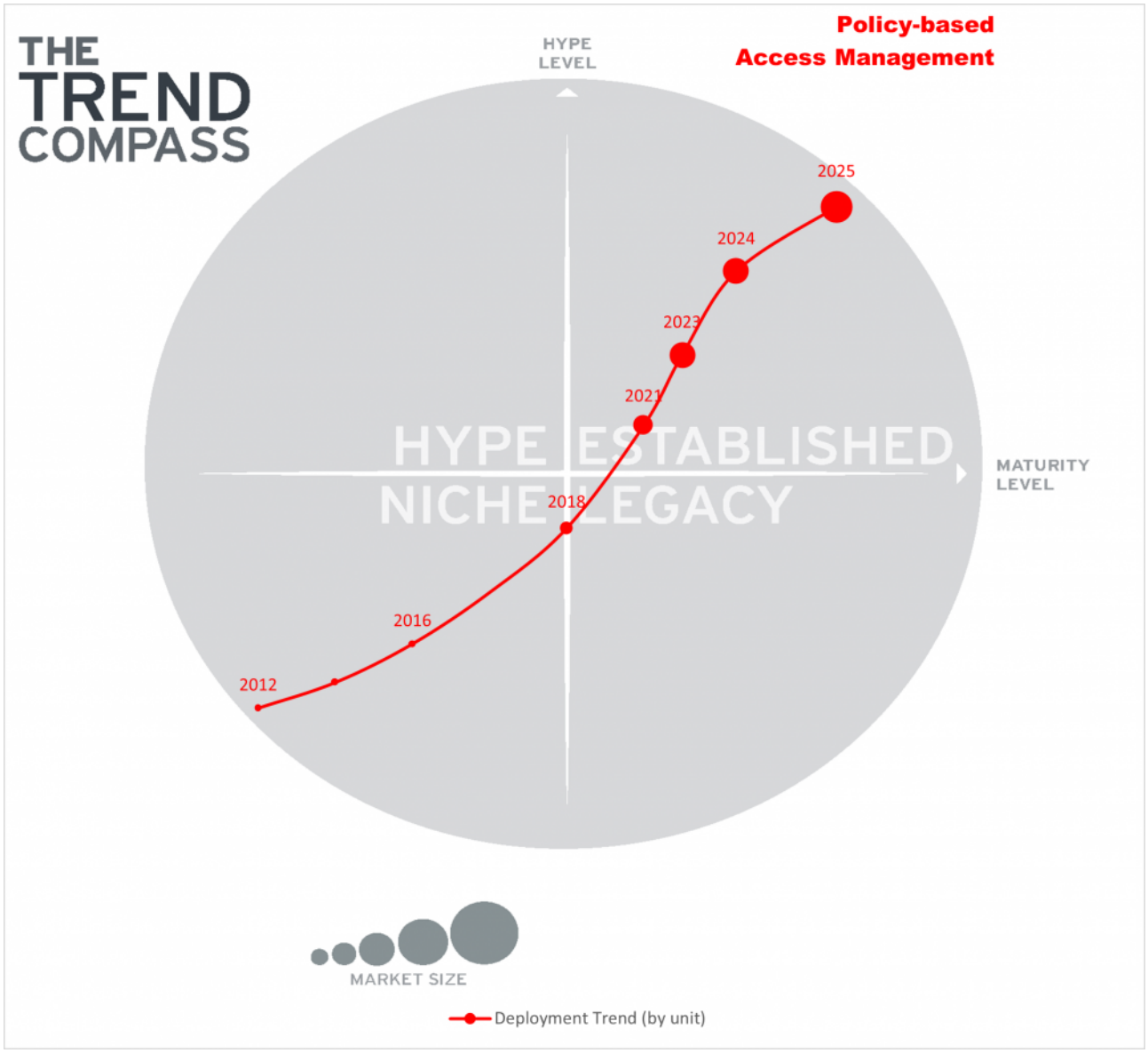


Figure 5: Trend Compass

There is another trend, driven by corporate governance, that is affecting the organization chart of companies. In software development environments the role of the CIO is being eroded and the role of the CISO (Chief Information Security Officers) is becoming more critical. While CIOs must set direction and provided C-level leadership, in the PBAM sector there is an increasing reliance on DevOps personnel to manage policy development and deployment; it is the CISO who is best placed to oversee this activity and ensure it meets corporate governance standards.

3 Capabilities

The Market Compass is designed to profile vendor solutions across specific capabilities. This section details the capabilities that one would expect to see in this market segment and breaks them down according to relevance to typical use cases.

3.1 All Capabilities

The PBAM market segment has a collection of standard capabilities that most solutions should include. These are listed in the table below.

Capability	Description	
Policy Decisions	The solution must be able to provide policy decisions to relying party applications and protected resources that externalize their access control logic. A centralized policy management capability is required for consistent access control decisions across the organization and support for diverse deployment options, including multi-cloud deployments.	Required
Policy Enforcement	Support for relying party applications is required. This might be SDKs for enforcement point code to be embedded in the application, or API support for a connector to an application or a gateway. For containerized cloud apps sidecar support is needed, for cloud-native deployments OPA support for a services mesh may be required. The ability to pass a constraint or additional attributes to enhance an authorization event is desirable	Required

Capability	Description	
Policy Administration	Creating and managing policies is required functionality. Solutions should have a business-friendly approach either through a graphical tool that assists non-programmers to create and modify policies, or via a drag-n-drop facility for policy creation. A micro-services environment, with a library of policies from which DevOps personnel can select, will improve consistency and accelerate software development. The ability to accommodate an organization's policy strategy i.e., a policy hierarchy, is highly desirable.	Required
Information Stores	The ability to ingest data from identity stores is required to support policy decisions. Connectors to common identity stores or support for standards (LDAP, SCIM etc.) are required. Delta updates to cached identity data is required and the ability to support real-time lookups is desirable.	Required
Technology Support	Vendor support for technology options is important. Some vendors focus on enterprise solutions for on-premises or monolithic cloud environments, a framework such as XACML is highly desirable using XML or JSON arrays. Some vendors focus on supporting hybrid environments for which REST APIs and JSON files are expected. Some vendors service cloud-native environments where support for micro-services APIs and the OPA model is needed.	Desirable
Hybrid cloud	Increasingly organizations want a common authorization solution for hybrid cloud and multi-cloud environments. This means that an ability to provide access control decisions to on-premises resources as well as cloud-based applications is required.	Desirable
Cloud-native	In a cloud-native environment authorization support for micro-services is required. These services are components of a larger application and typically require an authorization service to satisfy a specific purpose. Support for developers who must tailor an API for each micro-service is highly desirable. OPA will typically be supported via Rego policy files and JSAON data files.	Desirable

Capability	Description	
Governance	A base requirement is a policy analytics tool that allows users to test a policy to ensure correct results. There will typically be a reporting capability allowing periodic certification of policy decisions for a specific cohort of users. Support for corporate SOC/SIEM infrastructure either via a logging tool or alert messaging is required. AI tools to assist in policy orchestration, or to identify policy inconsistency, is desirable	Required

Table 1: Desired Capabilities

3.2 Capabilities Recommended per use case

The PBAM market segment is evolving to meet an increasingly diverse authorization environment as described in section 2.2. Typical use cases that must be supported are described below.

3.2.1 Enterprise Use Case

Large enterprises with mature corporate applications typically maintain on-premises infrastructure typically running ERP or financial administration applications. They will also have significant IaaS deployments, usually VMs on private cloud services. A small number of SaaS apps will be used for point solutions such a service desk or sales support apps.

Enterprises generally require a solution that supports a standard authorization model such as the XACML framework, whereby a policy decision point provides the decisions, an enforcement point applies the decisions, an information point provides the data for the decisions and an administration point provides the ability to manage the policies. Equally important to large enterprises are governance tools that provide analytics and audit capabilities.

3.2.2 Large Corporates - no DevOps Use Case

Large corporations with a reliance on packaged software for purpose-specific applications, typically service industries or omni-channel retail operations, will largely be in the cloud on both private and public infrastructure. These will typically be 'lift &shift' deployments on VMs. Some use of SaaS apps will be made, often with a SaaS front end for common services.

For this use case the solution must have the ability to service multi-cloud environments from a common administration tool with either replication of decision point code or use of a low latency network connection.

3.2.3 Large Corporates - with DevOps Use Case

Large corporations with a need for software development to suit custom business applications will have significant IaaS deployments often associated with their preferred IDE (Integrated Development Environment). This will be primarily public cloud-based and will make effective use of scalable computer services, the wide variety of database types and good security controls. Containerization has been adopted and a structured codebase allows segmented deployments to occur.

Increasingly these organizations are adopting cloud native services to minimize costs and maximize agility. A set of micro-services to support code segments needs to be developed and, increasingly, a service-mesh environment is being adopted.

3.2.4 SME Use Case

Small to Medium corporations will typically be heavy users of public IaaS services and SaaS apps to run their businesses. They will typically use managed services to support their cloud environments and will often engage external organizations to monitor their environments and manage their cybersecurity requirements.

This multi-cloud approach requires solutions that can integrate with services provided by the major public cloud providers and support APIs for private clouds. Integration of authentication services across disparate cloud service providers is required.

3.2.5 Start-ups Use Case

Start-ups are SMEs that are on a rapid growth trajectory and with a narrow business focus. They lack staff with capabilities outside their specific area of expertise and are heavy users of SaaS solutions for business support functions. If their area of focus is software-based, they will have a strong need for cloud-native technology and related services such as an IDE and deployment automation. Increasingly these companies are adopting a service-mesh architecture.

The importance of the PBAM capabilities to each of the use cases is broadly as follows:

USE CASES CAPABILITIES	Enterprise	Large Corp's – No DevOps	Large Corp's - DevOps	SMEs	Start-up
Policy Decisions	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Policy Enforcement	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Policy Administration	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Information Stores	★★★★★	★★★★★	★★★☆☆	★★☆☆☆	☆☆☆☆☆
Technology Support	★★★★☆	★★★☆☆	★★★☆☆	★★☆☆☆	☆☆☆☆☆
Hybrid Cloud	★★★★★	★★★★☆	★★★☆☆	☆☆☆☆☆	☆☆☆☆☆
Cloud-native	★★☆☆☆	★★☆☆☆	★★★★★	☆☆☆☆☆	★★★★★
Governance	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★

Figure 6: Use-case mappings to capabilities

4 Ratings at a Glance

Each vendor featured below brings a unique capability to what is essentially a diverse market segment. A start-up with no on-premise applications has a very different requirement when compared to a large enterprise which must support monolithic applications deployed in their own datacenter. Equally, a start-up not engaged in software development will have no interest in solutions for a micro-services environment and will likely prefer a SaaS authorization server solution.

The ratings below are subjective, based on vendor briefings. It is strongly suggested that organizations wanting a PBAM solution document their requirements and approach vendors in the context of the specific solution being sought.

4.1 General Product Ratings

Based on our evaluation, a comparative overview of the ratings of the general standing of all the products covered in this document is shown in Table 3.

Product	Security	Deployment	Interoperability	Usability	Market Standing
Aserto	strong positive	positive	positive	strong positive	neutral
Axiomatics	strong positive	positive	positive	positive	strong positive
Cisco Identity Service Engine	strong positive	positive	positive	strong positive	strong positive
Cloudentity	strong positive	positive	strong positive	positive	strong positive
EmpowerID	strong positive	positive	positive	strong positive	strong positive
NextLabs CloudAZ	strong positive	strong positive	positive	positive	strong positive
Okera	strong positive	positive	neutral	positive	neutral
PlainID	strong positive	strong positive	positive	strong positive	strong positive
Scaled Access/One Welcome	strong positive	positive	neutral	strong positive	neutral
Strata Identity Orchestration	strong positive	positive	strong positive	positive	neutral
Styra	strong positive	positive	positive	strong positive	neutral
Legend	critical	weak	neutral	positive	strong positive

Table 3: Comparative Overview of the ratings for the general standing of all products

4.2 Noteworthy Vendors for Specific Capabilities

Some vendors are better positioned to meet specific use cases, while others have stronger offerings across a range of capabilities. We have identified a few vendors that are notable for their strengths in specific areas. Vendors have been selected based on information collected during the solution research process.

