

KuppingerCole Report

MARKET COMPASS

By **Graham Williamson**
July 14, 2020

Dynamic Authorization Management

The KuppingerCole Market Compass provides an overview of the product or service offerings in a selected market segment. This Market Compass covers the Dynamic Authorization Management market and provides a comparison of the main product offerings. Dynamic Authorization externalizes access control decisions to a centrally-managed authorization service that evaluates access policies in real-time to permit or deny a user's access request to resources.



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

Content

1 Management Summary	3
2 Market Segment	5
2.1 Market Description	5
2.2 Market Direction	7
2.3 Capabilities	10
3 Vendors and Products	12
3.1 Vendors Covered	12
3.2 Featured Vendors	12
3.2.1 Featured for Capabilities: Axiomatics	13
3.2.2 Featured for Innovation: PlainID	13
3.2.3 Featured for Usability: NextLabs	14
3.2.4 Featured for Usability: Symphonic Software	15
3.3 Vendors to watch	16
4 Ratings at a glance	17
5 Product/Service Details	20
5.1 Atos	21
5.2 Axiomatics	24
5.3 EmpowerID	27
5.4 Jericho Systems	30
5.5 NextLabs	33
5.6 PlainID	36
5.7 Symphonic	39
5.8 WSO2	42
6 Related Research	45
Methodology	46
Content of Figures	49
Copyright	50

1 Management Summary

This KuppingerCole Market Compass addresses the market segment for Dynamic Authorization Management (DAM). DAM is part of the Access Management market sector and focused on access control via run-time evaluation of policies. These solutions externalize access control decisions to a policy-based authorization server.

Authorization (AuthZ) is the act of verifying a user's entitlements that grant them access to a specific controlled resource. This is often performed within a computer via an internal store of user accounts and entitlements to specific functionality, but such an approach makes it difficult to employ enterprise-wide access control policy management and enforcement. A properly deployed dynamic authorization service takes access control to the next level. It enables enterprises with sensitive data to more finely control access to protected resources, across a variety of use cases.

One reason for pursuing a dynamic authorization environment is the ability to establish consistent access control policy across an organization. Many companies use role-based entitlements often enabled via Microsoft Active Directory (AD) groups, which means a user's access rights are based on AD group memberships that are typically managed locally. This arrangement makes it difficult to impose consistency to access control decisions across an enterprise.

With a dynamic authorization model, access control decisions are managed via centrally administered policies that are applied across multiple applications and protected resources. This facilitates policy changes, which result in access control decision changes, to be implemented across all applications that use the authorization service, as opposed to static environments in which a policy change results in a re-assignment of user entitlements in an identity data store for future use in access control decisions. Furthermore, in a dynamic authorization environment, policies are evaluated in real-time against current attributes. As soon as an attribute changes, policy decisions based on that attribute will change, rather than having to wait for a nightly update of identity attributes before access control policy is correctly applied.

A dynamic authorization environment also facilitates the application of risk management to access control decisions. For instance, if access to an application outside business hours represents a greater risk, access policy can require elevation of a user's authentication assurance level when they attempt to access the application in the evening. In this instance the authorization service can prompt for an additional authentication factor before a permit decision is rendered.

There are several desired characteristics of a dynamic authorization solution:

- Access control decision are externalized. It is no longer necessary for access control logic to be coded into each application. Instead, when a user access request is received, a redirect to an external authorization service will be generated and the application will be sent a "permit" or "deny" depending on the evaluation of a user's request against the policies that have been established.

- It is attribute based. Rather than relying on the more widespread role-based access control a dynamic authorization service will evaluate a user's attributes, but also resource attributes, in real time, for example: ensuring a user still on the board of directors if they are accessing board meeting minutes. Sometimes context variables will also be evaluated, i.e. ensuring access only during business hours.
- Access control decisions are policy-based. Access control decisions in a dynamic authorization environment are determined via a set of policies, bringing consistency to access control decisions. With a central policy store the same policy can be used for multiple protected resources, so that granting access will no longer be dependent upon individual settings in isolated applications or databases.

Dynamic Authorization gives an enterprise the fine-grained control they need over access to protected resources. All organizations should consider deploying DAM as part of their data-loss protection strategy.

2 Market Segment

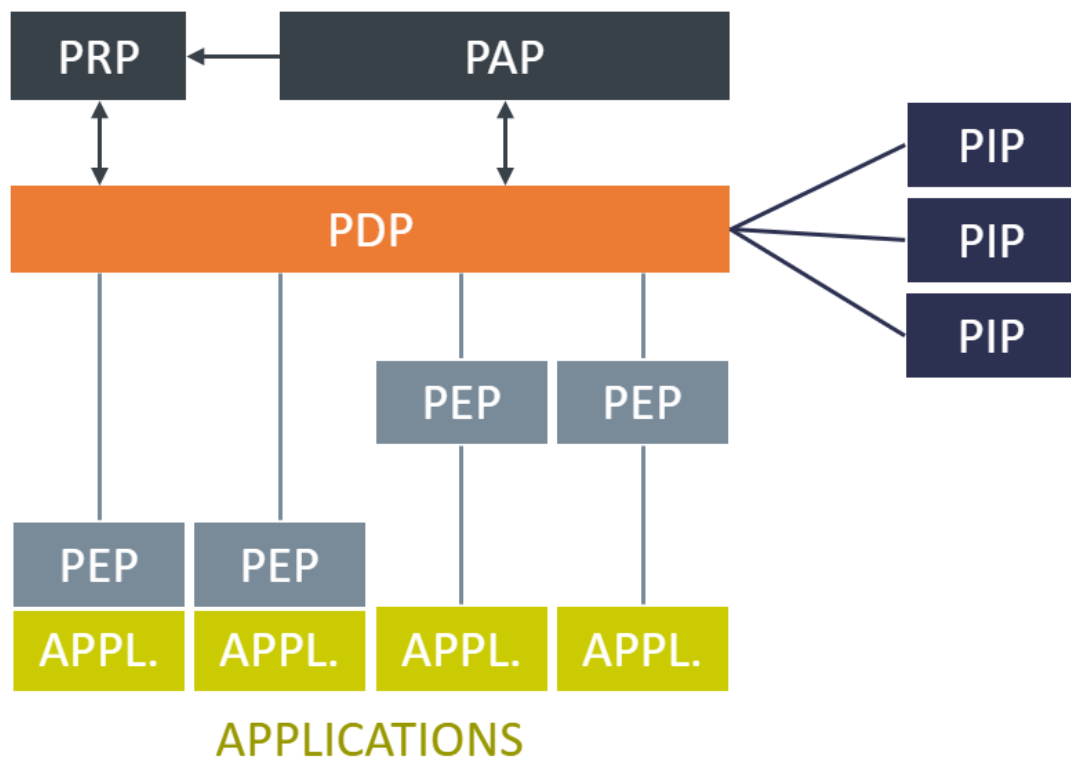
This Market Compass covers the dynamic authorization market segment. This is a special area of interest to organizations with sophisticated access control requirements. The specific segment of the authorization sector covered by this Market Compass includes solutions that allow the DAM software/appliance to control access to protected resources based on an externally managed policy.

2.1 Market Description

There are several drivers for the deployment of dynamic authorization technology:

- The desire for common policy deployment across an enterprise increases demand for DAM solutions. By externalizing access control decisions to a purpose-built infrastructure, common practices can be instigated that ensure access control policy is applied consistently across all business units.
- The need to accommodate diverse access control requirements within an organization is another trigger for increased DAM usage. In some cases a common entitlement might apply to all or most staff, but for some applications or databases strict control mechanisms might be required with fine-grained authorization policy.
- Organizations have an increasing requirement for real-time access control decisions. While this can be achieved with more conventional roles-based authentication environments, dynamic authorization infrastructure typically evaluates access requests against real-time data from connected systems.

A dynamic authorization environment is comprised of several components. Different vendors will achieve a solution in different ways but a generic depiction showing the components of a dynamic authorization service is shown in Figure 1.



