Symantec
A Division of Broadcom

Product Brief

Symantec Access Management

Key Benefits

- Accelerate app development by rapidly embedding security into mobile apps and IoT
- Improve user experience through frictionless authentication and single sign-on
- Secure communications and the entire user session from device to backend data stores
- Provide appropriate access to legitimate users based on dynamic and adaptive policies
- Optimize app performance by leveraging a platform with carrier-grade scalability and reliability
- Facilitate secure DevOps by externalizing data and services to developer communities

Key Features

- Multifactor credentials and risk analytics to positively identify legitimate users and devices
- Security standards seamlessly bridged to provide end-to-end security for mobile/Web/IoT solutions
- Single sign-on (SSO) and identity federation to provide convenient access to apps located anywhere
- Enhanced session assurance and granular access control policies to further protect access
- Enterprise directory service to deliver scalability and performance for the most demanding applications

Overview

The application economy has disrupted every industry. Every user interaction is being driven toward a connected app- or device-based interface that provides instant access to data and services. To thrive in this new reality, organizations must deliver a superior user experience with every touch—and things are only going to get worse. By 2025, the world will collectively create 175 trillion gigabytes of data1 and by 2023 there may be 3.5 billion connected IoT devices2. This explosion of data and an ever-expanding threat surface must be protected on a scale that is unprecedented.

Business Challenges

Because of the pressures to digitally transform and evolve, organizations are often rushing new applications to market without ensuring that adequate security controls have been implemented. The hybrid environment and reliance on APIs to connect users, devices, and applications to backend data only further complicate the approaches and technologies needed to secure the modern data center. Current security models are built around silos and point products, which depend on human scaling and static rules. These will soon be too slow, rigid, and error-prone to deal with tomorrow's digital infrastructure. These challenges must be addressed with a next-generation access management solution.

Solutions Overview

Symantec Access Management is designed to secure the modern enterprise through a unified platform that positively identifies legitimate users with multifactor authentication, provides seamless single sign-on (SSO) access to multiple apps, enforces granular access control policies, monitors the entire user session, and safeguards trust from mainframe to IoT.

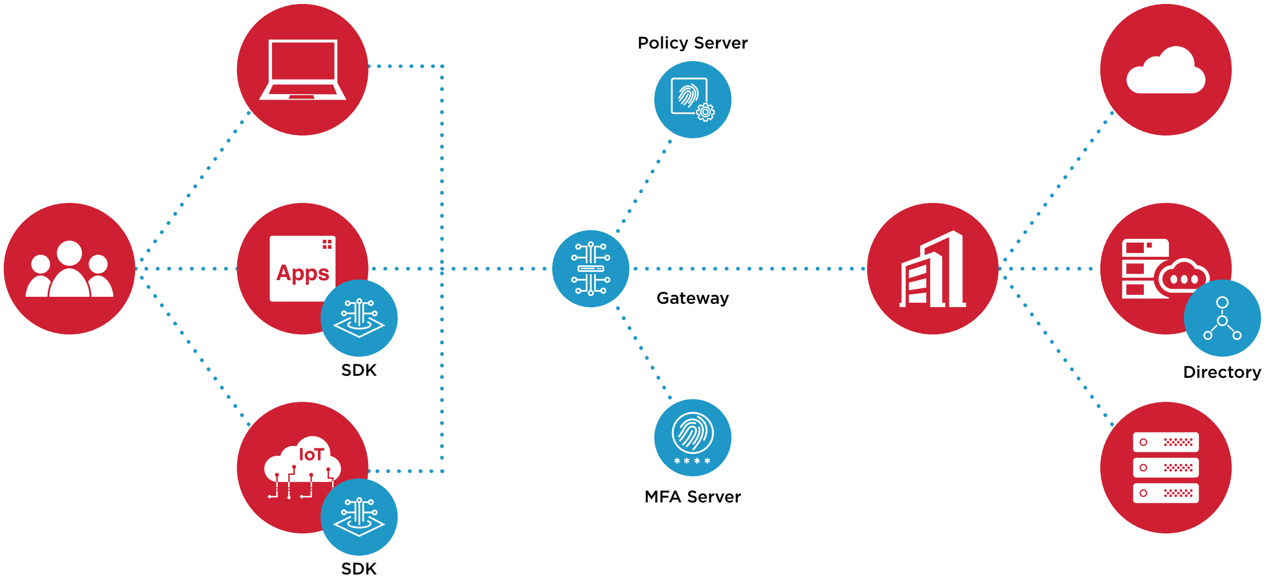
The solution uniquely identifies users, apps, and devices to establish a triangle of trust and patented enhanced session assurance that leverages risk analytics to prevent session hijacking. Finally, the Symantec Access Management solution is battle-tested and proven in the largest IT environments in the world.