4.2.1 Outstanding in Innovation: Aserto

It is difficult to select a single vendor for innovation because all vendors in the sector are displaying immense innovative spirit in the support of cloud microservices, a requirement that has only come to the fore in the last couple of years. But Aserto has taken a brazen approach to deploy an open source microservices component coupled with a hosted authorization service providing IdP connections and policy management.

Figure 7: Outstanding in Innovation: Aserto

4.2.2 Outstanding in Functionality: PlainID

PlainID continues to provide a full-service identity management, access control and governance solution available across multiple environments. They support wide and diverse environments from on-premises installations, multi-cloud deployments and SaaS functionality. They have an intuitive approach to policy creation and management; they fully support centralized management of policies and a variety of decision point deployment options.

Figure 8: Outstanding in Functionality: PlainID

4.2.3 Outstanding in Network Integration: Cisco

Being able to exert control over access to specific network segments gives Cisco an edge over vendors' focus on application support. With the trend toward software defined networking Cisco can provide policy-based access control to network segments by implementing access control at switches, gateways and firewalls, providing the capability to permit or deny user access to corporate resources based on corporate policy.

Figure 9: Outstanding in Network Integration: Cisco

4.2.4 Outstanding in Traditional Resource Protection: Axiomatics

Axiomatics has been a mainstream provider of policy-driven access control since the inception of the sector over 20 years ago. The company was heavily involved in defining the processes and protocols used in controlling access to protected corporate resources and continues to migrate their solution to meet the demands of modern IT environments.

Figure 10: Outstanding in Traditional Resource Protection: Axiomatics

4.2.5 Outstanding in Micro-services Capability: Styra

Styra is a leading proponent of access control solutions for cloud-native deployments and pioneered the development of OPA. Their solution provides an easy-to-use UI for the creation and management of policies, displaying policies by system clusters, platform types and container stacks. The rules engine provides quick impact analysis of policies allowing staff to interrogate and test the effect of rule changes. Styra provides strong support for DevOps personnel in the protection of resources in a micro-services environment.

Figure 11: Outstanding in Micro-services Capability: Styra

4.2.6 Outstanding in Database Access Control: Okera

With the migration away from monolithic applications, in which it is relatively easy to manage access to corporate data, to cloud-native deployments, which make it an order-of-magnitude more difficult to protect databases across diverse environments, Okera have developed a focused solution providing unified management for multi-database protection. The Okera solution takes what is essentially a complex array of differing access control capabilities across diverse data stores and collapses the management into a unified approach providing consistent access control. Okera is a universal policy platform that allows the business, security, and data privacy teams to collaborate with DataOps, providing the consistency and clarity required by data-driven enterprises.

Figure 12: Outstanding in Database Access Control: Okera

5 Product/ Service Details

In the following section, each participating vendor is profiled with particular attention paid to the functionality of its product. Several important capabilities for providing PBAM have been selected and rated, displayed as a spider chart. For this Market Compass, we look at the following ten areas, as defined in section 3.1:

- Policy decisions
- Policy enforcement
- Policy administration
- Information store support
- Technology support
- Hybrid cloud support
- Cloud-native support
- Governance tools
- SoC/SIEM support
- Protocol support

The spider graphs for each vendor provide comparative information by showing the areas where the products are strongest. Some products may have gaps in some areas, while being strong in others. These might be a good fit if only the specific features are required. Other services deliver strong capabilities across all areas, thus being a better fit for a generic policy-based access management solution.

Vendor details are presented in alphabetical order.

5.1 Aserto

Aserto was founded in November 2020 by technical specialists with experience in authorization and cloud native deployments. The company was established to provide a developer-friendly solution that solved the microservices authorization requirement. The company headquarters are in Seattle, Washington State USA.

Aserto is an authorization service that provides access control decisions based on user context and resource content. The solution ingests user data from identity provider services on a scheduled basis. Policies are managed via a policy registry tool specifically designed to suit the multiple ways in which a developer might want to create a new policy or select or modify an existing policy. Aserto uses a rule management approach to facilitate access control to protected resources. The 'Rule management' user interface abstracts policy decisions from applications, allowing DevOps staff to apply a policy to multiple applications.

The solution is in two parts:

- the Aserto control plane, consisting of the directory -- a cached, centralized key-value store, the policy registry -- the hosted authorizer -- the centralized policy decision point, and the decision logs for out-of-band analysis.
- the Edge Authorizer sidecar, close to the relying application or resource, consists of the edge directory of pertinent data, the policy store of pertinent policies, the decision engine rendering true/false decisions and the decision logging facility.

The directory can be connected to an IdP service such as Auth0 or Okta, additional Identity providers can be added through a provider mechanism. The information provided by the IdP is mapped into the user object, which is the property set made available to the authorizer as the contextual data based on the subject actor. The 'get user' interface defines the path and query parameters and the periodicity of updates.

The policy creation user interface provides a policy definition screen that allows permissions to be set for put, post, or get policy templates. Developers can view the policy detail code and the input file and verify the resulting decision.

GitHub is used for code distribution. The policy engine is OPA-based with policies in Rego, and data is provided in JSON datasets, in the form of arrays or maps of JSON objects. Policies are packaged in Open Container Initiative (OCI) image format. Modern technologies such as RESTful APIs, gRPC and GraphQL are supported.

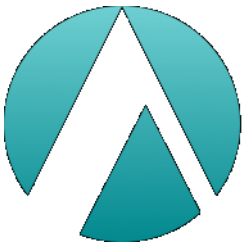
The Edge Authorizer is open source and can be deployed with any Kubernetes cluster but works well with the Hosted Authorizer. For customers not using Kubernetes, the Authorizer can be deployed as a microservice e.g., AWS Fargate or ECS.

The solution is targeted at the cloud native market segment. The features of the service are squarely focused on the developer community and the features offer a substantial advantage to developers, allowing them to develop and deploy secure code more quickly. On-premises applications are supported via Aserto's hybrid deployment model. On-premises applications can call the Edge Authorizer that is deployed in the company's private cloud. Furthermore, under the Enterprise support option organizations can deploy the control plane on-premises too.

Licensing is subscription-based. A four-level model is offered:

- Free for a limited number of id policies and users
- Essentials, unlimited polices, up to 5000 users
- Pro, unlimited users, managed edge authorizers, 30-day log retention
- Enterprise, run in client VPC, self-hosted IdP gateway

Security	●●●●●
Deployment	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Market Standing	●●●○○



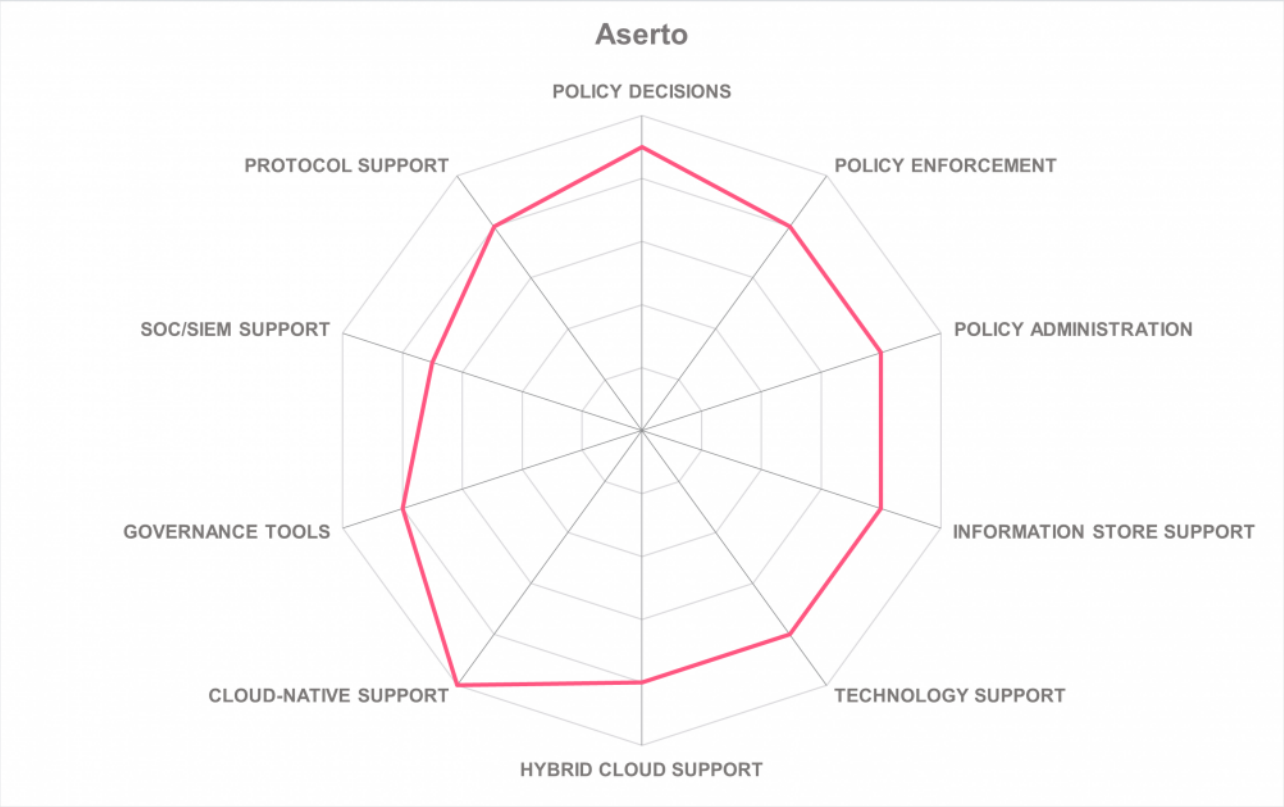
Aserto

Strengths

- Good developer support
- Open-source support for proof-of-concept
- SaaS Hosted Authorizer host with open-source sidecar authorizer
- Strong OPA model support
- Versatile licensing model

Challenges

- Policy administration by business personnel
- Some limitation to on-premises application support
- Limited localized support services in some geographies


Aserto
POLICY DECISIONS
POLICY ENFORCEMENT
POLICY ADMINISTRATION
INFORMATION STORE SUPPORT
TECHNOLOGY SUPPORT
HYBRID CLOUD SUPPORT
CLOUD-NATIVE SUPPORT
GOVERNANCE TOOLS
SOC/SIEM SUPPORT
PROTOCOL SUPPORT

5.2 Axiomatics

Axiomatics was founded in Stockholm, Sweden. The US headquarters are in Chicago and maintains a significant employee presence in Greece, Portugal and Canada. Axiomatics is a respected pioneer in policy-based access control and major contributor to the XACML standard.

Axiomatics provides a comprehensive solution for orchestrated authorization, providing fine-grained access control to protected resources. The Access Decision Service (ADS) can ingest policy information from a wide selection of sources using diverse protocols. ADS combines authorization for applications as well as databases, providing data protection that many applications fail to provide. For instance, a healthcare application may enforce access control at the table level but may be unable to meet regulatory requirements for more fine-grained control at the column or cell level.

There are four main drivers of the Axiomatics authorization strategy:

- Policy modelling to ensure business logic drives access policy
- Graphical and programming tools to assist businesspersons to contribute to policy management
- Policy translation to support diverse IT environments from on-prem to cloud native deployments
- Visualization tools to provide a clear picture of deployed policies across applications and a management dashboard to communicate authorization data in real-time.