PAP – Policy Administration Point
 PRP – Policy Repository Point
 PIP – Policy Information Point
 PDP – Policy Decision Point
 PEP – Policy Enforcement Point

Figure 1: Dynamic Authorization Management Service

- **Policy decision points (PDP)**

The product must be policy driven. This gives the product the capability of supporting a central policy store that an organization can use to support all their core applications and resources from a single point. Some vendors may use their own proprietary decision point software that supports their own technologies. Ideally vendors will support standards to allow their solution to interoperate with other

standards-based solutions.

- **Policy administration points (PAP)**

A mechanism is required to enter policies into the decision point. This is typically via an interface that lets users build expressions that implement a particular policy, e.g. to access the general ledger you must be a manager in the Finance Department. Approaches to policy administration are varied with some preferring a programming interface, and some using a drag-and-drop GUI to generate a natural language policy expression.

- **Policy Repository/Retrieval Point (PRP)**

In many cases the policy retrieval point will be co-incident with the PDP. In some cases there will be a requirement for multiple locations for policies storage. In a distributed environment there might also be multiple policy administration points. In an organization with multiple PRPs a mechanism to replicate policies is required.

- **Policy enforcement points (PEP)**

Each application, or control point, that uses the DAM tool must have a way to communicate with the decision point. A request-response mechanism is needed to allow for the return of a “permit”, “deny”, or “indeterminant” decision. A standard such as XACML can be used if a range of enforcement points is to be supported.

- **Policy Information Points (PIP)**

Data required to evaluate access control requests resides in one or more information points within an organization. Identity attributes are typically stored in a directory service and context variables are exposed by various services within the enterprise. Some solutions synchronize identity data to a dedicated PIP, others read and evaluate identity attributes in real-time.

In this Market Compass features that assist in the deployment of an externalized authentication service are more highly regarded. For instance, the ability of a product to handle specific variants of the standards was considered a benefit and the provision of tools to assist developers to deploy enforcement point software is considered beneficial.

2.2 Market Direction

Digital identity management and controlled access are becoming increasingly important within organizations. The reliance on identity data is beyond access control, which was historically the main reason for deploying an identity management solution. It is now necessary to be able to support corporate applications with identity data to allow organizations to provide sophisticated services to staff, business partners and customers. Fine-grained access to identity attributes provides the ability for applications to

optimize their user experience. The requirement now is for an 'Identity Fabric' that provides organizations with the ability to leverage major trends in the marketplace:

- Migration to cloud services which adds a level of complexity to the deployment of an externalized authorization service. Support is now required for on-premise applications, SaaS apps and multiple cloud environments. This means that PEP support for distributed applications is essential. 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 may require PDPs to be deployed on scalable cloud infrastructure. A vendor's micro-services approach that can fulfill the needs of managing access in microservice environments must therefore be considered.
- Multi-factor authentication is now ubiquitous. Smartphones are now ubiquitous and rapidly becoming the enabling factor for multi-factor authentication. Adaptive Authentication is the new normal, and context factors influence decisions about whether the required assurance level of a user login event has been met.
- Network monitoring improvements have significantly reduced cybersecurity vulnerability but network analyzers need real-time access to identity attributes in order to determine access rights to subnets and protected resources.
- User behavioral analytics also requires identity data support and access to end-point device identifiers for corporate staff and business partners.
- AI is another trend that requires support from the Identity Fabric. Access to a user's role within an organization, the department they're working in, their normal entitlements, any temporary entitlements, and date range for their validity, are common identity attributes that an AI engine typically requires.

DAM solutions from vendors are continually evolving and developing their products to accommodate these market trends. The IAM industry sector is expected to be increasingly flexible in its support for new technology and leveraging the opportunities it provides.

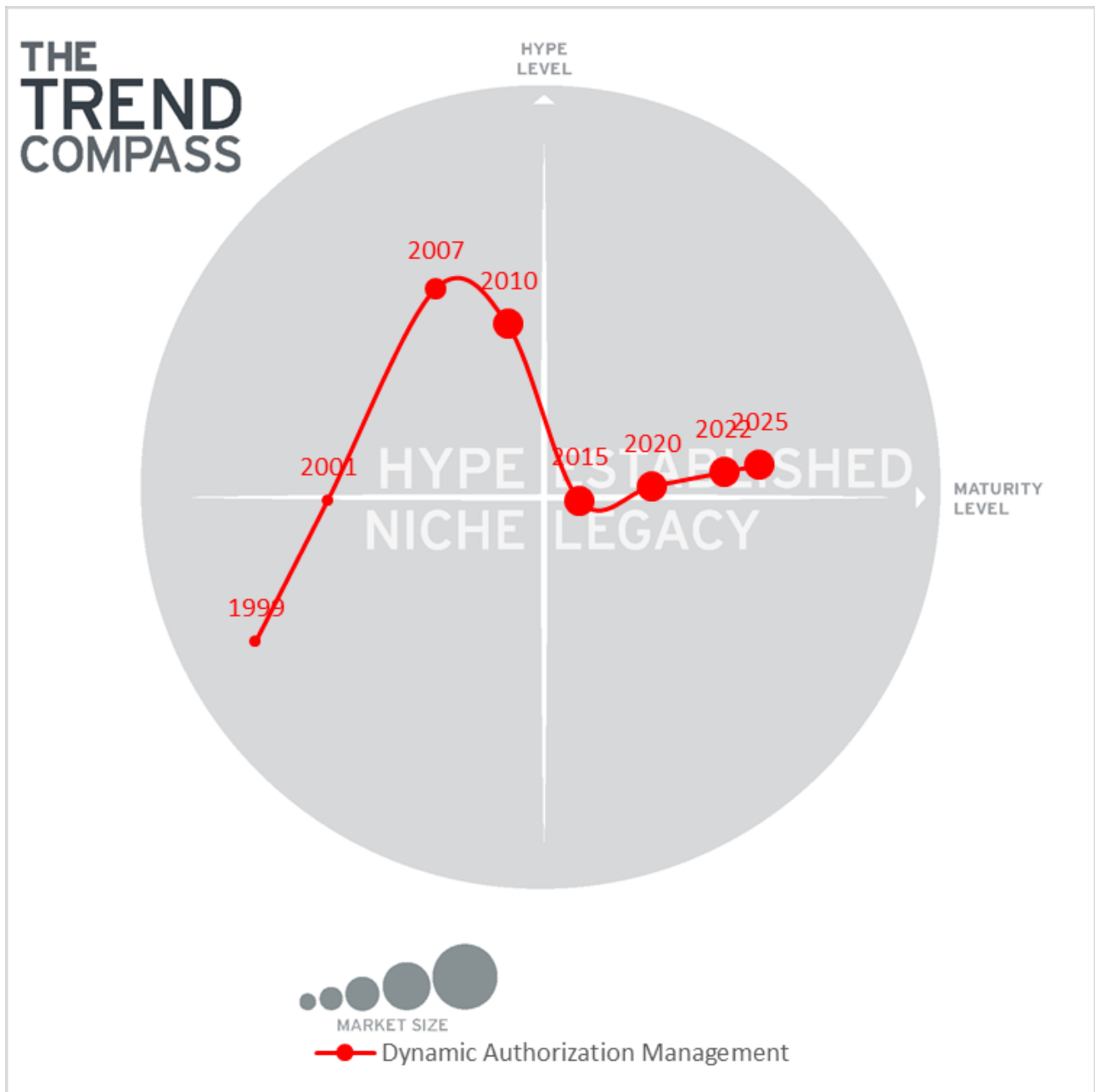


Figure 2: Dynamic Authorization Management

Figure 2 illustrates our view of how the market will evolve over the near term. The hype associated with dynamic authorization management is clearly over with trusted solutions and many mature deployments that demonstrate the improved efficiency and better security associated with an access control environment that centralizes policy administration and streamlines authorization processes. The market is constrained however, with DAM installations considered only by larger enterprises with the vision to appreciate its benefits and the resources to deploy such solutions. We can expect a steady growth in the DAM sector which is firmly in the “established” quadrant. It remains to be seen if new evolutions, particularly in cloud deployments, will drive adoption towards an increase in the size of the market segment.