Features and Capabilities

Symantec Access Management delivers a comprehensive solution to provide end-to-end security from users and devices to backend resources through the following core features and capabilities:

- **Universal SDK** enables developers to embed world-class security features, including strong authentication credentials, OAuth and OpenID Connect support, risk-based analysis, mutual SSL, secure data storage, and SSO into your mobile apps and IoT devices without having to be security engineers. This ensures that adequate security is built into the apps without impacting developer velocity.

Symantec Access Management Conceptual Architecture



- **Secure Communications** provide protection against OWASP Top 10 threats, protecting mission-critical APIs to facilitate secure, cross-domain information sharing while also protecting data at rest and in motion to make it extremely easy for developers to integrate backend services, legacy infrastructure, enterprise data, and third-party resources into scalable REST APIs.
- **Authentication** identifies legitimate users from fraudulent ones by supplying and supporting a comprehensive set of single and multifactor credentials across web, mobile, and IoT channels. The solution adaptively applies these mechanisms using a combination of dynamic real-time contextual data and policy-based rules to achieve the appropriate balance between security and user experience.
- **Authorization** explicitly grants or denies access to all protected applications and resources through security policies based on a user's profile attributes, group memberships, roles, and so on. You can also specify when a user can access specific resources (day/time restrictions), where the user can access a specific resource from (for example, only when logging in from specific IP addresses), and how the user should be handled if they are denied access to a resource (redirect, message, and so on).
- **SSO and Session Management** provides seamless access across multiple cloud, mobile, and web applications from any device, including social login through OAuth, Open ID Connect, and SAML support. The solution manages a user's session across the entire web environment, and this can be implemented with or without cookies. In addition, enhanced session assurance impedes hackers from hijacking legitimate sessions with stolen cookies.
- **Identity Store** is a battle-tested directory server that provides the scalability and reliability needed to support the most demanding on–premises, cloud, and IoT applications with minimal infrastructure and personnel resources. The solution's innovative design enables ultra–high–speed performance as well as transparent load balancing, multi-master replication, and state–based recovery.

Critical Differentiators

Symantec Access Management offers the following competitive differentiators:

- **Fast time-to-protection.** Quickly embed a broad range of native security features into an app or IoT device to protect the enterprise without impacting time-to-market development timelines.
- **Enterprise performance and scalability.** As one of the most scalable access management technologies, the solution has proven deployments handling millions of users and billions of authentications and authorizations.
- **Automated risk mitigation.** The solution analyzes user login data in real-time, continuously monitors user session activity, and can trigger automatic mitigation actions when unusual behavior is detected.
- **Flexible deployment architecture.** The solution supports five different SSO deployment options, which can be used individually or jointly to provide a comprehensive strategy to address access management challenges.
- **Meaningful insights.** The solution provides full visibility into risk rule decisions and outcomes, along with the ability to refine the balance of risk and user convenience that is appropriate for your organization.
- **Convenient access.** The solution supports a wide variety of authentication mechanisms and credentials that can be dynamically enforced based on the risk and/or resource requested.
- **Total cost of ownership.** The solution offers best-in-class total cost of ownership because the solution is quick to deploy, easy to use, and scales. Additionally, the new portfolio license agreement offers flexibility and lower, predictable costs, for your organization.

Value-Add Capabilities

Broadcom offers a broad portfolio of infrastructure software designed to meet and exceed the largest, most complex, and most demanding IT environments. The following capabilities can be easily added to further extend the Symantec Access Management solution:

- **Application Performance Management** optimizes the user journey across web, mobile, and wearables to improve performance and enhance application development.
- **Identity Management** delivers critical self-service and broad provisioning support for on-premise and cloud apps to enable integration with other IT systems and consumer-grade scale.
- **DX AIOps** generates actionable, predictive service intelligence and insights, enabling IT teams to act on and remediate potential issues much earlier before they affect the business.

For more information, please visit **broadcom.com/symantec-iam**.

[1].Data Age 2025: The Digitization of the World From Edge to Core, IDC 44413318, November 2018

[2]Ericsson: Mobility Report, June 2018

Symantec
A Division of Broadcom

For product information, visit our website at: broadcom.com