Axiomatics supports both on-premises environments and cloud environments. The authorization engine can be deployed in a containerized architecture to meet scalability and resilience requirements. Kubernetes containers and the Docker platform are supported. The latest update of the Axiomatics Services Manager, released in early 2022, is now deployed using Docker containers. Axiomatics is being used in a DevOps lab partnership using an Istio service-mesh with multiple application components accessed via an Envoy proxy, managed via an Istio control plane.

Axiomatics policy-based access management extends beyond support for applications to fine-grained access control for databases, down to the table column and row level. If a user is not authorized to see certain data, those columns/cells will be redacted. Supported datastore includes those accessible Databricks or, Spark. Attribute sources can be pulled from JDBC/ODBC datastores, Collibra, BigID and others.

Policies are built via a drag-and-drop user interface, or the ALFA policy language can be used to code policies, providing developers a high degree of control over policy creation and management. Alfa is now supported via Visual Studio providing an ‘authorization as code’ approach for DevOps staff. The Jenkins tool is typically used for the policy deployment CI/CD pipeline.

Analytics include a policy analysis engine that can perform reverse analysis to understand the entitlements for a particular user. Governance tools include re-certification reports and SoC/SIEM logs.

Axiomatics has created an integration prototype for OPA, to connect to the OPA ecosystem of applications and a policy editor for application owners or business analysts is in development.

Licensing is subscription-based per number of authorized users. It can be scaled up or down to suit an organization's requirements.

Axiomatics maintains strategic partnerships, including MuleSoft and Databricks.

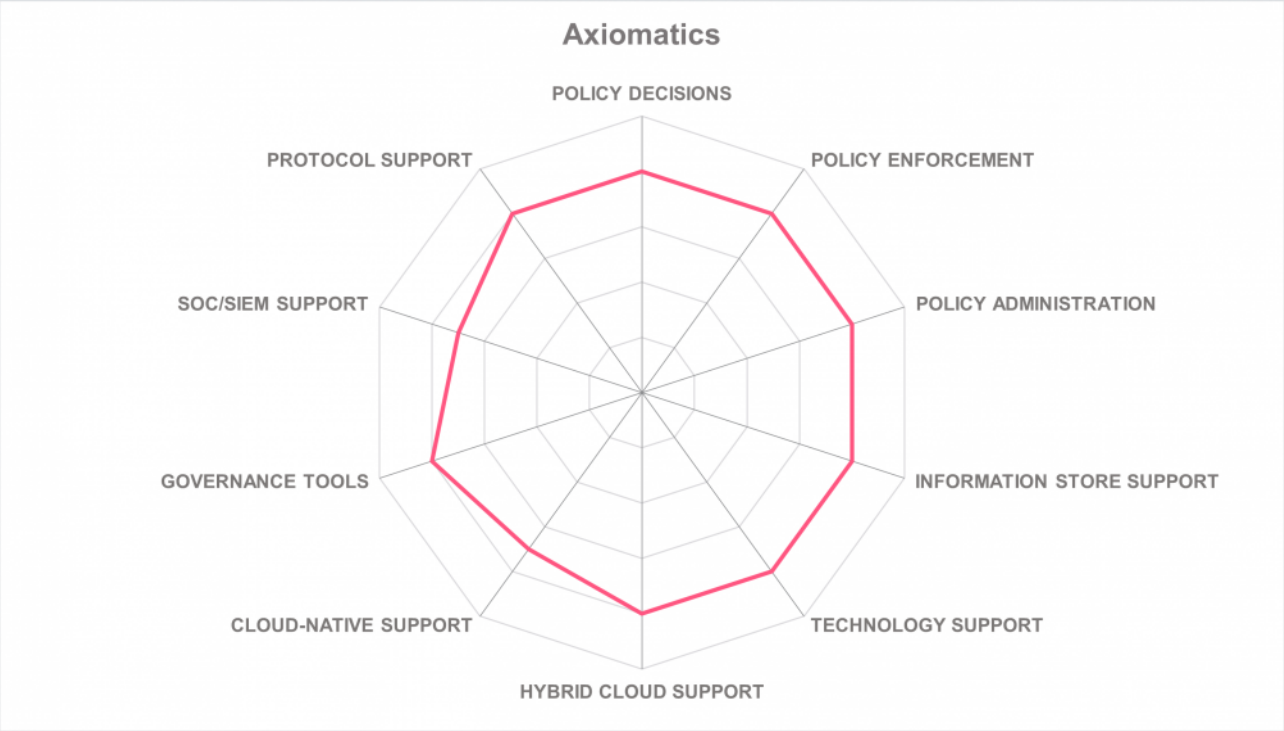
Security	●●●●●
Deployment	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Market Standing	●●●●●

Strengths

- Extensive experience in PBAM with good penetration of the enterprise market
- Support for XACML protocol
- Good policy creation support via ALFA
- Good AI support for policy analytics with data filtering and masking
- Fine-grained database authorization support
- Global presence and partner network

Challenges

- Productizing policy management for micro-services and service-mesh environments
- Unifying policy management across legacy and cloud-native environments
- Support for smaller companies with limited resources


Axiomatics
POLICY DECISIONS
POLICY ENFORCEMENT
POLICY ADMINISTRATION
INFORMATION STORE SUPPORT
TECHNOLOGY SUPPORT
HYBRID CLOUD SUPPORT
CLOUD-NATIVE SUPPORT
GOVERNANCE TOOLS
SOC/SIEM SUPPORT
PROTOCOL SUPPORT

5.3 Cisco

Cisco is headquartered in San Jose, CA, USA. For over 10 years Cisco has been providing the Identity Service Engine (ISE). It enables dynamic access to protected resources via an automated approach to policy management. ISE has become a differentiating point for Cisco in comparison to other suppliers of networking technology. ISE provides sophisticated access control to network devices using Radius authentication.

ISE provides access control to the target network nodes on AWS, with Azure support coming soon. It is typically connected to the organization's AD and will ingest group data to be used with the access control policies set-up in ISE. The solution unifies access control policy across multiple environments, manages policy lifecycle, provides secure remote access, and provides flexibility to maintain critical on-premise functions while centralizing administration in the cloud. An ISE instance is typically deployed in AWS VPCs in selected Availability zone(s), a security group is set up and a VPN is established to on-premise infrastructure with integration to the corporate AD. ISE provides strong horizontal scalability across network segments. An Ansible playbook facility is provided to automate deployment activity.

The ISE maintains an internal identity service that can be set up for real-time access to AD or to refresh the cache on a periodic basis. Network access users can be established directly in the ISE identity datastore.

Policies for network access control are set up in ISE and attached to the nodes they support. Each node has a 'persona' that indicates the access types allowed. The Deployment tab in the UI provides the facility to test polices to determine the policy response for a particular user's access request. The Terraform Visual Studio code editor provides developer support.

Once operational the ISE user interface provides a dashboard indicating the number of authentications, the connected network devices, the connected endpoints, and authentication event alarms. The UI can also show known vulnerabilities and threat events.

ISE can then pass authentication detail, including user context attributes such as device type, via a SAML message to a relying application that can use the data for authorization purposes.

ISE's network device technology can also be used for asset inventory purposes with the dashboard displaying device profile information collected by the network probes on each connected asset in the network. ISE can then be used to assign corporate policies to those assets. ISE AI capabilities provide 'end-point analytics' based on the collected information.

Cisco's ISE has approximately 150 partners that maintain integrations with ISE and can provide global support to Cisco customers. The API documentation provides support for custom integration by Cisco partners.

ISE licensing is based on the number of endpoints being supported. It is available at three levels: Essentials, Advanced and Premier.

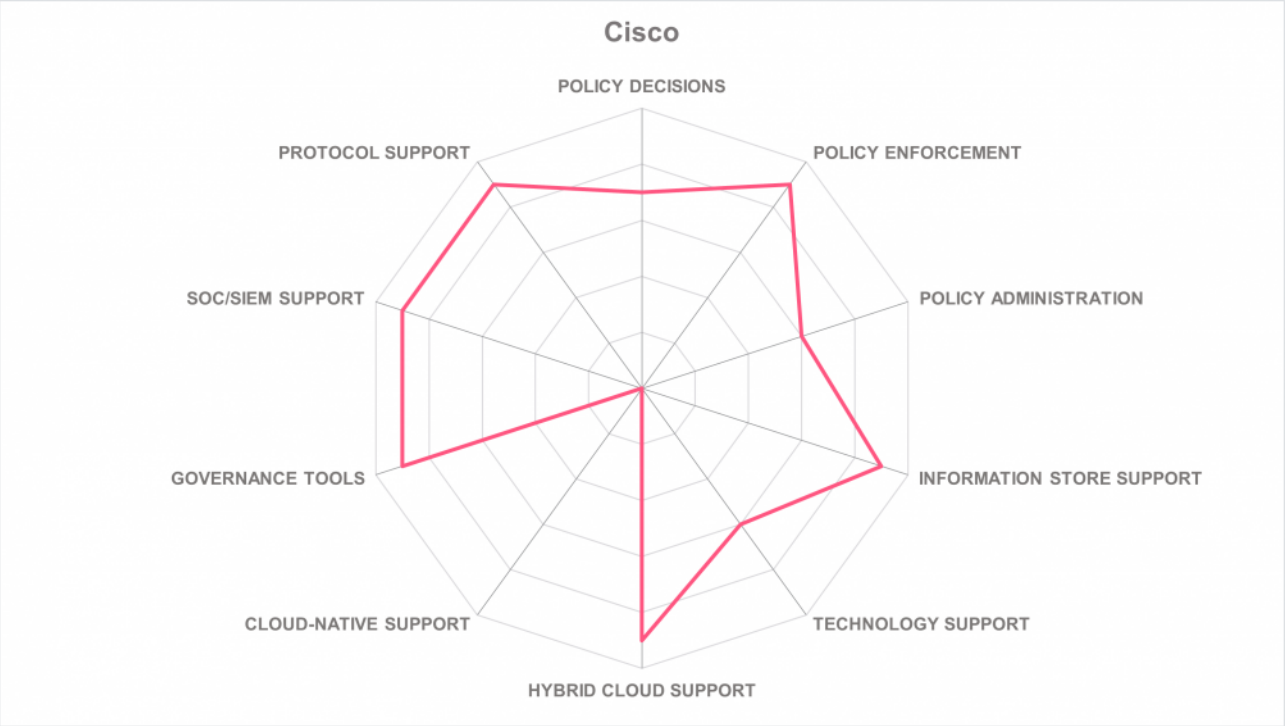
Security	●●●●●
Deployment	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Market Standing	●●●●●

Strengths

- Longevity in the access control market sector
- Strong network authentication capabilities with fine-grained authentication to subnets
- Wide partner network for ISE
- Ability to profile devices from the management UI

Challenges

- Limited support for some cloud environments
- Fine-grained authorization to application features
- Support for smaller companies lacking significant network infrastructure


Cisco
POLICY DECISIONS
POLICY ENFORCEMENT
POLICY ADMINISTRATION
INFORMATION STORE SUPPORT
TECHNOLOGY SUPPORT
HYBRID CLOUD SUPPORT
CLOUD-NATIVE SUPPORT
GOVERNANCE TOOLS
SOC/SIEM SUPPORT
PROTOCOL SUPPORT

5.4 Cloudentity

Cloudentity is a private company headquartered in the US with global coverage via regional offices in the EU, UK, Sao Paolo and Indonesia. The European office is in Poland and the US office is in Seattle. The solution provides a cloud-based service for access control and identity services. The focus is fixing broken corporate Identity Fabrics using externalized policy-based dynamic authorization.