2.3 Capabilities

The basic functionality that should be provided by all products/services in the sector includes:

Capability	Description	Relevance
Policy Administration	The solution must provide a mechanism for the creation and management of policies. While it is recognized that some organizations will employ an IT function for policy administration, it is considered advantageous if a natural-language or GUI facility is provided to enable business people to manage policies. Support for a distributed approach to policy management was viewed favorably, recognizing that multiple business units are typically involved in mandating access control policy.	Essential
PEP/PDP Architecture	The environment within which an external decision service is to be deployed will determine the preferred topology. In a wholly on-premise environment a single service, typically a VM, will suffice. In hybrid or cloud environments the deployment is more complex.	Essential
Standards Support	While it is recognized that efficient operation can often be achieved within a proprietary framework, standards-adherence is viewed favorably. While XACML is the most widespread authorization protocol, readers should be aware that XACML deployments will differ somewhat and plug-and-play cannot be assumed.	Essential
Target System Support	By definition, target systems can be diverse. In a largely web-application environment, target system support is relatively simple; if client-server or mainframe applications must be supported the authentication task becomes more complex. The ability to integrate application enforcement points into a variety of environments is considered important.	Essential
Governance	The support for enterprise audit events is considered important. Tools to facilitate the testing of policies and to ensure compliance to both internal and regulatory requirements was viewed favorably.	Desirable

Capability	Description	Relevance
Security	Provision of cybersecurity features to protect against unauthorized and malicious activity is advantageous. This includes control on access to management consoles, protection of data in transit and encryption of data repositories.	Desirable
Ease of Deployment	Support for connectors to other enterprise systems and diverse IT environments is necessary. The ability to support on-premise and hybrid deployments, including various cloud-based infrastructure, is a requirement.	Essential
Interoperability	The ability of the solution to work with other vendors' products is considered advantageous. This factor evaluates the extent to which a solution supports industry standards or provides extensive API support.	Desirable
Usability	This factor gauges support for the user experience for administrators using the management console, or users when accessing product features. User interfaces should be intuitive and consistent.	Desirable

3 Vendors and Products

The vendors in this market covered by this report are those that provide an offering that allows customers to externalize their authorization service. In other words, rather than relying on an internal, application-based facility for access control to protected resources, applications perform a “call out” to an external service to determine if a user is to be granted access to the requested service or document. Such a service should ideally support a standard protocol/architecture such as defined by XACML or a framework such as NGAC.

3.1 Vendors Covered

The vendors selected for this Market Compass are as follows:

- Atos – is a global leader in digital transformation services, headquartered in France. DAM is supported via the DirX portfolio, more particularly with the DirX Access product..
- Axiomatics – is a pioneer in attribute-based access control. The company is headquartered in Stockholm, Sweden and has a major presence in North America.
- EmpowerID – based in Ohio, USA. EmpowerID is a provider of a complete IAM solution that provides policy-based authorization based on a NGAC architecture.
- Jericho Systems – based in Texas, USA. Jericho Systems is a pioneer in the standards-based authorization services market and a long-time supplier to the defense sector.
- NextLabs – a pioneer in the provision of standards-based authorization services for the aerospace/defense sector solutions. NextLabs is headquartered in California, USA.
- PlainID – is based in Israel and provides real-time, fine-grained, policy-based access control through the evaluation of identity and environmental attributes.
- Symphonic Software – is a UK-based company providing an advanced technology platform for the deployment of policy-based access control systems.
- WSO2 – is headquartered in Mountain View, CA and is a leading supplier of API gateway software on a global basis. They support both static and dynamic access control.

3.2 Featured Vendors

Selecting a product for deployment can be a challenging task since there will typically be several solutions that fit an organization's requirements. This section seeks to highlight those vendors who offer specific functionality or industry expertise that might aid in the prioritization of shortlisted solutions.

3.2.1 Featured for Capabilities: Axiomatics

The Dynamic Authorization Suite offers an extensive solution: the PDP functionality supports a variety of deployment environments, multiple PEP code snippets support various application integration requirements and the ALFA language for policy development facilitates PAP management. In addition, policy analysis and maintenance will benefit from Axiomatics reverse query facility.

A strength of Axiomatics is that they also offer support for intercepting and controlling database access and access to big data environments. Due to their length of time in the market, they provide a broad set of integrations with other solutions.



Figure 3: Featured for Capabilities

3.2.2 Featured for Innovation: PlainID

PlainID has focused on the provision of an easy-to-use yet functional authorization service. Its strength is in

the policy administration that makes the management of access control policies a business function rather than a technical function. The package also supports a variety of deployment options that will suit organizations operating in a distributed environment.

With their approach, they are helping to simplify deployments and use of DAM solutions and helping to get these solutions out of the technical layer, and moving them closer to the business.



Figure 4: Featured for Innovation

3.2.3 Featured for Usability: NextLabs

The NextLabs Dynamic Authorization Platform takes a unique 4GL approach to policy administration and provides strong analytics to support compliance requirements. Out-of-the-box integration with the main cloud environments, and connectors to SAP and the major enterprise applications, facilitates deployment of the solution. A history in regulated industries such as Aerospace & Defense or Life Sciences ensures that the solution has the necessary certifications and regulatory compliance required for high assurance environments. Development of the CloudAz managed service is a major focus for NextLabs.



Figure 5: Featured for Usability

3.2.4 Featured for Usability: Symphonic Software

Symphonic is focused on ease-of-use by business users. It incorporates a powerful abstraction layer which facilitates the use of business terms within the policy manager. Innovative attribute modelling and data orchestration capabilities allow identity attributes and contextual information needed authorization decisions, to be gathered from disparate sources both internal and external to the organization. Symphonic's decision engine design uses highly configurable caching and stateless architecture to deliver scalability.



Figure 6: Featured for Usability

3.3 Vendors to watch

In addition to the vendors covered in detail in this report, we observe the following vendors that are not considered providers of a complete DAM solution. However, they are notable because they do offer functionality to enable development of a policy-based authorization service and should be considered by companies when selecting a dynamic authorization solution.

- **AWS** – As a cloud vendor AWS has a rich identity management capability and has an ABAC approach built into the capabilities provided in the platform. AWS users should familiarize themselves with this functionality. The ability to tag user accounts provides a useful feature for attribute-based access control policy evaluation.
Why worth watching? AWS is a pure-play cloud service provider with no legacy identity management capability. Of late significant development has been focused on identity and access management and it is likely that access control functionality will be extended.
- **Auth0** – While not included as a full solution vendor, Auth0 have powerful tools and services to enable deployment of a comprehensive policy-based approach to access control based on identity attributes; the Rules feature facilitates the establishment of a centrally managed policy environment.
Why worth watching? Auth0 is a trusted supplier of access control tools with many organization's building Auth0 services into their access control infrastructure. The current offerings could be extended with the development of policy-based services.

4 Ratings at a glance

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in table 1.

Product	Security	Interoperability	Usability	Deployment	Policy Admin	Architecture	Standards	Target Systems	Governance
Atos DirX Access	●	●	●	●	●	●	●	●	●
Axiomatics Dynamic Authorization Suite	●	●	●	●	●	●	●	●	●
EmpowerID IAM Suite	●	●	●	●	●	●	●	●	●
Jericho Systems EnterSpace	●	●	●	●	●	●	●	●	●
NextLabs Control Center	●	●	●	●	●	●	●	●	●
PlainID Policy-based Access Control	●	●	●	●	●	●	●	●	●
Symphonic Software	●	●	●	●	●	●	●	●	●
WSO2 API Gateway	●	●	●	●	●	●	●	●	●
Legend	● critical ● weak ● neutral ● positive ● strong positive								

5 Product/Service Details

Spider graphs

In addition to the ratings for our standard categories we add a spider chart for every vendor for quick assimilation of product strengths. For this Market Compass, we look at the following areas:

- **Policy Admin**
The level of support for centralized policy creation and management ideally by line-of-business personnel
- **PDP/PEP Architecture**
The breadth of support for various application environments and PDP deployment options
- **Standards adoption**
Support of standards such as the XACML protocol or NGAC architecture
- **Target systems support**
Degree to which various application (HTTP, Client-server etc.) environments are supported; includes database access control
- **Governance**
Provision of tools for audit, monitoring and reporting functions, including support for enterprise governance solutions
- **Security**
The level of cybersecurity features to protect the authorization service from malicious events
- **Ease of Deployment**
The variety of deployment options supported and the provision of integration tools such as connectors and APIs
- **Usability**
How well the solution provides a good user experience for users and administrators.

