HAUMOUN
IT PIONEERS

PRODUCT BRIEF

BROADCOM SOFTWARE

SiteMinder™

AT A GLANCE

SiteMinder™ centralizes authentication and authorization services to ensure only authorized users gain access to resources.

KEY BENEFITS

- Enable secure access to cloud, mobile, and web apps
- Improve user experience through frictionless access
- Provide appropriate access based on dynamic and adaptive policies
- Deliver operational efficiencies through centralized access management
- Leverage a platform with carrier-grade scalability and reliability

KEY FEATURES

- Authentication Management
- Identity Federation
- Single Sign-On
- Authorization Management
- Session Management
- Enterprise Scalability

Overview

The IT environment is more complex and more dynamic than ever before. Applications are being deployed faster and faster to support continuous and agile development processes. Every user interaction is being driven by a connected app or a 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, governed by the requisite security, with every touch. For many business owners and developers, this means providing seamless access but how to do you balance user convenience with security concerns? The core capabilities of SiteMinder help to strengthen security and maximize user experience.

Symantec® SiteMinder secures the modern enterprise through a unified, DevOps-friendly access management platform to address this challenge through six key features:

- **Authentication Management.** SiteMinder enforces the appropriate level of login credentials and mechanisms based on context and risk.
- **Identity Federation.** SiteMinder provides frictionless access across identity providers and hybrid environments through native support for OpenID Connect, OAuth, and SAML.
- **Single Sign-On.** SiteMinder streamlines access across hundreds to thousands of cloud, mobile, and web applications by providing single sign-on services.
- **Authorization Management.** SiteMinder grants or denies access to protected resources by enforcing consistent security policies based on contextual data, resource requested, and risk.
- **Session Management.** SiteMinder enables continuous identity and device verification and prevents session hijacking by monitoring user activity as they engage with your apps.
- **Enterprise Scalability and Management.** SiteMinder achieves global service performance and availability through policy and session stores with distributed caching and seamless failover and/or failback with automatic data synchronization. SiteMinder also provide REST interfaces for policy creation and management as well as authentication and authorization services.

With these core features, SiteMinder applies the appropriate level of security to authenticate and authorize users across your hybrid environment with minimal impact to user experience.

SITEMINDER IS PROVEN TECHNOLOGY, SUPPORTING ENVIRONMENTS WITH HUNDREDS OF MILLIONS OF USERS, PROTECTING THOUSANDS OF APPLICATIONS, AND DELIVERING UNPARALLELED PERFORMANCE.

Authentication Management

Being able to positively identify legitimate users from fraudulent ones is an important first step to achieving Zero Trust, and a critical step in your Identity Fabric. Authentication management unifies your authentication strategy to ensure the right level of security across online applications. SiteMinder 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, including passwordless, phishing resistance credentials, organizations can easily achieve the appropriate balance between security and user experience.

Identity Federation

A critical aspect of your Identity Fabric are the identity providers, each of which provides invaluable user data that is needed to facilitate both authentication and authorization. Identity federation enables the organization to weave both internal and external identity providers into your fabric through native support for open standards, including OpenID Connect, OAuth, SAML, and WS-Federation. With this support, organizations can easily integrate third-party services and partner applications, which improves the digital experience and user satisfaction.

Single Sign-On

During a session, consumers may interact with dozens of applications and services, whereas employees and internal users may interact with hundreds. Single Sign-On (SSO) provides seamless access across multiple cloud, mobile, and web applications from any device or location. SiteMinder supports the following five SSO architectures that can be used independently or mixed and matched to meet various business needs:

- **Agent-based** policy enforcement points
- **Centralized gateway** enforcement points
- **Identity federation** standards
- **Agent-less based** approach to securely pass claims to applications without the use of proprietary APIs
- **REST and SOAP-based** Web APIs to allow applications to remotely call SiteMinder as a web service for authentication or authorization

With these architectures, customers successfully integrated thousands of applications into their SiteMinder SSO environments; however, perhaps you do not want to provide seamless access to every application. SiteMinder also provides mechanisms to segregate or restrict access within a SSO environment: realms, protection levels, and security zones.

Authorization Management

Authentication is critical and foundational, but it is not enough. Once you have positively identified users, you still need to authorize them before granting access to the resources they are requesting. SiteMinder provides course-grained authorization across all protected web applications and resources. This is achieved through security policies, which explicitly grant or deny access to a resource based on a user's profile attributes, group memberships, roles, and other criteria. You can also specify day and time restrictions for user resource access, IP address and login parameters for user resource access, and whether a user is redirected or receives a message if they are denied access to a resource.

SECURE THE MODERN ENTERPRISE

Six key SiteMinder features work together to balance strong security with a seamless user experience:

- **Authentication Management.** Enforce the appropriate level of login credentials.
- **Identity Federation.** Frictionless access across identity providers and hybrid environments.
- **Single Sign-On.** Streamlined access across hundreds to thousands of applications via SSO.
- **Authorization Management.** Enforce consistent security policies based on contextual data, resource requested, and risk.
- **Session Management.** Continuous identity and device verification plus user activity monitoring.
- **Enterprise Scalability and Management.** Global service performance and availability.

Session Management

Zero Trust states that you must verify everything trying to connect to your resources before granting access; this requires continuous verification. SiteMinder can manage a user's session across the hybrid environment, and this can be implemented with or without cookies. Session management is not only used to support SSO for users, but also to enforce session and idle timeouts. By monitoring the user's session, SiteMinder can provide continuous verification by promoting the user to re-authenticate when they are attempting to access a more sensitive application or resource. Additionally, SiteMinder can also protect users through enhanced session assurance, which helps prevent unauthorized users from hijacking legitimate sessions with stolen cookies. When the user is initially authenticated, the solution collects specific data from the client machine and uses our patented DeviceDNA process to fingerprint the device. This fingerprint is stored in the session cookie and it is validated on each new request. This validation assures that the client who initiated the session is the same client that is requesting access, which prevents unauthorized users from hijacking legitimate sessions with stolen cookies.

Enterprise Scalability

Scalability and reliability are needed to support the most demanding on-premises, cloud, and IoT applications. SiteMinder is proven technology, supporting environments with hundreds of millions of users, protecting thousands of applications, and delivering unparalleled performance. Load balancing and failover is built into the software at each tier of the application, and the policy and session stores with seamless failover and failback with automatic data synchronization. To scale, you simply need to add parallel processing power at each appropriate stage.

Summary

Symantec SiteMinder delivers unparalleled reliability, availability, scalability and manageability. For over twenty years, it has been the de facto gold standard in enterprise-class secure web access management. Deployed in some of the largest and most demanding environments, SiteMinder helps organizations provide seamless access across hundreds of applications to millions of users.

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

BROADCOM SOFTWARE

About Broadcom Software

Broadcom Software is a world leader in business-critical software that modernizes, optimizes, and protects the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software is building a comprehensive portfolio of industry-leading infrastructure and security software, including AIOps, Cyber Security, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security for the largest global companies in the world.

For more information, visit our website at: software.broadcom.com

Symantec-SiteMinder-PB102 November 28, 2022