The Cloudentity solution supports multiple and diverse data sources including IdPs (Okta, ForgeRock, AD etc.) and any data source accessible via API, SQL, NoSQL, LDAP or SCIM. Cloudentity unifies the authorization experience across applications and databases at a fine-grained data object level. Cloudentity supports both traditional and modern services with full support for OPA, OAuth, OIDC, SAML and policy portability across cloud environments with direct integrations into Kubernetes, Istio, Functions and the leading API gateway vendors, creating a Zero-Trust Authorization strategy for customers across their application cloud environments. Distributed or decentralized applications are supported through delegated policy administration and policy lifecycle management at various levels: global, tenant, workspace, application and developer.

The Authorization control plane provides either a visual or code-based policy builder for policy creation in Rego, javascript or JSON, and the orchestration of policy lifecycle and authorization services for applications and other protected resources. The management UI generates a graphical depiction of the data sources, the applications, backend services, and the authorization policies they are using, to show how data is being shared internally as well as to external services. The editor assists in the enforcement of privacy and data-sharing consent rules by showing the PII being used by various services and how it's being shared. Cloudentity supports open standards including OIDC/Oauth/JWT to pass identity data, contextual variables, entitlements, and consent details.

Deployment options include public SAAS, private SAAS or a customer VPC. The platform is entirely cloud-native and scales to support hundreds of thousands of token mints and policy decisions per second. The policy decision points can leverage existing OPA agents. Richer functionality such as API discovery is available through the control plane, Authorizers which support API Gateways and microservices APIs. Legacy apps will typically use API access for authorization calls.

The Cloudentity Integrated Development Environment provides tools for code integration and supports developers via the API/service management tool allowing them to select from a library of APIs to suit their specific requirements. API management supports the major API environments including: AWS API gateway, Azure APIM, Istio, Apigee, Kong, NginX and Kubernetes. Cloudentity provides a discovery tool for APIs, microservices and functions, and applies authorization policies in real time to any newly discovered APIs or services. Cloudentity protocol support includes REST, SOAP/XML, GraphQL and gRPC.

The management dashboard uses the Elk stack and reports on new applications/services/APIs found, authorizations performed, most used services, data types being authorized, services alerts and access attacks. The raw stream of events is processed in the SaaS environment and exports via a REST API for real-time monitoring.

Futures include an application builder, an AI based policy creation tool, improved analytics, and enhanced workflows for policy management.

Security	● ● ● ● ●
Deployment	● ● ● ● ○
Interoperability	● ● ● ● ●
Usability	● ● ● ● ○
Market Standing	● ● ● ● ●

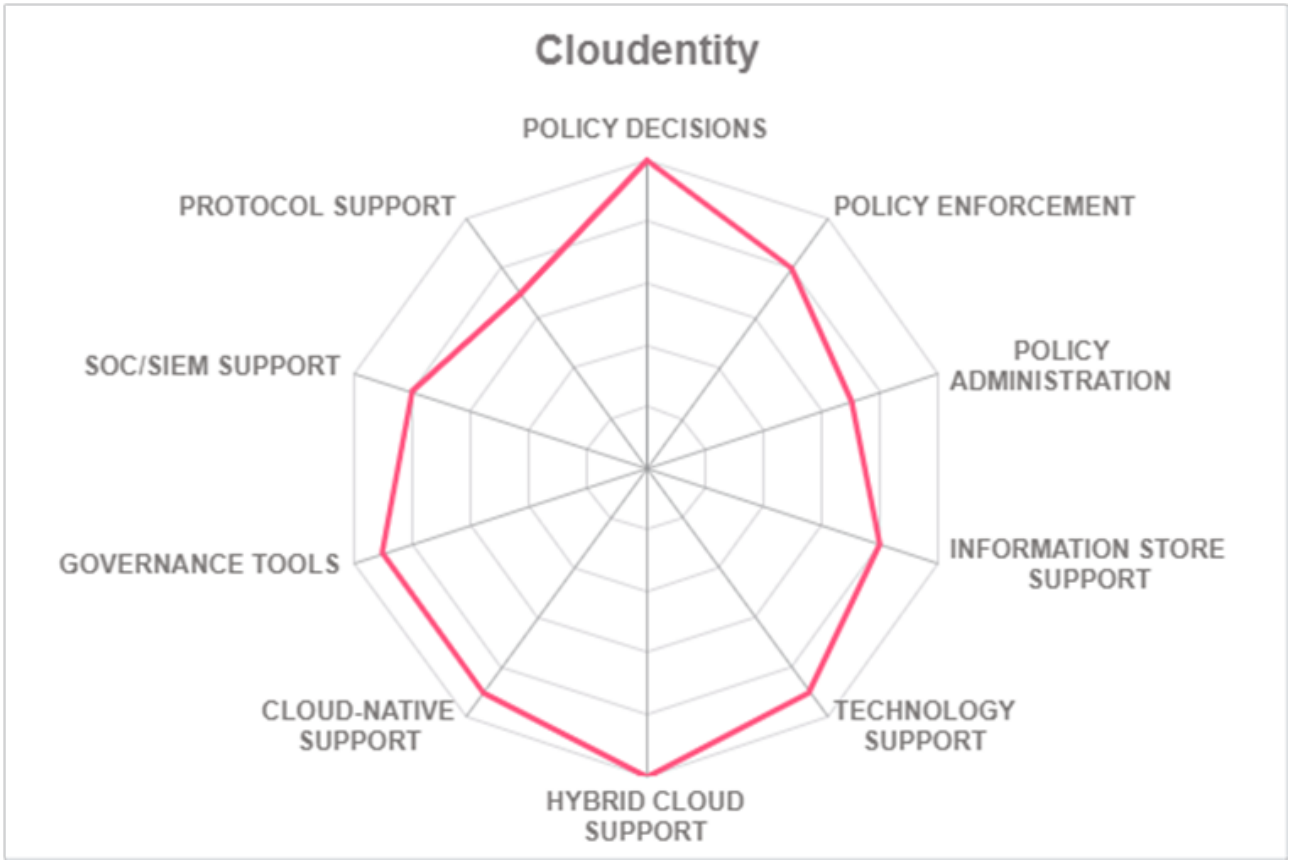
CLOUDENTITY

Strengths

- Support for diverse cloud environments
- Strong support for the developer community
- Real-time monitoring and API support for governance tools
- Automated discovery and on-boarding for services and APIs
- Full-stack authorization for client apps, APIs and microservices
- Delegated administration for B2B and B2b2c scenarios

Challenges

- Limited database support
- Enhanced policy lifecycle management
- Global support for customers lacking proficient DevOps personnel


Cloudentity
POLICY DECISIONS
POLICY ENFORCEMENT
POLICY ADMINISTRATION
INFORMATION STORE SUPPORT
TECHNOLOGY SUPPORT
HYBRID CLOUD SUPPORT
CLOUD-NATIVE SUPPORT
GOVERNANCE TOOLS
SOC/SIEM SUPPORT
PROTOCOL SUPPORT

5.5 EmpowerID

EmpowerID is based in Columbus, Ohio. They are a 'full-service' provider of identity provisioning, entitlement management, diverse deployment support, solid governance capabilities and proof-of-concept support. The Company's focus is on real-time authorization. This can be roles-based, attribute based or policy-based. The solution uses a business role-tree to determine what a user can see or do and to facilitate access control decisions based on established policies. EmpowerID is a strong proponent of User Managed Access (UMA) to allow users to manage consent to their access control preferences to, for instance, IoT devices.

EmpowerID provides REST API support for claims, either on an ABAC basis or via PBAC policies. Data is maintained in a person-object meta directory that allows for normalization of identity data from a variety of data stores. A management console provides entitlement-based access to devices, credentials, role management and micro-service applications, to support cloud applications that are becoming increasingly compartmentalized with each component needing an authorization service, EmpowerID can register components of an application into policy groupings to manage user access. For instance, if a component is enrolled in a web-app group, any user with web-app entitlements will be granted access to the component. In addition, applications can maintain 'controls' that are assigned to users. The management console will display the controls in an application to which a specific user has been assigned. In this way an application can maintain fine-grained control over access to the functions and features it exposes. Rights to specific functionality in an application can be bundled into application roles, that can be explicit i.e., access to a specific device, or generic i.e., access to document folder. Application rights such as 'delete file' can be defined for a specific application or group of applications, this can be very fine-grained; a specific access right can be constrained to a single client or partner.

EmpowerID is also developer friendly. The package exposes APIs that developers can select for specific functionality. Postman collections are available on-line from the EmpowerID application. Onboarding applications are facilitated via the library of existing policies that a developer can use if appropriate. If not, policies can be modified to accommodate required changes and incorporated into new policy sets. Another option is to adopt a gateway proxy approach.

EmpowerID supports cloud native via the OPA model providing a loosely coupled distributed access control environment. Each enforcement point can have an OPA running as a Docker sidecar for fast decision and attribute support. OPA uses generic Rego files in conjunction with pulled-down attributes in JSON data files to support local off-line decisions

Analytic tools include a management interface to evaluate a specific user's access and entitlements within an application. The console displays the JSON code associated with a lookup and returns a 'true' or 'false' result depending on the evaluation of the appropriate policies for a user. Analytic tools are provided that can check and report on application rights, application role groupings, rights to application resources and sharing, and access rights required for APIs. Risk management tools provide risk mitigation via functional analysis of the risk associated with authorization events. Strong governance tools, with a full recertification

engine with workflows and audit capabilities, are provided.

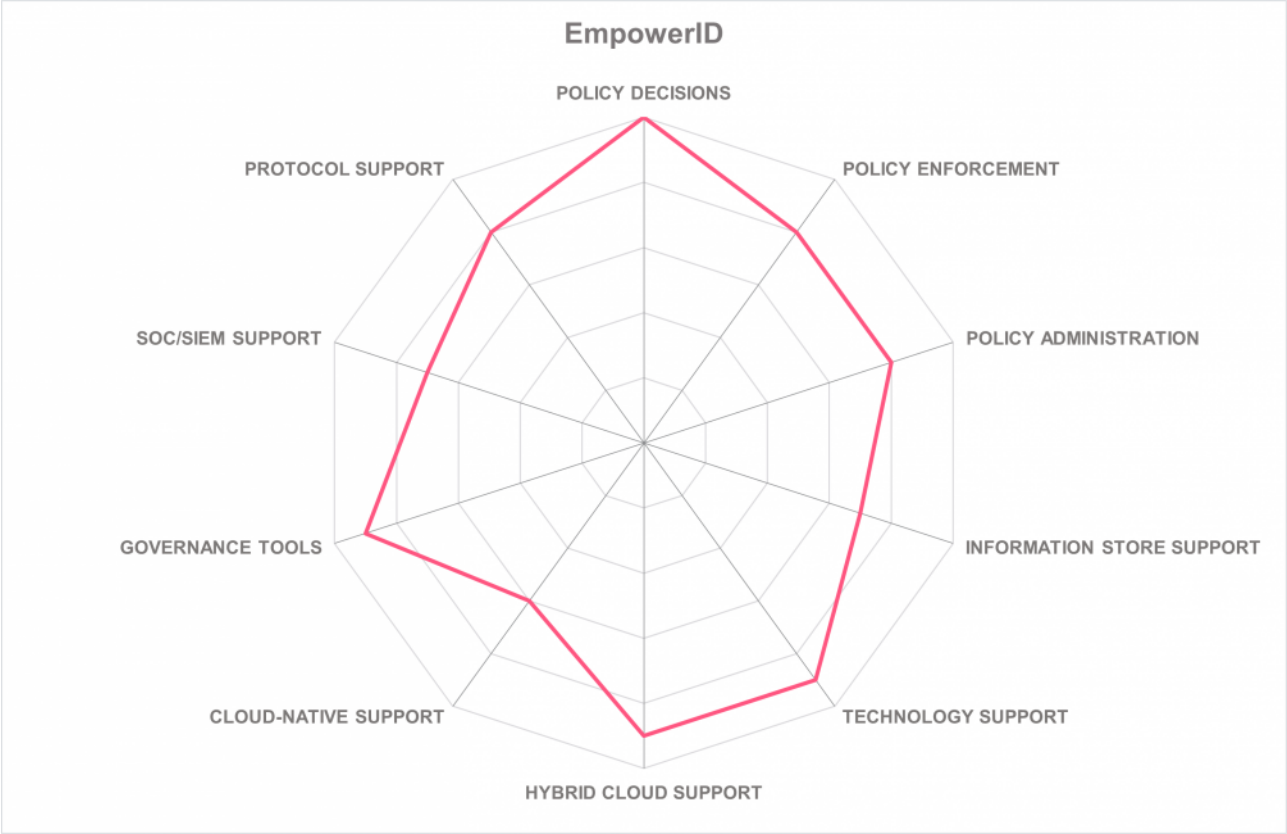
EmpowerID employs subscription- based on the # of managed person identities or active users, not based on the count of AD objects.