The spider graphs provide comparative information by showing the areas where the products are stronger or weaker. Some products may have gaps in some areas, while being strong in others. These might be a good fit if only certain features are required. For solutions that deliver strong capabilities across all areas might be required for strategic enterprise-wide requirements.

5.1 Atos

Atos is a well-established global IT services supplier headquartered in France with operations in 73 countries worldwide. In recent times Atos Origin was formed with the merger of several IT companies. In 2011 the company became Atos with the merger with Siemens IT Solutions & Services. The Siemens DirX product suite was expanded under the Evidian DirX brand name and comprises an extensive identity and access management suite with strong access control capabilities, including federated authorization.

DirX Access is a complete access management server with federated authentication and authorization services. DirX supports SAML-based federation with out-of-the-box support for the mainstream service providers and OpenID connect identity layer on top of OAuth2.0 is supported. A central administration tool supports the creation and management of access control policies. The GUI allows administrators to set-up resource access rules that sets the permissible actions and any conditions associated with the entitlement. DirX Access supports the XACML 1.x/2.0/3.0 protocol for attribute-based access control, role-based access control and discretionary access control. PEP SDKs are provided for Windows, Redhat Linux and SUSE Linux environments for Web services and Java clients. PEP messaging can be protected via PKI technology. DirX tracks user access by session and can be configured to record login failures, IP address, location etc. This means that anomalies in user behavior can be identified with step-up authentication invoked if necessary. Governance within the product provides logging and monitoring features, full integration with DirX Audit supports Java Logging (Log4J2) for default solutions, and provides auditing extension points for custom solutions. SQL Database governance guidelines are supported.

A variety of integration options are supported. DirX provides comprehensive PEP support with protocol PEPs, agent PEPs or application-embedded PEPs to suit most current and legacy application technology. Both push (DirX initiated) and pull (relying party initiated) are supported. All communication endpoints can be configured with PKI technology. The DirX Access cluster approach accommodates ease-of-deployment features and customization capability. The DirX suite is well integrated into the Windows environment with good support for O365.

Security	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○
Policy Admin	● ● ● ● ○
Architecture	● ● ● ● ○
Standards	● ● ● ● ●
Target Systems	● ● ● ● ○
Governance	● ● ● ● ○

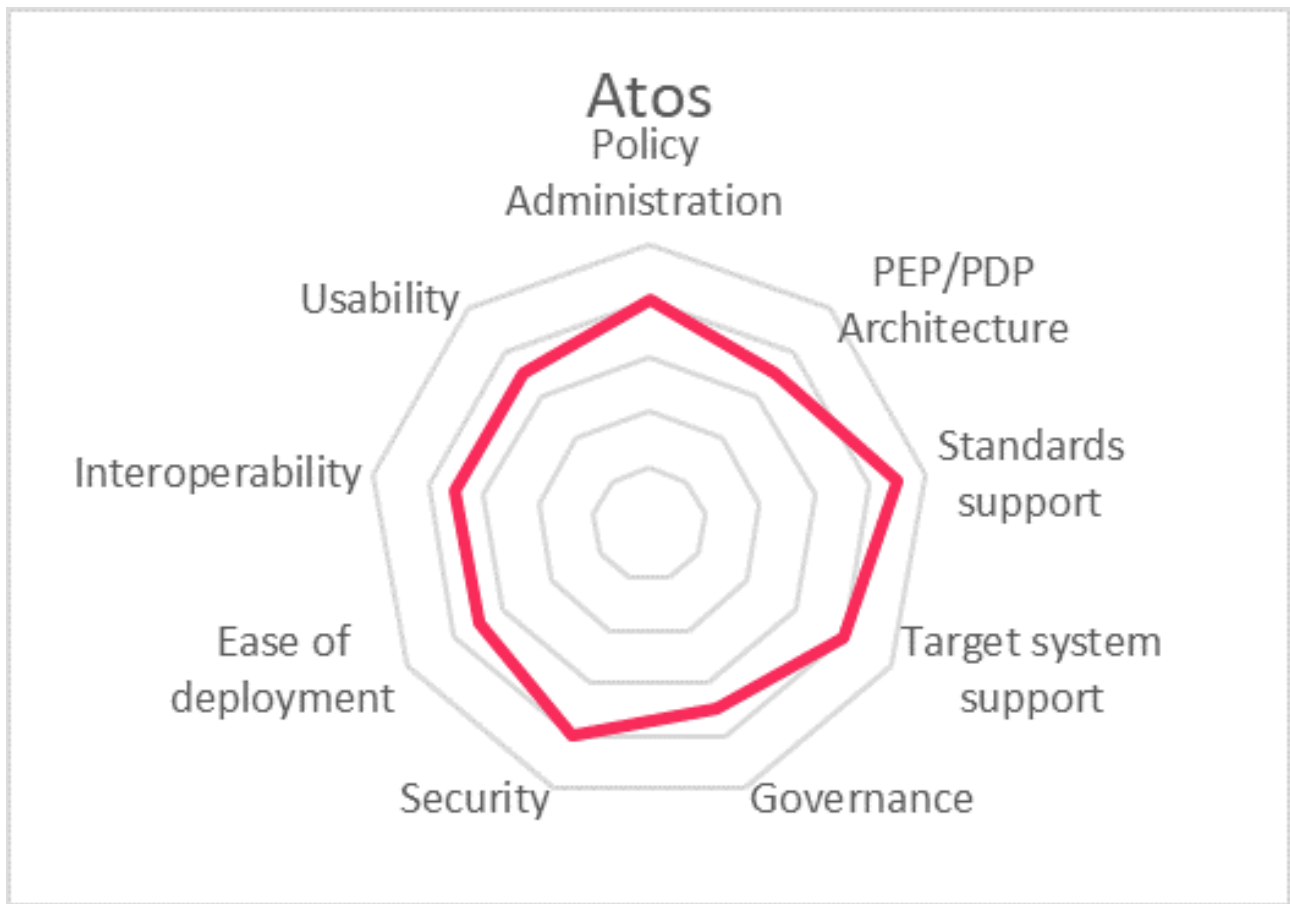


Strengths

- Mature supplier of identity and access management solutions
- Comprehensive auth'n & auth'z features and standards support
- Full monitoring (Nagios) and audit log features
- Good support for risk and context-based authentication

Challenges

- Deciding how much of the DirX Suite to deploy to get the required functionality could be difficult.
- DirX is well-suited to on-premise deployment, but cloud deployment might be more problematic
- Matching the agility of some point solution providers offering advanced features could be a challenge



5.2 Axiomatics

Axiomatics has pioneered the development of attribute-based access control. The company is headquartered in Stockholm, Sweden but has a major presence in North America. The Authorization Suite is used by many Fortune 2000 companies and by government agencies in Europe and the US.

The Policy Server maintains an organization's access policies. There are multiple ways in which a policy can be established: the policy editor provides a GUI approach to allow the user to construct policy statements or the Abbreviated Language for Authorization (ALFA) can be used. The PDP component can be deployed as a core service or integrated into an application for higher performance. Axiomatics supports a cloud-native approach to PDP deployment. It can be containerized for deployment in environments such as Docker, and the stateless nature of the PDP lends itself to a micro-services approach using orchestration tools such as Kubernetes. Axiomatics supports the Open Policy Agent framework that provides a unified toolset across a cloud-native stack. A multi-layered approach to policy administration provides support at the developer level, governance level and via an overarching orchestration facility. As for PEPs there are a variety of options: code is provided for the main development environments and third party XACML solutions are supported. The Services Manager provides monitoring of the system's operation.

The Axiomatics Reverse Query functionality provides the capability to search a multi-dimensional policy dataset and display results based on a user's entitlements. This extends to a sophisticated functionality for controlled access to relational databases. Filtering on data elements based on a user's attributes, and masking data for information redaction, are supported.

Axiomatics has a long history in the dynamic authorization market segment being one of the pioneers of policy-based ABAC solutions. Their expertise provides clients confidence in the ability of the Authorization Suite to meet their requirements.

