Symantec
A Division of Broadcom

Product Brief

Symantec® SiteMinder

Key Benefits

- Facilitate DevOps by enabling secure access to cloud, mobile, and web apps.
- Improve user experience through frictionless authentication and single sign-on.
- Provide appropriate access to legitimate users based on dynamic and adaptive policies.
- Deliver operational efficiencies through centralized access management and auditing.
- Optimize app performance by leveraging a platform with carrier-grade scalability and reliability.

Key Features

- Single sign-on and identity federation to provide convenient access to apps located anywhere.
- Interoperability through open standards support, including OpenID Connect, OAuth, SAML, and WS-Federation.
- Support for multiple authentication credentials and mechanisms to balance security and user experience.
- 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 driven by a connected app, or device-based or web-based interface, that provides instant access to data and services. To thrive in this new reality, organizations need to deliver superior user experience with every touch. And things are only going to get worse. In 2025 we will collectively create 175 trillion gigabytes of data[1] and there could be 3.5 billion connected devices by 2023[2]. This explosion of data produces an ever-expanding threat surface that must be protected on an unprecedented scale.

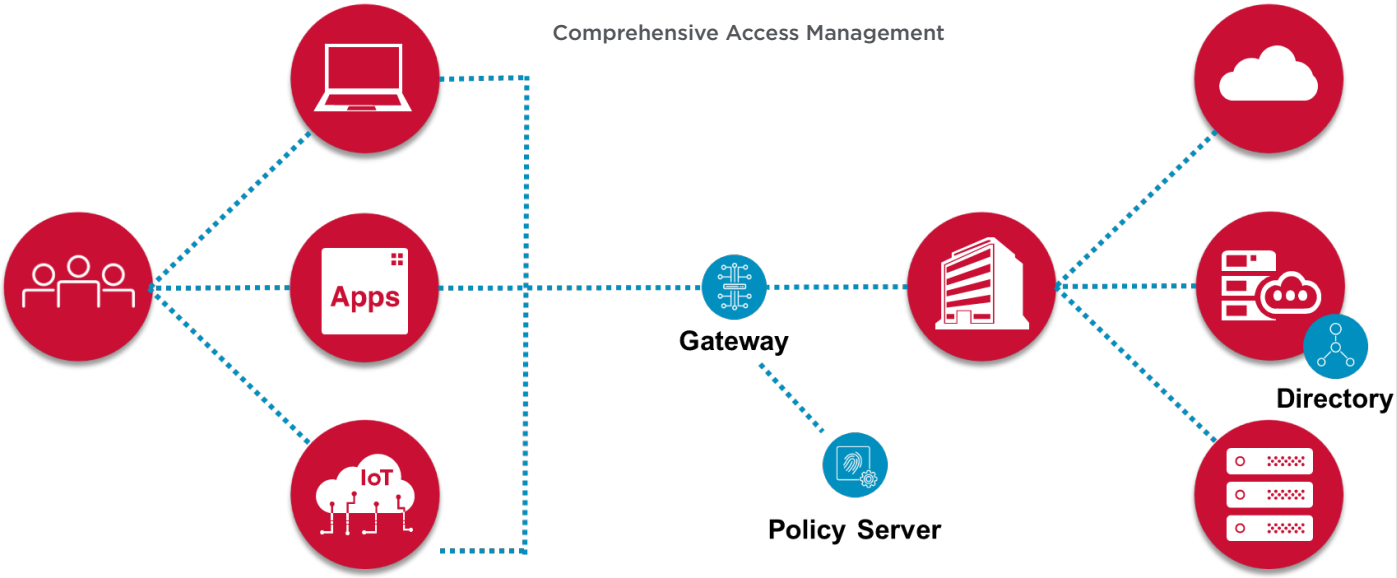
Business Challenges

Because of the pressures to digitally transform and evolve, organizations are rushing new applications to market and expanding into the cloud, often without ensuring that adequate security controls have been implemented. This new hybrid environment, and a 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 approaches to address these newer challenges are built around new security silos and point products, which creates a disjointed experience for the end user and a management burden to the security team. You need to address these challenges with a consolidated access management platform.

Solutions Overview

Symantec® SiteMinder is designed to secure the modern enterprise through a unified access management platform that applies the appropriate authentication mechanism to positively identify users; provides single sign-on and identity federation for seamless access to any application; enforces granular security policies to stop unauthorized access to sensitive resources; and monitors and manages the entire user session to prevent session hijacking. Finally, Symantec SiteMinder is battle-tested and has been deployed in the largest IT environments in the world.

1 Data Age 2025: The Digitization of the World From Edge to Core, IDC 44413318, November 2018
2 Ericsson: Mobility Report, June 2018



Features and Capabilities

Symantec SiteMinder delivers a comprehensive access management solution through two critical components: the access gateway and the policy server, which provide the following core features and capabilities:

- **Authentication management** unifies your authentication strategy to ensure the right level of security across online applications. The solution enforces stronger authentication methods to access higher value or more sensitive applications but allows simpler username and password approaches for lower risk resources. Supporting a wide variety of authentication credentials and mechanisms, the solution helps organizations easily achieve the appropriate balance between security and user experience.
- **Identity federation and single sign-on** provide seamless access across multiple cloud, mobile, and web applications from any device, including social login through OAuth, Open ID Connect, and SAML support. Organizations can easily integrate partner applications and third-party services, which improve the digital experience as users journey across these disparate systems during a single session.
- **Authorization and access control** explicitly grant or deny access to all protected applications and resources through security policies based on a user's profile attributes, group memberships, roles, and other criteria. You can also specify when a user can access specific resources (day and time restrictions), where the user can access a specific resource from (only when logging in from specific IP addresses), and how the user should be handled if they are denied access to a resource (redirects or messages).
- **Session security and management** monitor and protect the user throughout their entire session as they move across your web environment. Implement session management with or without cookies, providing a clear audit trail of everything the user did during a session and impeding 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

- **Fast time-to-protection.** Quickly deploy the solution in dynamically scaled environments such as Kubernetes, Docker, and OpenShift to protect your enterprise without incurring major deployment costs.
- **Enterprise performance and scalability**. 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 and continuously monitors user session activity. Further, the solution can trigger automatic mitigation actions when unusual behavior is detected.
- **Flexible deployment architecture.** The solution supports five different single sign-on deployment options, which you can use individually or jointly to provide a comprehensive strategy to address access management challenges.
- **Meaningful insights**. The solution audits all user activity, including all successful and failed authentications or authorizations, and also tracks all session and site activity.
- **Convenient access**. The solution supports a wide variety of authentication mechanisms and credentials that can be dynamically enforced based on risk or the requested resource.
- **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 scalable. Additionally, the new portfolio license agreement offers flexibility and lower, predictable costs, for your organization.

Related Products and Solutions

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 SiteMinder solution:

- **Symantec Authentication** provides a variety of multifactor credentials and mechanisms that can be deployed on-premise or from the cloud and used to positively authenticate users before granting them access.
- **Symantec 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.

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

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

Symantec-SiteMinder-PB100 February 4, 2020