Strengths

- Comprehensive identity access control solution
- Rules-tree-based approach to access decisions
- Identity-store cache for rapid response and normalization of data
- Support for software development personnel
- Strong governance tools

Challenges

- Cloud-native service-mesh support
- Support for smaller clients lacking development staff
- Selecting the appropriate cloud-native platforms to support


EmpowerID
POLICY DECISIONS
POLICY ENFORCEMENT
POLICY ADMINISTRATION
INFORMATION STORE SUPPORT
TECHNOLOGY SUPPORT
HYBRID CLOUD SUPPORT
CLOUD-NATIVE SUPPORT
GOVERNANCE TOOLS
SOC/SIEM SUPPORT
PROTOCOL SUPPORT

5.6 NextLabs

NextLabs is a mature vendor in the policy-based access control sector with many patents for dynamic authorization, ABAC & PBAC, runtime enforcement and data-centric security control technology; they are a technology partner for the NIST National Cybersecurity COE (NCCOE).

The Control Centre Server product supports on-premise deployments, the CloudAZ solution is a SaaS application that provides policy management and renders policy decisions. The Control Centre server ingests identity attributes from LDAP, SQL, REST APIs etc., it maintains a policy server, an attribute datastore providing identity attributes, resource attributes and context variables, and an audit server. Policy evaluation (PDP) is available as a cloud service via a microservice container, a virtual appliance, a REST Policy Controller, a Windows Policy Controller or a Java Policy Controller for embedding in relying-party applications. Policy decisions can be rendered via a REST API, an XACML request and response, various SDKs for programming languages, Rego, or via a SAML or OIDC access token which can carry authorization decisions.

Policy enforcement is handled by the microservice architecture with the Cloud Integration module for cloud services, the Dynamic Authorization module for applications and databases, and by the SkyDRM (Digital Rights Management) for unstructured data. Enterprise applications such as SAP, Siemens Teamcenter, SharePoint, and Exchange are fully supported, as are cloud apps such as Office 365, Dynamics 365, Teams, Slack, ServiceNow and Salesforce. All major datastores are supported including Amazon S3, RDS, Dynamo, Aurora & Redshift, Azure File Storage, Azure SQL, Google BigQuery, Cloud SQL & Apigee, and SAP HANA. Additional big data and analytics applications such as Hadoop, SAP Analytics Cloud, SAP BW/4 HANA, Tableau, Power BI, and DBMS are supported. PEP tools include: SAML & OIDC tokens, out-of-the-box PEP code for supported apps, REST or HTTP application proxy, API Gateways, embedded Java runtime code, REST API or custom code using the NextLabs SDK.

Policy administration is very user-centric and supports approval workflow, policy lifecycle, and delegated administration. Policy creation can be achieved via a 'drag-and-drop' natural language interface and policy management follows the NIST reference architecture (NIST SP 800-162).

NextLabs supports diverse deployment models. The SaaS model is the most prevalent but hybrid models with an on-premise component, or fully on-premise with either Windows or Linux environments. VMware OVA environments or Kubernetes deployments are also fully supported via an no code/low-code automation for deployment of authorization services for container sidecars. The Control Centre provides separate services for the policy validator, the policy controller, the management server as well as administrator and reporter modules.

NextLabs maintain a number of policy analysis and audit tools to support governance. Policy models and a standard taxonomy are initially established and policies can be previewed to validate correct decisions. A full policy life-cycle management approach with a set of policy validation processes and approval workflows is supported. Policy libraries can be assigned to specific users to foster policy collaboration across business units.

An API hub is maintained for publishing microservices APIs. Rego code can be created via NextLabs 4GL tool. RedHat's OpenShift platform is supported as well as Terraform for deployment.

Mainstream IdPs such as AD, LDAP, Azure AD and Okta are supported, and a SAML service is also provided.

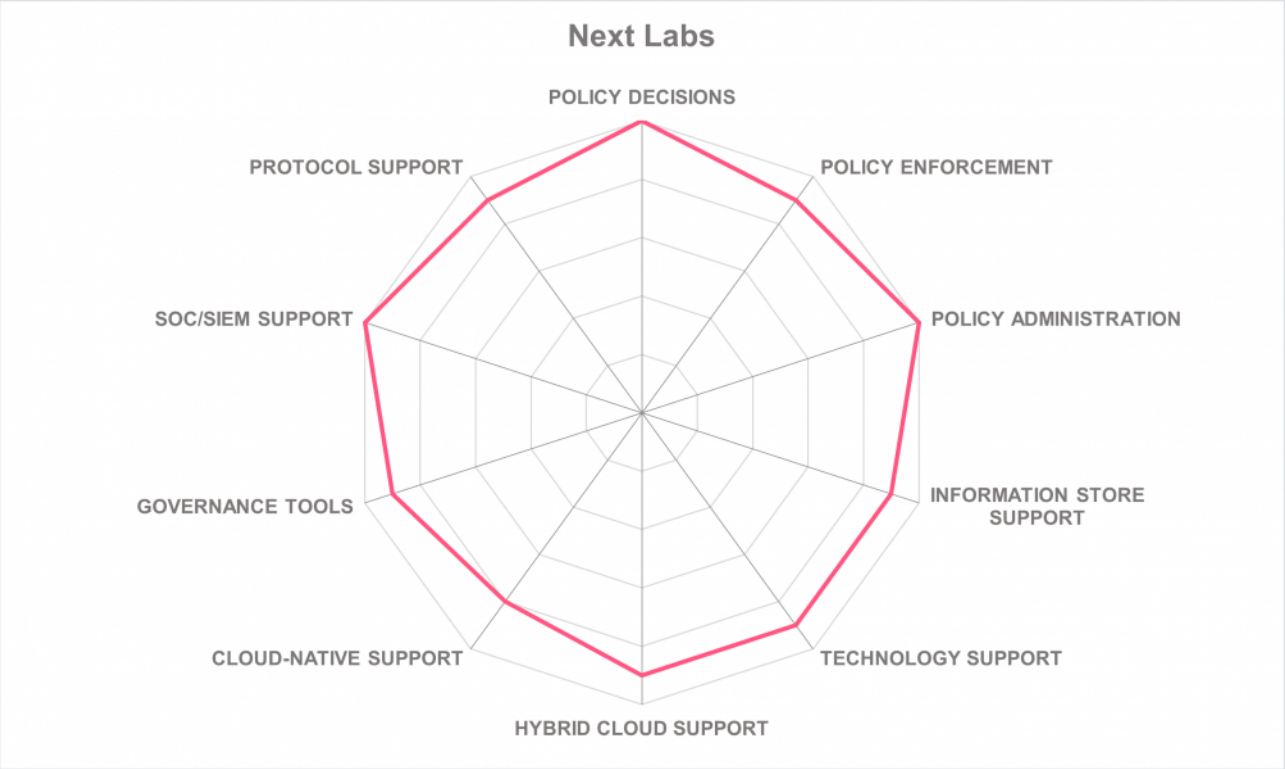
NextLabs offers a flexible user-based subscription model.

Strengths

- Extensive experience in the access control market and ABAC/PBAC deployments
- Support for diverse deployment models
- Strong governance capabilities
- Microservices API publishing support
- User-based licensing model

Challenges

- Provision of policy set deployment tools for developers
- Support for smaller companies lacking DevOps personnel
- Supporting a true service-mesh environment


Next Labs
POLICY DECISIONS
POLICY ENFORCEMENT
POLICY ADMINISTRATION
INFORMATION STORE SUPPORT
TECHNOLOGY SUPPORT
HYBRID CLOUD SUPPORT
CLOUD-NATIVE SUPPORT
GOVERNANCE TOOLS
SOC/SIEM SUPPORT
PROTOCOL SUPPORT

5.7 Okera

Okera was founded in 2016 by technology innovators in the big data sector. The company was established to address the increasing need to expand big data analytics and data science, to more users, and to do so in a way that protects confidential, PII, and regulated data. Okera is focused on dynamic data authorization for data stores, not applications. This enables organizations to apply consistent data control policies across a wide variety of data storage and compute environments, such as Amazon S3, EMR, Redshift, and Athena; Azure ADLS and Synapse; Google File Store and BigQuery; Snowflake, Databricks, Dremio, Starburst, Cloudera CDP, and more.?

Most of Okera's clients are in financial services and FinTech. Financial data, while generally better protected, is often open to abuse from down-stream processing. The recent adoption of open banking in many jurisdictions requires banks to make their customer data available to third party payment providers, necessitating strong access controls. Often, data lakes and other cloud data warehouses are inadequately protected leaving them open to 'leakage' or they are locked down such that analysts and data scientists cannot access even the non-sensitive information within them for legitimate business purposes. ?

Okera 's solution rectifies this vulnerability by allowing consistent access control policies across multiple data stores to be deployed. A UI is provided for all data stakeholders, including security and Data Protection Officers, to collaborate with the technical implementation team to ensure that data protection policies are implemented and applied consistently across all data platforms, cloud-based or on-premise. The mission of Okera is to "Enable everyone to use data responsibly."???

Okera functionality is provided through four core components:

- Automated Data Classification. Detection and classification of data is the key to simplifying and standardizing data access control. Okera can scan, detect, and classify data for attributes such as PII, and it can integrate with classification tools such as Alation, BigID, and Collibra, and AWS Glue or Hive Metastore catalogs and can read tags directly from Snowflake.?
- Universal Policy Management. Okera separates the policy from the platform enabling all data stakeholders to collaborate on policy definition such as which users can access PII data or location variables. Data from different platforms such as Snowflake, Databricks, or S3/ADLS/GFS data lakes are then registered for enforcement by the policies. Okera offers distributed stewardship, supporting data mesh and similar federated data management models.?
- Dynamic Policy Enforcement. Okera integrates with enterprise authentication and Single Sign-On (SSO) solutions such as oAuth, SAML (Okta, Ping), Microsoft Active Directory. The policy engine supports multiple enforcement patterns and makes real-time decisions on how to enforce queries. Okera's optimized enforcement ensures low-latency response and supports hybrid deployments, facilitating

cloud migrating and can multi-cloud data workloads.?

- Policy Audit and Sensitive Data Usage Intelligence. InfoSec, data protection officers, and auditor are given privileged access to see who has access to sensitive data and when a policy was changed, by whom and through what methods.

Okera works closely with the major cloud providers such as AWS, Azure, and GCP to streamline data access governance in multi-cloud and hybrid cloud environments.