Security	●	●	●	●	●
Interoperability	●	●	●	●	○
Usability	●	●	●	●	●
Deployment	●	●	●	●	○
Policy Admin	●	●	●	●	●
Architecture	●	●	●	●	●
Standards	●	●	●	●	●
Target Systems	●	●	●	●	○
Governance	●	●	●	●	●



Strengths

- Experienced supplier of central policy-based authorization control solution
- Standards support with participation in XACML and JSON development
- Flexible support for cloud migration
- Reverse query functionality to build user entitlements lists
- Policy-based, dynamic filtering for relational databases

Challenges

- Policy administration is a technical rather than business function e.g. no natural language functionality
- Partner support outside North America and Europe might be limiting
- Integration of new IdPs data storage technology may require API development



5.3 EmpowerID

Based in Ohio (USA), EmpowerID offers a complete IAM solution for user provisioning with password management, group management with role optimization, privileged access management, and identity governance. While they don't offer a stand-alone authorization server, the EmpowerID solution does provide policy-based access control features that will satisfy the requirements of most organizations.

The EmpowerID identity management solution is comprehensive. Solutions are provided for privileged account management and access control to web and mobile applications with support for SAML, OAuth, Open ID Connect, WS-FED and JWT technology. A point-and-click UI is provided for policy assignment but programming ABAC rules is in C# and typically managed via Workflow Studio. While rules can be read by policy administrators, development staff are required to maintain the policy service. EmpowerID does not provide XACML support but they do provide "NGAC hybrid" support. This means that it is possible to create sophisticated access control environments that grant or deny access based on rich relationship-based decisions.

EmpowerID is Microsoft focused with .NET support for PEPs provided. An access control solution for SharePoint is also offered.

Security	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ○
Policy Admin	● ● ● ○ ○
Architecture	● ● ● ○ ○
Standards	● ● ● ○ ○
Target Systems	● ● ● ○ ○
Governance	● ● ● ○ ○

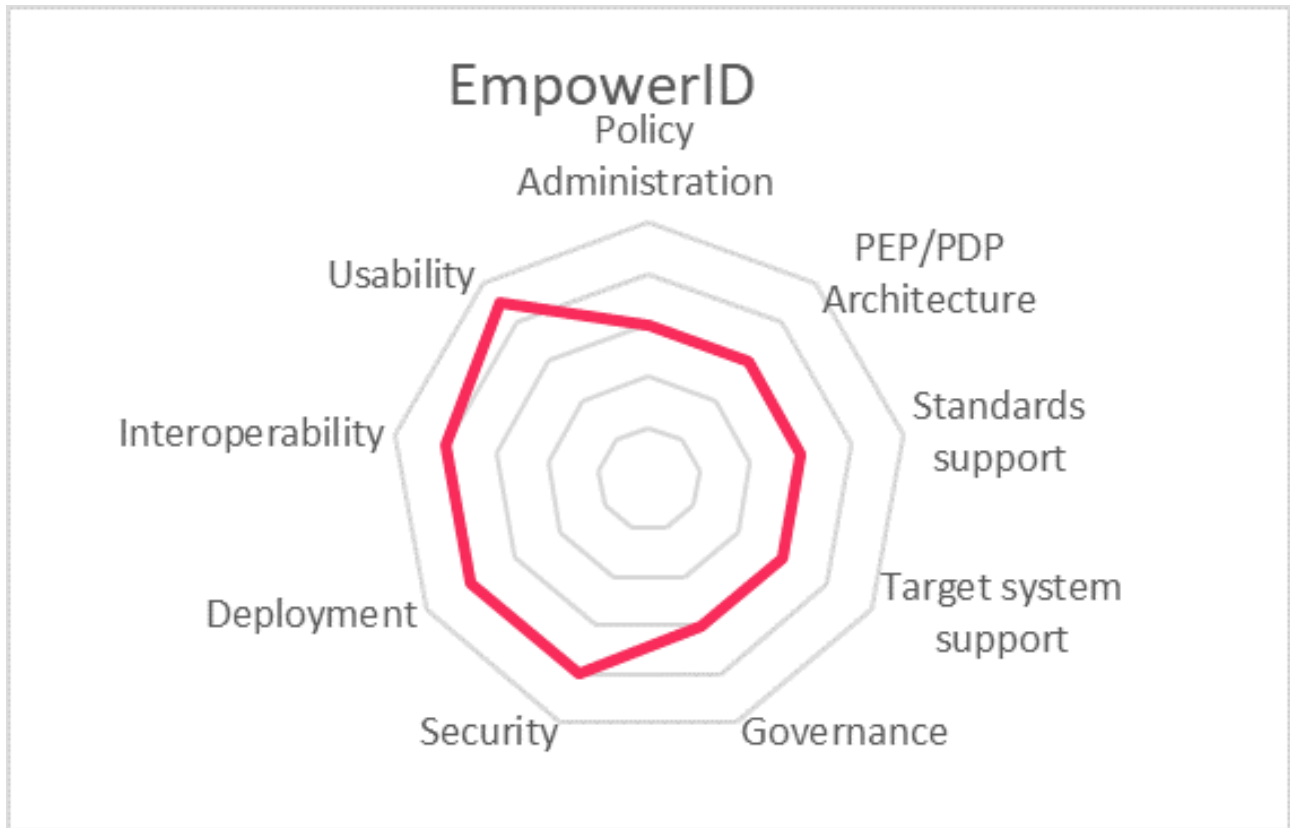


Strengths

- Complete identity management solution
- Support for hybrid authorization including dynamic authorization management
- Easy policy configuration and workflow management
- Strong access management capabilities for Windows-based technology

Challenges

- Current Microsoft focus may limit suitability in other environments
- Lack of support for the XACML protocol could be a detractor in some situations
- Policy administration is a technical rather a business-person function



5.4 Jericho Systems

Jericho Systems is a long-term participant in the dynamic authorization sector. Established in 2002 Jericho Systems Corporation has built an enviable reputation in the Defense industry, servicing clients such as Lockheed Martin, NSA, DISA, and the US Military. Jericho has followed a robust development program and has been granted several patents for its technology. The Enterspace Rules Mark-up Language supports both the Security Suite and the Marketing Suite. Policy administration accommodates the management hierarchy required in modern businesses, providing policy inheritance and delegated administration. Jericho Systems have been “trail blazers” in the adoption of policy-based decision point technology and a long-term user of the XACML protocol; they are active on several industry boards establishing standards for interoperability.

Jericho has expanded into the healthcare sector providing fine-grained access control for hospitals and healthcare professionals. Jericho Systems approaches the dynamic authorization management task a little differently than other vendors. They support the use case in which a policy evaluation initiates an event (rather than the relying application). The Company provides support for a variety of PEP environments including SOAP (both Java and .NET), HTTP reverse proxy, Java Web servlets, REST services and SAML. Support for the Microsoft environment is provided, as well as out-of-the box support for SharePoint.

Governance is supported via logs maintained in a database or accessed by third-party tools. Portal users can access an audit widget to search audit data. The service can run on both Windows Server and Linux (CentOS recommended). Various licensing models are supported.

Security	●	●	●	●	●
Interoperability	●	●	●	○	○
Usability	●	●	●	●	●
Deployment	●	●	●	○	○
Policy Admin	●	●	●	●	●
Architecture	●	●	●	●	○
Standards	●	●	●	●	●
Target Systems	●	●	●	○	○
Governance	●	●	●	●	○

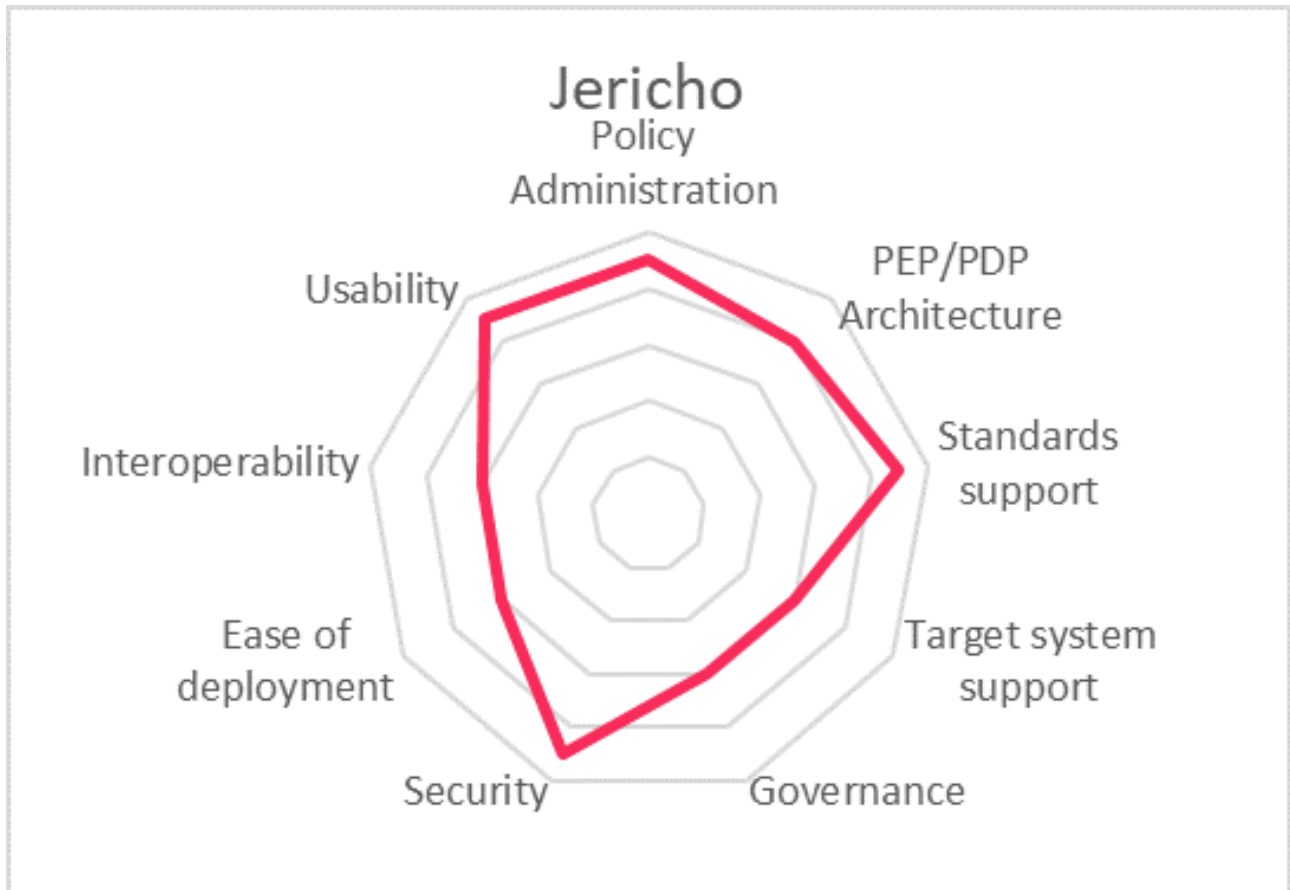


Strengths

- Mature provider of dynamic authorization solutions
- Both simple and advanced policy administration are supported
- Extensive standards support
- Patent protection on designs

Challenges

- Specialist knowledge required for policy development
- PDP deployment in cloud environments could be a challenge
- Wider support for MFA may be required



5.5 NextLabs

NextLabs is a long-term supplier of a dynamic authorization management solution with a highly functional product offering for externalized decision making with specific support for target industries. Solutions are provided as a suite of pre-integrated products. NextLabs has a strong partner focus maintaining relationships with SAP, Microsoft, Siemens, IBM, Oracle, AWS, Google, Salesforce, Workday and Okta.

NextLabs provides extensive integration facilities with out-of-the-box (OOTB) support for popular enterprise applications and cloud environments. SDKs are available for the main development environments. Policy Administration utilizes a versatile 4GL solution. The development environment enables administrators to create policies with a high-level programming language that automates policy creation independent of the underlying technology. Policies can be read as natural language statements that clearly indicate the subject, action, object, constraints and any obligations. The system incorporates strong policy framework analytics to identify anomalies.

The OOTB reporting facilities facilitate forensic analysis of user group entitlements and activity. The Activity Server can report on activity logged in the Audit Repository. Anomalies across applications can be identified and correlations, of access denials across applications can be alerted via the dashboard or via email. The major SIEM and SOC tools are supported. Compliance tools provide the capability for policy validation during the creation phase and can be used to perform 'what if' analysis to test policy results. Post deployment analysis can be performed to identify policies that might be returning a high rate of denials, possibly due to under-permissioning.

Deployment options are extensive. NextLabs follows a 'cloud first' strategy with a containerized approach to support a variety of deployments on the main public and private clouds and the product is certified on OpenShift. The CloudAz 'Authorization-as-a-Service' provides the NetLabs system functionality via a managed service.

Security	●	●	●	●	●
Interoperability	●	●	●	●	○
Usability	●	●	●	●	●
Deployment	●	●	●	●	●
Policy Admin	●	●	●	●	●
Architecture	●	●	●	●	●
Standards	●	●	●	●	●
Target Systems	●	●	●	●	○
Governance	●	●	●	●	○

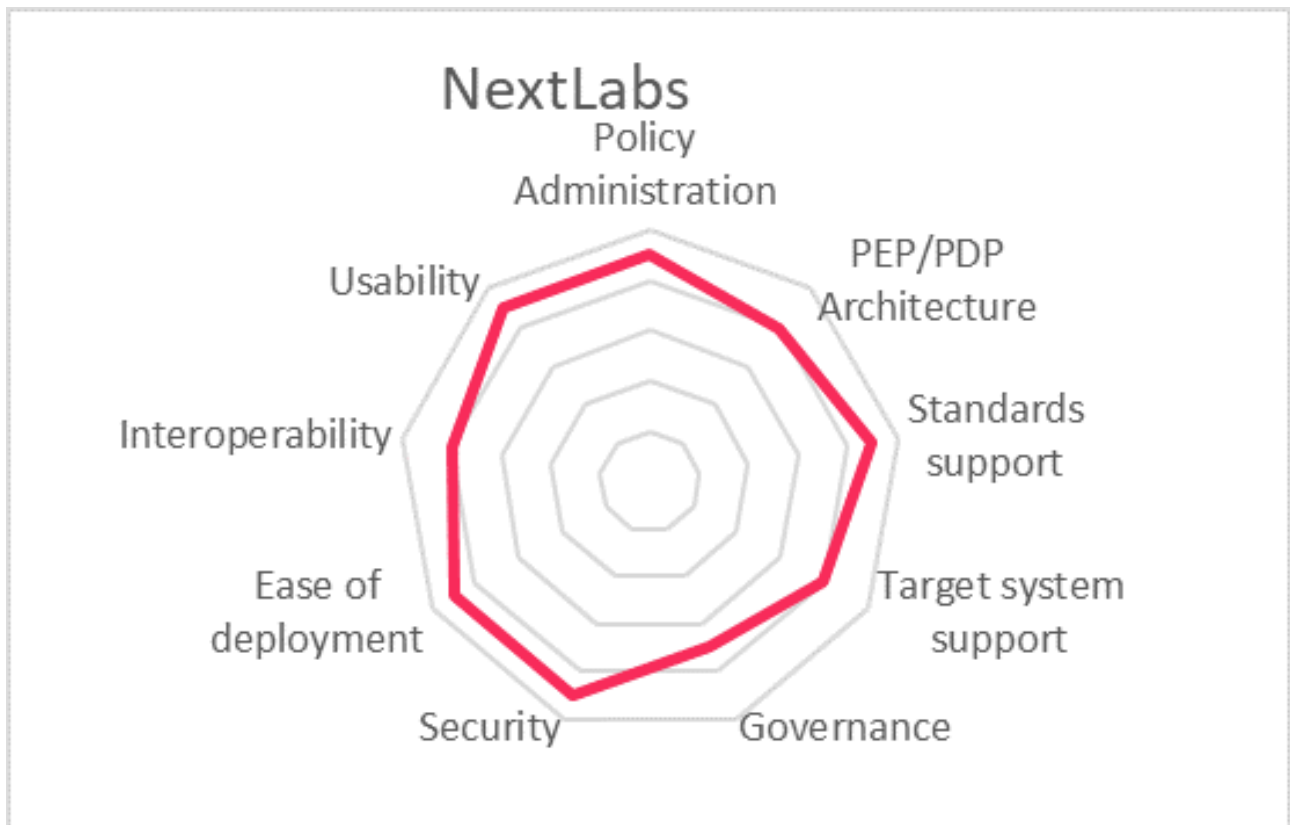
NEXTLABS®

Strengths

- Mature customer base in high-risk industry sectors
- Architected solution with easy-to-use policy editor
- Turn-key operation with delivery of custom solution for clients
- Strong security features for protection of data-in-transit and data-at-rest