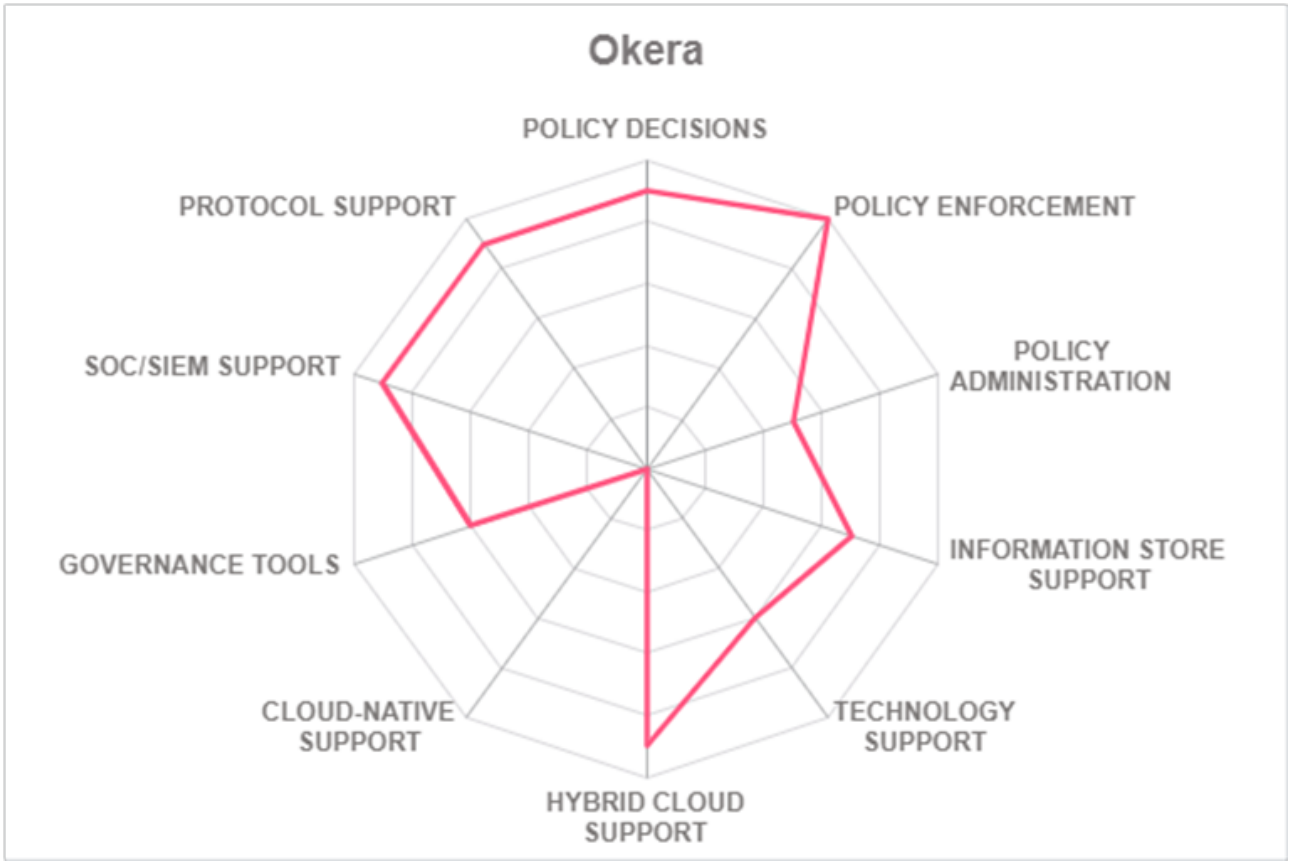
Licensing is subscriber-based on the number of users.

Strengths

- Comprehensive database access control
- Unified identity attributes across an organization
- Consistent policy management across data repositories
- Support for mainstream identity data sources
- Good governance tools to report on database access history

Challenges

- Support for a services-mesh environment
- Integration with policies for access control to applications
- Provision of DevOps tools


Okera
POLICY DECISIONS
POLICY ENFORCEMENT
POLICY ADMINISTRATION
INFORMATION STORE SUPPORT
TECHNOLOGY SUPPORT
HYBRID CLOUD SUPPORT
CLOUD-NATIVE SUPPORT
GOVERNANCE TOOLS
SOC/SIEM SUPPORT
PROTOCOL SUPPORT

5.8 PlainID

PlainID's goal is to connect any kind of identity (employee, business partner, customer, machine account, system account) to any application, service, or database. The target sector is enterprise customers.

The PlainID Policy Manager product can be installed on customer infrastructure (cloud, hybrid etc.) or it is available on a SaaS basis. The core authorization service consists of a policy decision point, a policy management tool, and a policy information repository. At the Application level the authorization service communicates with an enforcement point agent integrated with each application. If an API gateway is being used a PlainID agent is deployed on the gateway devices. In a cloud-native environment a PlainID sidecar provides the authorization service to the microservices API. If fine-grained access to a database is required, a PlainID interceptor is employed to protect access to the data.

PlainID provides a comprehensive PBAM solution: a graphic policy authoring tool, with all the necessary features for lifecycle management of policies including approval workflows and version control, a rich PIP running on an open-source data visualization service, with identity context management supporting a wide range of identity data sources, and a PDP run-time interface to provide permit/deny decisions, user token management and policy resolution for database access.

PlainID's authorization strategy focuses on centralized management (creating policies, auditing etc.) but distributed enforcement, providing low-latency authorization support service multi-cloud environments. This enables PlainID users to maintain a consistent policy strategy across the organization, collapsing silos of access control that otherwise might exist. It also supports diverse application environments in which corporate resources are deployed across multiple, and different, infrastructures. The policy manager is a single management platform but supports delegated administration to allow policy management at a business-unit level. A policy analytics tool supports the governance task.

In a cloud-native environment a 'microPDP' sidecar supports an Envoy proxy to service the relying party app container. It can provide a simple permit/deny decision or can enhance the authentication with additional attributes. Istio is supported, Consul, Kuma, Linkerd and Grey Matter service meshes are planned. PlainID supports the OPA model.

Data access with row and column filtering is provided. Google BigQuery, Denodo, Dremio, Data Virtuality are supported, Snowflake and Cloudera support is imminent.

IdP's supported include Okta, Ping, SAP, Auth0 and Azure.

PlainID's governance tools include policy analytics, with a full audit trail for policy modification provided, as well as a simulation tool for 'what if' scenarios.

PlainID's licensing supports both customer-deployed or SaaS via subscription-based licensing.

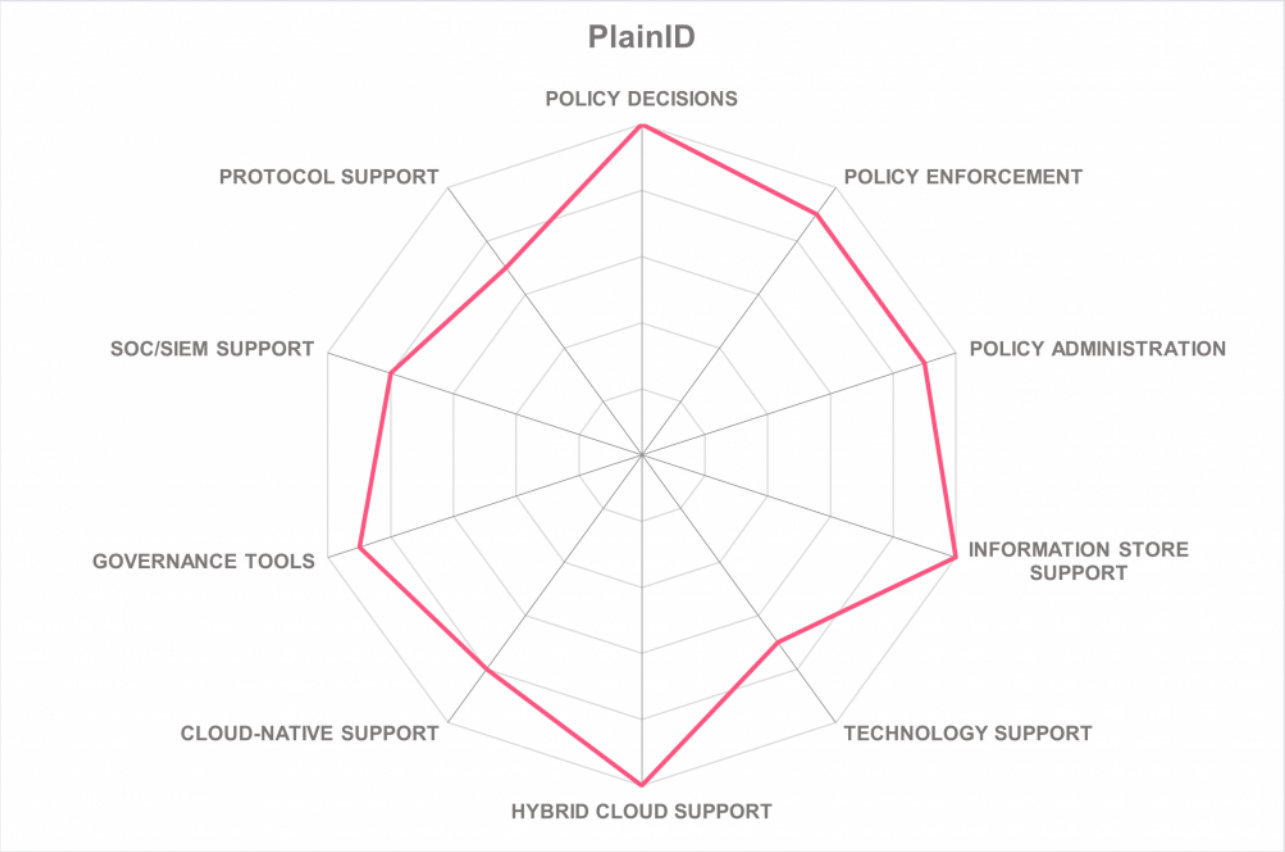
Security	● ● ● ● ●
Deployment	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Market Standing	● ● ● ● ●

Strengths

- Hybrid support for diverse access control environment deployments
- Sidecar support for containerized cloud environments
- Graphical policy authoring tool
- Database access control features
- Mainstream identity data sources are supported

Challenges

- Support for true micro-services environments & OPA
- Extension of hierarchical policies to cloud-native deployments
- Provision of DevOps deployment tools for CI/CD to micro-services


PlainID
POLICY DECISIONS
POLICY ENFORCEMENT
POLICY ADMINISTRATION
INFORMATION STORE SUPPORT
TECHNOLOGY SUPPORT
HYBRID CLOUD SUPPORT
CLOUD-NATIVE SUPPORT
GOVERNANCE TOOLS
SOC/SIEM SUPPORT
PROTOCOL SUPPORT

5.9 Scaled Access

Scaled Access was established in Belgium and was recently acquired by OneWelcome to provide a powerful policy management engine to their identity platform. The Scaled Access solution takes a unique approach to access control. Recognizing the agile nature of identity data and its dependence on relationships, Scaled Access uses a graph database as its core repository upon which it determines access entitlements. This allows Scaled Access to provide a rich, context-aware authorization environment. Scaled Access uses three different integration patterns in its support of relying party applications:

- Token Enrichment - In this pattern Scaled Access provides IdP + services, adding context data to the access control decision to allow the relying party application to provide better authorization to requested services
- Provisioning - Scaled Access establishes the user node and relationship data to the graph database to support policy decisions
- Policy Decision Endpoint- Scaled Access sends a JSON file to a REST API to render an access decision, allowing management of the level of detail to be communicated to the relying application.