Challenges

- Integrations into smartphone technology for authorization only by customization
- Focus on the enterprise market, might be cost-prohibitive for smaller organizations
- Deploying solutions outside NextLabs' traditional industry sectors might prove problematic



5.6 PlainID

PlainID was founded in 2014 and is headquartered in Israel. The company focuses on delivering fine-grained authorization functionality that scales for large enterprise applications. The PlainID Policy Based Access Control Solution takes a unique approach to attribute-based access control; the task is to manage policies not entitlements. This starts with defining management units (not workgroups or lines-of-business) and determining the governance hierarchy. At the bottom of the hierarchy are the application owners who ensure compliance to their application requirements. At the next level in the hierarchy a line-of-business might group policies for multiple applications, above this a compliance group might have oversight over several lines-of-business, and so on.

Policy creation is graphical with actors, actions and resources displayed in a GUI. Policy creation commences with the selection of actors to which the policy applies, constraints can then be placed i.e. business hours access only, the action can then be selected i.e. read only, and then the target is then selected i.e. medical records. At each point menus assist in the selection of actors, constraints, actions and resources. A policy can therefore be constructed in a few minutes. The PlainID solution has the ability to provide nuanced responses to relying applications, rather than a simple permit/deny. The system can respond with a user 'access token' in which a user's access rights can be passed, or an 'asset token' can be passed to a resource indicating which users have access rights. Analysis of entitlements can be performed via an interrogation of applicable policies to construct a complete view of a user's access rights. It's then possible to undertake permission analysis and determine the 'coverage' of a policy set. An acceptable correlation percentage is set and then PlainID will calculate the coverage that is attained with the current policies. This allows compliance personnel to understand how efficient their policy management is, and to undertake role optimization to improve efficiency.

SAP uses the PlainID authorization solution and both Okta and Ping are supported. Hybrid environments are supported with no additional cost for replicating multiple instances. The product is deployed in a UNIX (CentOS or Red Hat) environment.

Security	●	●	●	●	○
Interoperability	●	●	●	●	○
Usability	●	●	●	●	●
Deployment	●	●	●	●	●
Policy Admin	●	●	●	●	●
Architecture	●	●	●	●	○
Standards	●	●	●	●	○
Target Systems	●	●	●	●	○
Governance	●	●	●	●	●

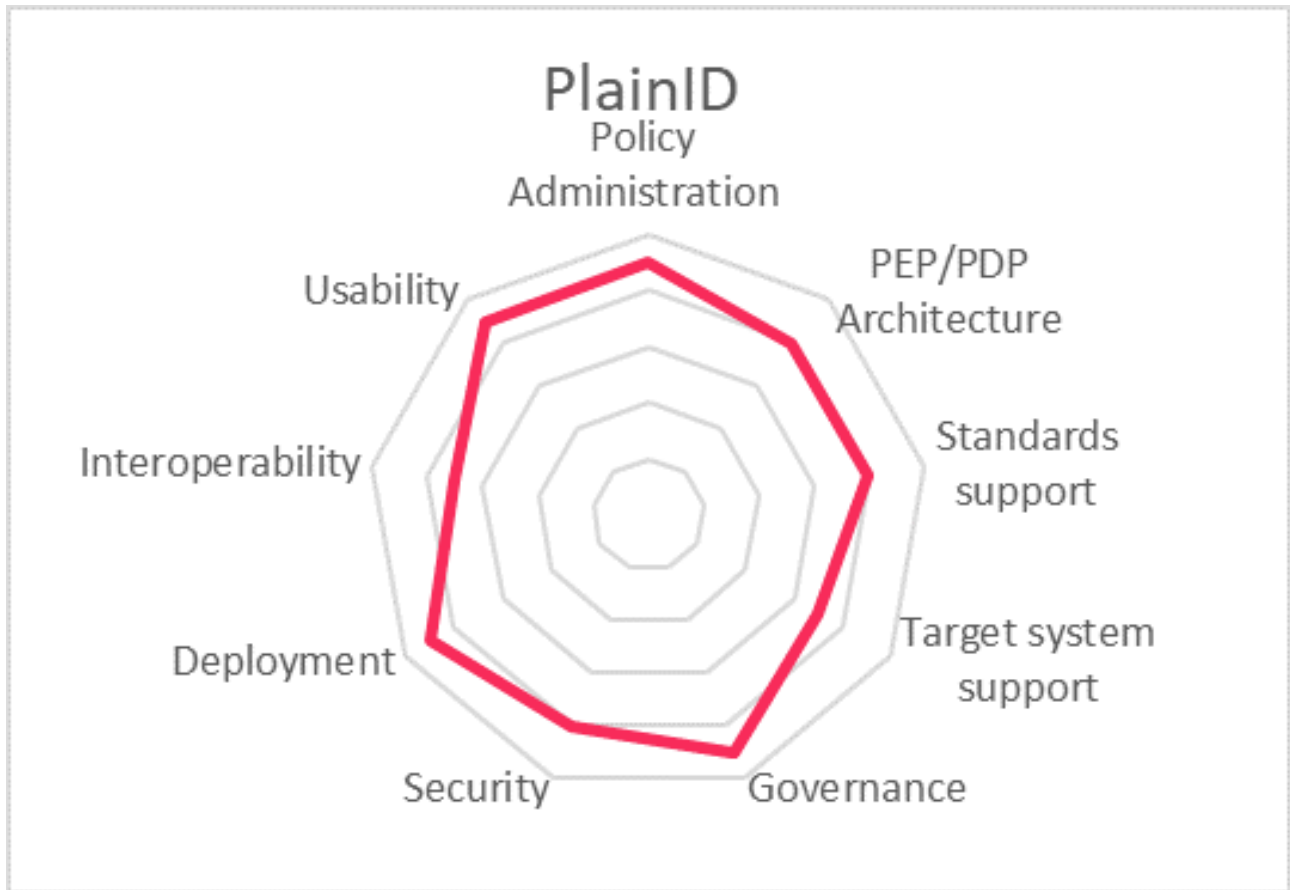


Strengths

- Administrative GUI for writing policy obviates the need for deep XACML expertise
- Policy modeling tools allows administrators to test effects of policies and changes
- Proprietary PDP technology for high performance, standards support for interoperability
- Strong support for policy control by business personnel

Challenges

- Ensuring sufficient SDK support for legacy applications
- Real-time integration of cloud-based repositories of identity attributes and context variables is lacking
- Deployment in some geographies might prove problematic



5.7 Symphonic

Symphonic Software is a UK-based company with a growing global customer-base. The company has many years' experience in the development of policy-based access control systems and the solution leverages their customer experience in order to provide clients with an advanced technology platform that provides a sophisticated real-time decisioning engine that uses context and policies to assure access to protected resources. The solution takes an API-first approach to interfacing corporate applications; a graphical UI supports the integration.

Customers can choose to use Symphonics' proprietary PEP protocol, leverage existing API gateway and Nextgen firewall extensions. If the relying application supports it, the XACML protocol can be deployed. Policy Administration is facilitated by a GUI that allows access control policy to be developed without the need for any programming by the operator. Drop-down menus and drag and drop building blocks are provided that facilitate policy definition by a business person, rather than an IT person. The policy management function facilitates incremental testing as policies are developed and the reusable-component library capability aids deployment. Governance is supported via extensive logging facilities which provide such features as log replays and the attribute secrecy feature preserves privacy. Symphonic supports complex decision point topologies. Multiple instances of PDPs can be deployed in order to minimize network latency, with each PDP running individual or common policy sets which are centrally managed and deployed from the PAP administration console. Sophisticated decision logic determines the policies to be used for a specific scenario.

Symphonic's business model is based on a client's company size rather than being server-based. This means that license fees are not levied per software package deployment, which allows a diverse variety of architectures to be supported without excessive software license costs.

Security	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ●
Policy Admin	● ● ● ● ○
Architecture	● ● ● ● ●
Standards	● ● ● ● ○
Target Systems	● ● ● ● ○
Governance	● ● ● ● ○

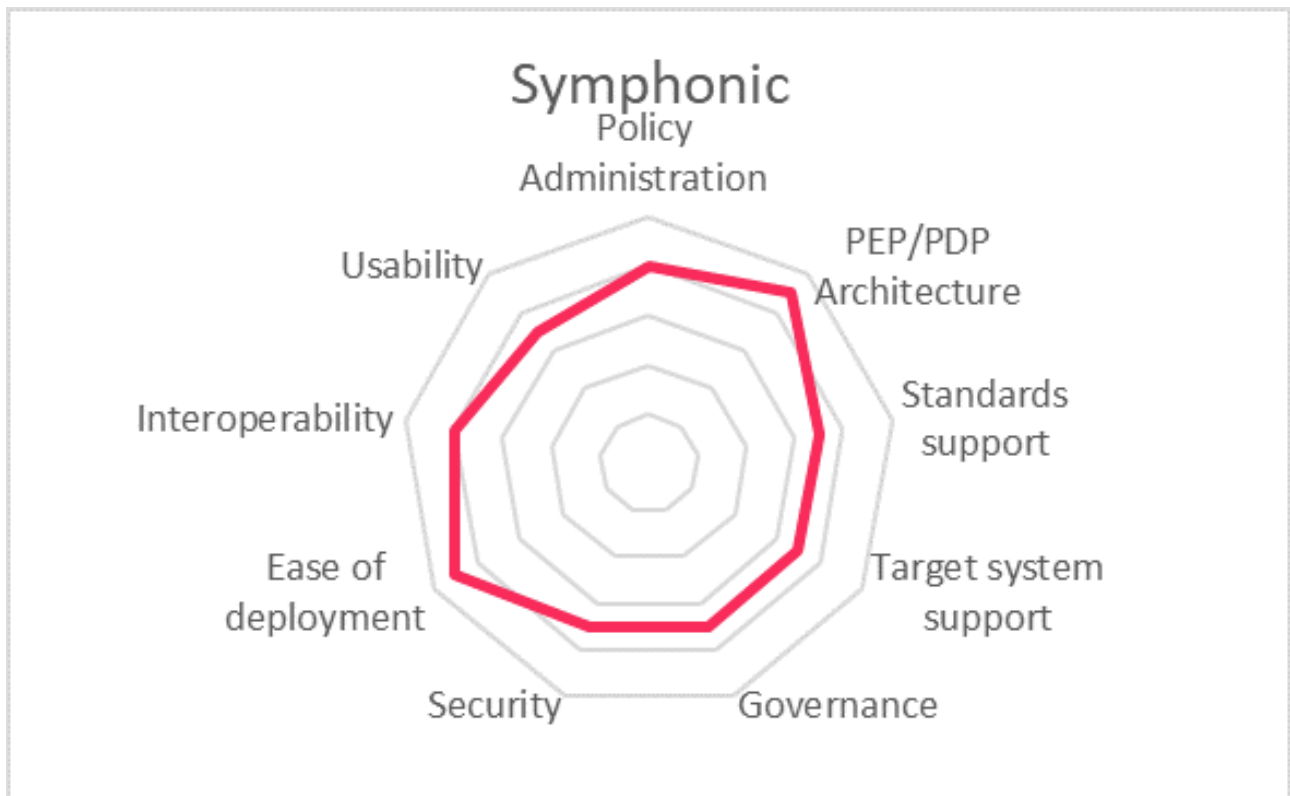


Strengths

- Business focused access control with a drag-n-drop policy administration UI
- Policy analysis tool to identify policy conflicts and redundant policies
- 200+ app connectors make it easier to externalize authorization
- Provision of a unified view of attributes and context variables

Challenges

- A disciplined approach to policy administration will be required to ensure consistency and avoid policy contention
- Custom development might be required for API support for legacy applications
- Partner availability in some geographies might be limited



5.8 WSO2

WSO2 is a specialist supplier of gateway technology headquartered in Mountain View, CA. The company has built a formidable global presence in the API gateway market sector and is a leading supplier of systems-integration technology. WSO2 customers are focused in North America and the EMEA regions, with a growing presence in the APAC region. They support organizations, from small to large, via their partner ecosystem. WSO2's target market is interconnected systems within an enterprise. While not a classic DAM vendor, authorization via the WSO2 gateway can be static, whereby message data is validated against a predefined set of rules or policies, or the gateway can ingest an access decision from an external authorization server. System functionality includes dynamic security checks such as access token validation and anomaly detection.

The Enterprise Integrator provides multiple integration options including REST, SOAP, JSON and XML services. The API Manager includes a complete development environment in which to design, develop and deploy APIs. The Developer Studio provides a programming environment for the development of policies, and the XACML engine supports PEPs in relying applications that adhere to the XACML protocol. WSO2 also provides an identity and access management platform, either using its own LDAP store of user data or it can access an enterprise LDAP directory or Active Directory to support access control within API interfaces. As expected from a provider of API technology there is strong support for standards. The API manager supports XACML for PDP communication to validate API requests and there's a strong focus on security with support for PKI and encryption of API calls. The Analytics and Stream Processing functionality provides monitoring and reporting capability for strong governance. API security is enhanced by AI technology that can recognize the unique vulnerabilities of each API and detect instances of abnormal usage and enable real-time response to attacks.

The WSO2 product is distributed as software modules with multiple deployment options, including Kubernetes support. Customers will generally have a DevOps capability to leverage the agility provided via the solution. An extensive partner network supports customers, assisting them to exploit the capability built into the product. The WSO2 product is delivered in two forms: open source, offered under Apache Software License V2.0, and the commercial version which is fully supported under an end-user license agreement

Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ○ ○
Deployment	● ● ● ● ●
Policy Admin	● ● ● ○ ○
Architecture	● ● ● ○ ○
Standards	● ● ● ● ○
Target Systems	● ● ● ● ○
Governance	● ● ● ● ○



Strengths

- Extensive experience in the provision of API gateways provides a mature product offering
- Integrated product solution with the API Manager Identity and Access Management
- Flexibility in product deployment across on-premise and cloud environments
- Strong governance capabilities if the Analytics and Stream Processing module is included

Challenges

- Programming expertise is required to exploit policy creation and maintenance functionality
- A DevOps capability or an integration partner will typically be required for solution deployment
- Co-operation between multiple groups will be required to optimize gateway and dynamic authorization capabilities



6 Related Research

[Executive View: Atos DirX Access - 80167](#)

[Executive View: Axiomatics APS - 80314](#)

[Executive View: EmpowerID - 70297](#)

[Executive View: NextLabs Data Centric Security in the Hybrid Cloud - 72531](#)

[Executive View: PlainID Policy Manager - 80315](#)

[Vendor Report: Jericho Systems – Attribute-Based Access Control - 71513](#)

[Executive View: Symphonic – Intelligent Authorization - 80154](#)

[Leadership Compass: API Management and Security - 70311](#)

[Leadership Compass: Identity API Platforms - 79012](#)

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
- Functionality
- Ease of Delivery
- Interoperability
- Usability

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.

Ease of Delivery 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.

We focus on security, functionality, ease of delivery, interoperability, and usability 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

Figure 1: Dynamic Authorization Management Service

Figure 2: Dynamic Authorization Management

Figure 3: Featured for Capabilities

Figure 4: Featured for Innovation

Figure 5: Featured for Usability

Figure 6: Featured for Usability

Copyright

© 2020 Kuppinger Analysts AG. All rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice.

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 back 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.