Establishing the graph database with the user nodes and appropriate relationship data is core to the operation of Scaled Access. This is achieved via a graphical interface that provides a depiction of each user entity and associated relationships. In a healthcare environment a doctor-node is typically connected to a health care facility and a patient-node is connected via a relationship that defines the patient's consent for access to their health record. A nurse-node can be attached to the health care facility with another relationship that defines their permitted access to the patient's healthcare data. The graphical policy editor also incorporates a text description of the selected nodes and relationships to assist developers. The graph database provides a competitive advantage for Scaled Access in its ability to manage a rich domain model allowing relationships to be used in policy decisions. Each user is a node in the database and the domain model governs the relationships between the components of the model. This means that there are no constraints on the attributes of a node whether it be an employee, contractor, business partner or a customer. Relationships can be queried for analytical purposes to provide governance reporting on user access entitlements to protected resources.

Policies can be managed graphically via the policy engine that facilitates visualizing and testing policies, including approval workflows. Alternatively, policies can be created and altered via Rego code. Scaled Access supports a traditional PDP approach with subject-action-object policies using JSON rather than XML. A REST API can be locally supported for fast response.

Scaled Access also implements consent management with full life-cycle control of consent scope and maintenance of consent records. This allows Scaled Access to satisfy multiple IdP governance requirements. For instance, if the IdP is a government database there will be multiple conditions in the

provision of data and a need to comply with regulation in the jurisdiction. Scaled Access can gather the appropriate consent to access and share data. It can also combine local (self-managed) consent constraints and, with the graph database is such a rich source of additional attributes, other data can be added to enhance the user experience.

Scaled Access fully supports OAuth2.0 with authorization decisions in custom claims, or it can set the scope in an access token. The product is licensed on a user-based subscription model.

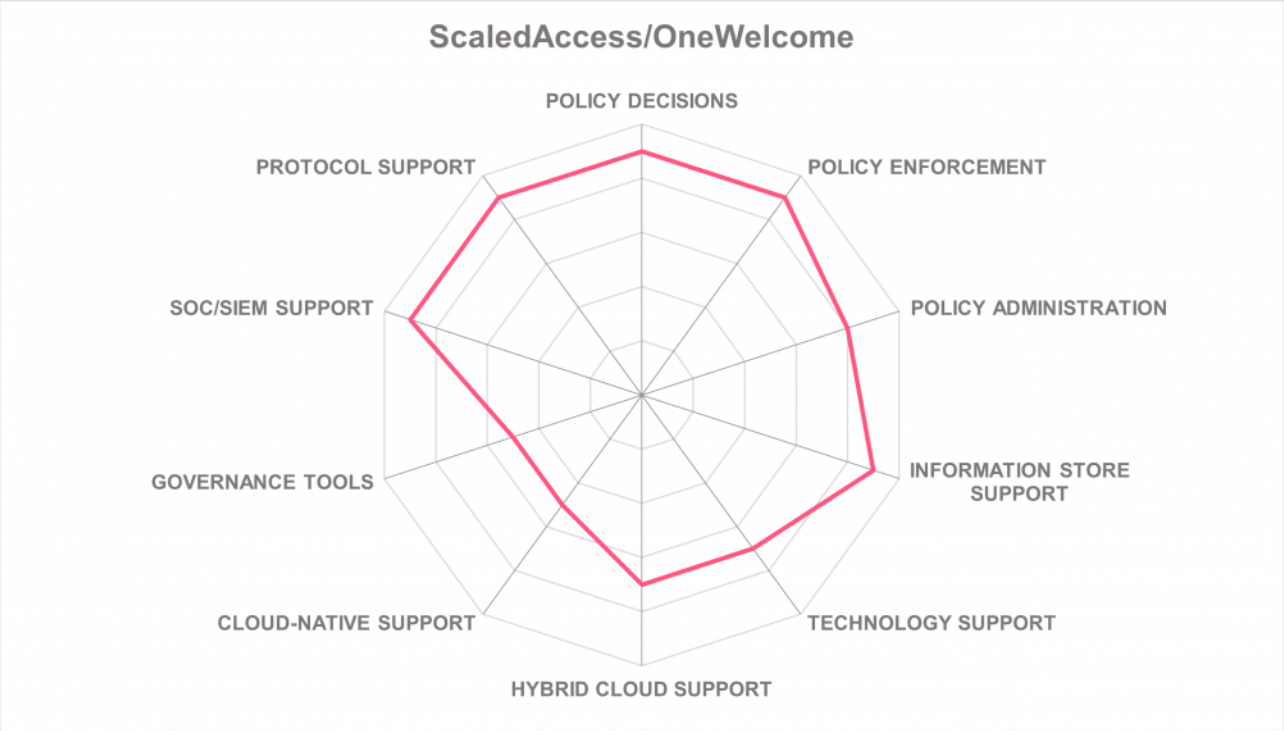
Security	● ● ● ● ●
Deployment	● ● ● ● ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ● ●
Market Standing	● ● ● ○ ○

Strengths

- Relationship-based identity store on a graph database
- Graphical tool for policy management
- Ability to enhance identity records for fine-grained access control
- Ability to manage consent-based access control
- License costs based on number of users

Challenges

- Satisfying enterprise-level governance requirements
- Supporting fully cloud-native environment
- Limited customer support in some geographies


ScaledAccess/OneWelcome
POLICY DECISIONS
POLICY ENFORCEMENT
POLICY ADMINISTRATION
INFORMATION STORE SUPPORT
TECHNOLOGY SUPPORT
HYBRID CLOUD SUPPORT
CLOUD-NATIVE SUPPORT
GOVERNANCE TOOLS
SOC/SIEM SUPPORT
PROTOCOL SUPPORT

5.10 Strata Identity

Strata Identity, Inc was established in 2019 by personnel with long experience in the identity access management sector. The company is head-quartered in Boulder, Colorado with a branch office in Canada.

Strata's Identity Orchestration platform is called 'Maverics'. It provides a cloud entitlement solution across a multi-cloud identity fabric.

Maverics is a comprehensive solution for cloud platforms, supporting both \'north-south\' authorization for a user access an application, and 'east-west' authorization to support the authorization service required by myriad micro-services in a service mesh environment

Logically the platform sits between the various sources of identity data and the multiple relying parties. It provides authentication and authorization services based on pre-defined access control policies. The product is the glue between identity data and relying containerized applications or micro-services APIs. Strata.io incorporates integrations with Oracle E-Business Suite and IBM Application Server technology as well as supporting just-in-time connections to other corporate applications.

The intent of Maverics is to:

- Decouple apps from deep identity integrations via a distributed abstraction layer
- Consolidate fragmentation caused by multiple solutions requiring identity data
- Relieve lock-in to legacy IAM, multiple IdPs, or other identity components
- Integrate dis-organized policies into consistent policy sets
- Allow for coexistence of multiple relying parties in a hybrid environment.

Maverics removes the need to write custom code in order to integrate disparate identity solutions or to integrate relying party apps. This is especially important when support for multi-cloud environments is required. It supports the roll-out of services such as MFA to provide elevation of authorization assurance levels.

The product consists of several core components that are brought together in a single identity orchestration solution that serves both hybrid (on-prem & cloud) and multi-cloud installations. That means there is consistency in policies managing access across an organization's diverse environment.

Policies can be created and managed via a programming interface using a declarative, human-readable format and via a SaaS-based wizard. Policies can also be inferred from IdPs with access policies ingested into Maverics. OPA 'bundles' are supported providing business unit segmentation of policy deployment. Strata's 'policy-as-code' approach supports developers deploying across multiple environments.

Strata personnel are active in the combined development of the IDQL protocol standard and the reference

implementation for Hexa policy orchestration. Future development includes a focus on policy analytics to control proliferation of policies and to provide better governance. Enhanced event management is also planned.

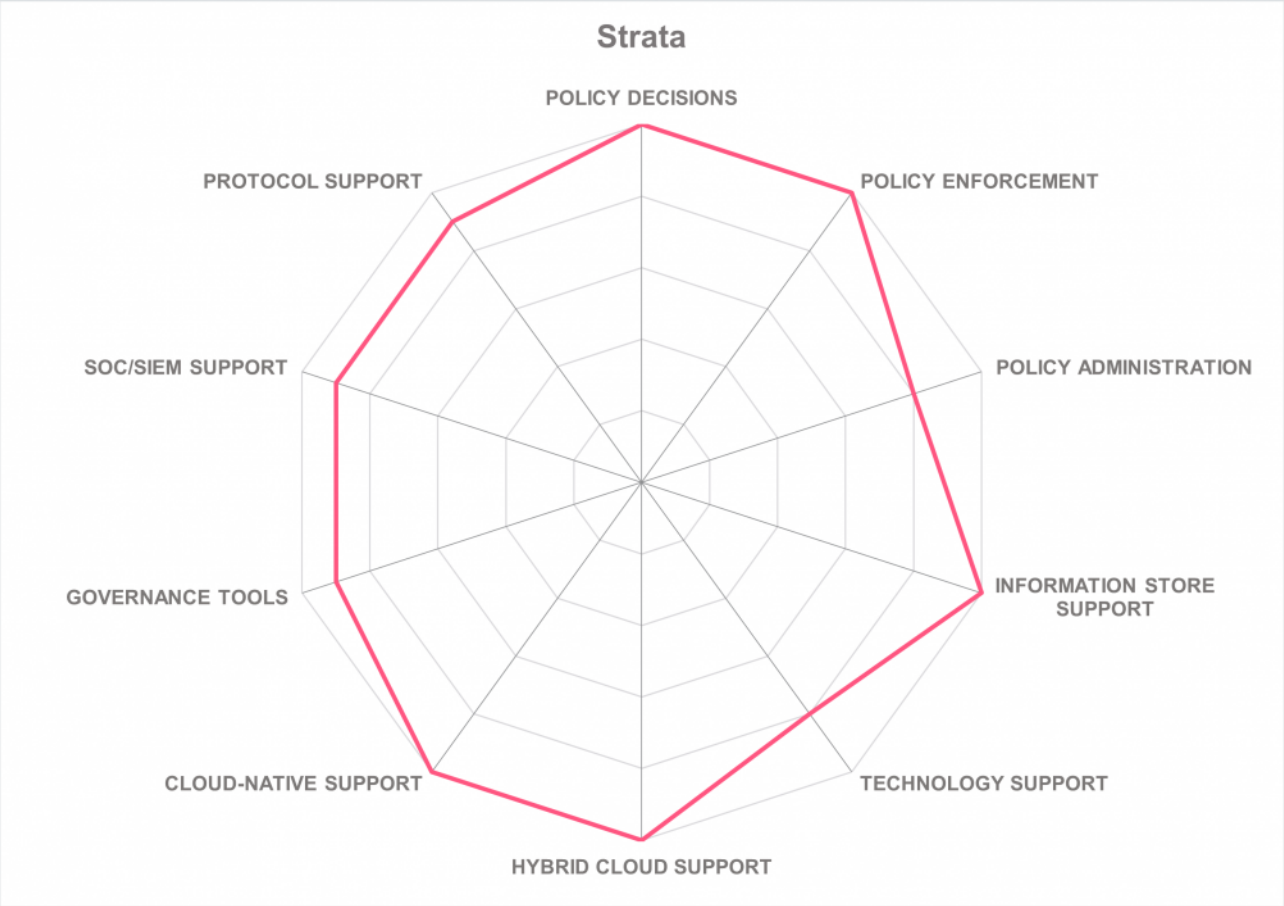
Licensing for the solution is based on the number of connections that are maintained to IdPs and the number of relying party applications.

Strengths

- Comprehensive access control solution with inferred policy capability
- Policy management via programming interface or SaaS app
- Unified and consistent policy management
- Strong cloud-native support
- Licensing based on connections and supported applications rather than users

Challenges

- Interface development for on-premises applications using internal authorization
- Policy administration support for business-unit hierarchies
- Support for smaller companies with limited DevOps capability


Strata
POLICY DECISIONS
POLICY ENFORCEMENT
POLICY ADMINISTRATION
INFORMATION STORE SUPPORT
TECHNOLOGY SUPPORT
HYBRID CLOUD SUPPORT
CLOUD-NATIVE SUPPORT
GOVERNANCE TOOLS
SOC/SIEM SUPPORT
PROTOCOL SUPPORT

5.11 Styra

Styra Inc was founded in 2015 in the San Francisco Bay Area. While headquartered in Redwood City, CA, the company operates on a fully remote basis..

The company's mission is to rethink the policy and authorization for cloud-native environments. The company's goal is to become the de facto policy & compliance solution for cloud native ecosystems. Styra's Open Policy Agent (OPA) open source project was donated to the Cloud Native Computing Foundation in 2018. The company's flagship product is called Styra Declarative Authorization Service (DAS).

As we migrate from monolithic cloud deployments where the requirement is to enforce 'who can get to what', to a microservices cloud environment where the authorization task is more nuanced, microservices need to externalize the 'who can get to what' and 'what can get to what' decisions.

In cloud native environments there is a abundance of tools, and more are coming. Envoy is an open-source service proxy, Istio and Kuma provide service mesh frameworks, Apigee and Kong provide microservices connectivity platforms. The OPA framework is therefore vitally important to provide a common way to communicate with authentication APIs, OPA defines a method to instantiate access control policies. The intent of Styra DAS is to support an organization's preferred platform via OPA.

The Styra DAS solution assists in managing access control complexity. For instance, if there is a GDPR (General Data Protection Regulation) compliance requirement to control the type of personal data that can be accessed from a database, Styra can ensure that a user's access via the API to the data store is appropriate.

Source identity attributes can be ingested from multiple IdPs with integrations to LDAP, AD, Okta, SCIM, HTTP, S3 datastores etc. and data transformations can be performed to suit the desired object model. The frequency of updates is configurable.

The Styra solution provides strong support for DevOps staff. In a cloud-native environments the DevOps unit will typically manage the authorization environment and ensure relying micro-services and cloud infrastructure are adequately served. In order to include IAM staff in the process the Styra DAS UI provides the capability for collaboration. The policy packs allow authorized persons in the organizationto view the policy-as-code used to make decisions, as well as the results of those decisions over time. DAS comes with out-of-the-box policy packs that can be modified for organization-specific requirements, and provides full lifecycle management for custom OPA policy from authoring, to testing, to deployment and audit. Policy hierarchy supports inheritance, policies down the hierarchy inherit parent policies and separation of duties (SoD) policies can be instantiated via this hierarchy. When policies are published, DAS supports developers by ensuring that appropriate policy "bundles" are pushed to relevant OPA instances, and kept up-to-date as needed.

Styra DAS supports an organization's governance hierarchy by providing full visibility over policy

management allowing groups within the company to view applicable policies to ensure their requirements are being met. Authorized users can track, log and audit policies by displaying the ‘allows’ & ‘denies’ associated with a policy evaluation. DAS also addresses the governance requirement by providing a tool to monitor policy development and modification. It can perform impact analysis on policies before, during and after changes. The UI displays policies for the selected system cluster. In the event of a compromise Styra DAS can be used to shut down access to a system. The DAS UI can then assist in forensic analysis to determine potential vulnerability points.

Styra DAS is subscription based and pricing varies based on the size and configuration of the environment under management.

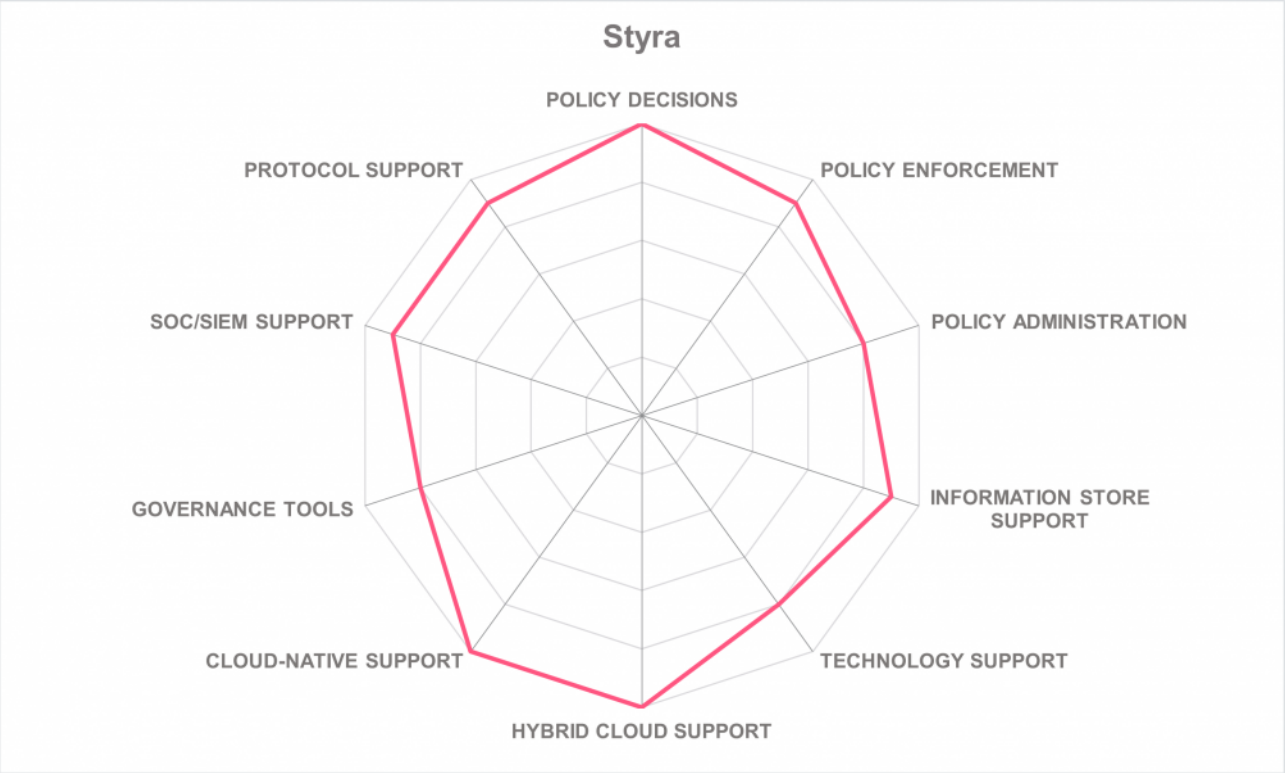
Security	●●●●●
Deployment	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Market Standing	●●●○○

Strengths

- Strong cloud-native support
- Good Developer support tools
- Intuitive user interface for policy management
- Configuration-based licensing

Challenges

- Support for legacy environments
- Governance tools for policy analysis and recertification.
- Policy management support for business personnel


Styra
POLICY DECISIONS
POLICY ENFORCEMENT
POLICY ADMINISTRATION
INFORMATION STORE SUPPORT
TECHNOLOGY SUPPORT
HYBRID CLOUD SUPPORT
CLOUD-NATIVE SUPPORT
GOVERNANCE TOOLS
SOC/SIEM SUPPORT
PROTOCOL SUPPORT

6 Vendors to Watch

Besides the vendors covered in detail in this document, we observe other vendors in the market that readers should be aware of. While not fully fitting the market definition, other vendors offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document or for their unique methods of addressing the challenges of this segment.

- **Aqua Security** provides a platform for cloud-native deployments that secures the development work, secures deployment on cloud infrastructure, and improves the security of application workloads. The focus is on DevSecOps support to bring order and management to the software development task and apply controls over deployment automation.

  Aqua provides security to Kubernetes containers, scans for vulnerabilities and performs threat analysis to advise programming staff.

- **Authomize** is a company focused on automating the management of access control environments. The goal is to provide heightened visibility over the privileges assigned to persons and entities for access control to relying party applications and resources. The solution can ingest identity data, SSO detail, SaaS entitlements, and more, to provide visibility to the access privileges afforded individuals across multi-cloud environments. Authomize can then apply security analytics to expose risk and gauge compliance with access governance policy. Authomize's ML capabilities include recommendations for improvements to raise security and facilitation of audit and attestation activity. Authomize can automate the identity lifecycle processes to enforce a least-privilege approval to access control.

  While Authomize does not provide a policy-based access control solution, they enable clients to reach an enhanced level of security more quickly, providing a shorter time to market without the need to engage experienced personnel.

- **Axway** is a leader in the provision of API gateway functionality. With their focus on architecture Axway provides an enterprise-grade approach to management and security of a gateway-based deployment to facilitate the connection of applications, mobile devices, IoT devices and third-party systems.

  The API Gateway enables real-time monitoring and analytical reporting across an IT environment, providing API usage data and informing governance systems.

- **ForgeRock** is a leader in identity and access management solutions. The Identity Gateway product provides identity data support to authentication and authorization services across disparate environments, from on-premises to multi-cloud to cloud-native deployments.

  The Gateway bridges legacy applications and modern infrastructure to provide seamless connectivity that raises the security of cloud apps and enables microservice APIs, in order to accelerate the

enterprise digital transformation journey.

- **Okta** is a leader in cloud-based access management services and in the provision of Identity-as-a-Service offerings. The Okta Integration Network offers a broad set of integration capabilities across multiple, and disparate, cloud service providers.

  The IDaaS solution supports multi-factor authentication and elevation of privileges to raise the assurance level of an authentication event. Okta have also acquired Auth0 to expand their capabilities in the provision of sophisticated identity-based solutions for cloud infrastructure.

- **Ping** is a leader in identity and access management services which includes an Identity-as-a-Service offering. Ping maintains a wide number of connectors to platforms, productivity tools and collaboration services.

  The Symphonic acquisition brings a policy-based authentication capability to the Ping solution with support for a wide selection of enforcement protocols to suit both on-premises and cloud deployments.

- **TrustBulder.io** integrates multiple IdPs and uses the data to provide authentication services to users accessing protected resources. The ID Hub is the core component that maintains the identity data and policy store. The mobile authenticator module provides multi-factor authentication, and TrustBuilder.io provides connections to third party identity services

  Together the components comprise a rich environment that supports both on-premises and cloud deployments with a comprehensive and dynamic authorization orchestration service. Strengths are the ability to integrate third party IdPs and applications with a robust federated authentication service and the graphical workflow tools to accelerate time to market when deploying the solution.

7 Related Research

80517 Leadership Compass Access Control Solutions for SAP and other Business Applications
80802 Leadership Brief Prepare and Protect against Software Vulnerabilities
80279 Advisory Note Redefining Access Governance

Methodology

About KuppingerCole's Market Compass

KuppingerCole Market Compass is a tool which provides an overview of a particular IT market segment and identifies the strengths of products within that market segment. It assists you in identifying the vendors and products/services in that market which you should consider when making product decisions.

While the information provided by this report can help to make decisions it is important to note that it is not sufficient to make choices based **only** on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e., a complete assessment.

Product Rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Deployment
- Interoperability
- Usability
- Market Standing

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and

the way the vendor deals with them.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

Market Standing is a measure of financial strength and market position. This is based on publicly available information, and takes the amount of funding received, the profitability, and the private or public status of the vendor into consideration.

We focus on security, deployment, interoperability, usability, and market standing for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

Rating scale for products

For vendors and product feature areas, we use a separate rating with five different levels. These levels are:

- **Strong positive**

Outstanding support for the subject area, e.g. product functionality, or security etc.)

- **Positive**
  Strong support for a feature area but with some minor gaps or shortcomings. Using Security as an example, this could indicate some gaps in fine-grained access controls of administrative entitlements.

- **Neutral**
  Acceptable support for feature areas but with several of our requirements for these areas not being met. Using functionality as an example, this could indicate that some of the major feature areas we are looking for aren't met, while others are well served.

- **Weak**
  Below-average capabilities in the area considered.

- **Critical**
  Major weaknesses in various areas.

Content of Figures

Copyright

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.