PRODUCT BRIEF

Identity Security Platform

Identity Security Without Compromise

AT A GLANCE

Symantec® Identity Security Platform (IDSP) is a cloud-native identity and access management solution that unifies authentication, identity services, and access control to simplify and modernize enterprise identity management, with risk-based policies, self service, and delegated administration for large, hybrid environments.

KEY BENEFITS

- Unify authentication, identity, and access control in a single cloud-native platform
- Reduce identity fraud and account takeover through risk-based, phishing-resistant authentication
- Enable self-service identity and session management to reduce IT overhead
- Implement fine-grained access and resource authorization policies across the enterprise
- Simplify administration with scoped roles and delegated control at scale
- Accelerate secure digital transformation with cloud-native, API-first architecture

Overview

Organizations face mounting pressure to secure identity and access across hybrid cloud, remote workforces, and complex application ecosystems. Traditional point solutions—separate authentication, identity management, and access control platforms—create operational silos, inconsistent policies, and integration gaps that expose organizations to identity fraud, compliance violations, and unauthorized access.

Rather than deploying disconnected point solutions that require costly integrations and fragmented operations, Symantec® Identity Security Platform (IDSP) unifies authentication, identity services, access policies, and resource authorization into a single, integrated cloud-native solution.

Building on the proven foundation of VIP Authentication Hub and evolved through customer feedback and real-world deployments, IDSP delivers not only strong, phishing-resistant authentication but also centralized identity storage, fine-grained authorization, and comprehensive access control services designed for Zero Trust:

- Primary and secondary authentication with FIDO2 phishing-resistant credentials, passwordless methods, and a wide range of multi-factor options to positively identify users at scale
- Embedded identity store with SCIM v2 provisioning and federated identity support
- Policy-orchestrated authentication and access control with contextual, risk-based decision-making
- Fine-grained resource authorization using OAuth2/OIDC-style scopes, roles, and consent flows so applications can request exactly the access they need, and user consent management
- Self-service console empowers users to manage accounts, sessions, and tokens
- Granular administrative roles with scoped delegation and resource-based access control
- Cloud-native architecture with API-first design, Kubernetes support, and zero-downtime updates

This unified approach reduces complexity, lowers total cost of ownership, and enables organizations to implement Zero Trust principles across the entire identity fabric—spanning authentication, identity services, access policies, and resource authorization—without the integration headaches and operational fragmentation of multi-product approaches.

KEY FEATURES

- Unified identity and access platform
- Risk-based, phishing-resistant authentication
- Embedded identity services
- Advanced policy engine for access and authorization
- Self-service console and token management
- Granular administration and delegated control
- Cloud-native, enterprise-grade operations

Key Capabilities

Unified Identity and Access Platform

Unlike disconnected point solutions, IDSP combines authentication, identity services, access policies, and resource authorization in a single integrated solution. This integration eliminates data silos, reduces operational complexity, and ensures consistent security policies across all resources. Organizations no longer need to license and integrate separate authentication, identity management, and access control solutions—everything is delivered as one coherent platform.

Risk-Based, Phishing-Resistant Authentication

The platform protects against the weakest link in security: compromised credentials. Its risk engine analyzes device posture, login behavior, and contextual factors to detect anomalous access attempts and prevent account takeover. IDSP embeds risk-based decision making natively into its authentication policy engine. Combined with FIDO2 phishing-resistant credentials and support for passwordless methods (biometric, passkeys), organizations can enforce strong authentication while minimizing friction for legitimate users through adaptive policy orchestration.

Embedded Identity Services

Rather than relying on external identity directories, the platform provides a built-in identity store with password management, account recovery, and SCIM v2 standards-based provisioning. This eliminates dependency on separate identity management systems and supports flexible federation with external identity providers (SAML, OIDC). Bring-your-own identity (BYOI) and just-in-time (JIT) provisioning flows enable seamless integration with existing directory services while centralizing identity decisions in a single platform, simplifying architecture and reducing integration complexity.

Advanced Policy Engine for Access and Authorization

The platform's expression-based policy engine goes beyond simple role-based access control (RBAC). Authentication policies, post-authentication access policies, and resource authorization policies all use a unified rule engine with contextual conditions (risk score, group membership, IP location, time of day). This allows organizations to craft complex, dynamic access decisions without code. Policies can be prioritized and tested before deployment, reducing risk and implementation time.

Self-Service Console and Token Management

IDSP delivers an integrated self-service console where users can manage passwords, account recovery, sessions, tokens, and application consent from a single interface. This reduces IT support burden, improves user experience, and centralizes identity governance, eliminating the need for multiple disconnected portals across the identity ecosystem.

Granular Administration and Delegated Control

Rather than all-or-nothing admin access, the platform enables scoped administrative roles and resource authorization. Administrators can be restricted to specific applications, user groups, or resource types, enabling safe delegation at scale. The administrative UI includes advanced searching, filtering, and delegation workflows. This allows organizations to operationalize identity management across teams without creating security risks or over-provisioning admin access.

Cloud-Native, Enterprise-Grade Operations

The platform is built from the ground up as a cloud-native, multi-tenant SaaS solution with API-first architecture. It supports Kubernetes, Docker, Helm Charts, and integrations with monitoring tools like Kibana and Grafana—enabling seamless adoption in DevOps and containerized environments. IDSP delivers zero-downtime updates, automatic scaling, and high availability with active-active database configurations. This cloud-native foundation ensures rapid deployment (within minutes), eliminates infrastructure management burden, and positions organizations for future innovation. IDSP can easily be deployed on a variety of platforms, including Google (GCP), Azure (AKS), Amazon (EKS), OpenShift as well as the VMware Cloud Foundation® VKS environment.

IDENTITY IS THE NEW PERIMETER. IDSP DELIVERS A SINGLE, UNIFIED FOUNDATION FOR MODERN IDENTITY AND ACCESS MANAGEMENT.

Why Symantec Identity Security Platform

Unified, Not Fragmented

A single platform unifies authentication, identity services, access policies, and resource authorization—eliminating the complexity, cost, and operational overhead of integrating multiple point solutions.

Built In, Not Bolted On

Risk-based authentication, embedded identity services, policy-driven access control, and self-service capabilities are all natively integrated. This ensures consistent behavior and reduces complexity across all identity functions.

Purpose-Built for Enterprise Scale

From cloud-native architecture to active-active database support, the platform is engineered for enterprise deployments. Built from the ground up for modern, distributed, high-scale operations.

VMware®-Aligned Identity Services

IDSP is optimized to run on VMware Cloud Foundation and VMware vSphere® Kubernetes Service, delivering authentication, authorization, and identity services as a first-class part of your VCF-based cloud platform. This alignment enables simple deployment, automatic scaling, and lifecycle management of IAM components alongside your VMware-based infrastructure, while keeping identity services contained within your secured environment.

Rapid Deployment, Low TCO

Cloud-native SaaS delivery, API-first design, and minimal configuration reduce time-to-value. Organizations achieve lower total cost of ownership while gaining superior capability and operational simplicity.

Summary

Identity is the new perimeter. As organizations embrace hybrid cloud, remote work, and digital transformation, the need for a unified, intelligent identity platform has never been greater. Symantec Identity Security Platform delivers a single, unified foundation for modern identity and access management.

By combining authentication, identity services, access policies, and resource authorization in one cloud-native platform, organizations can implement Zero Trust faster, simplify operations, reduce costs, and enable secure digital transformation without the complexity and compromise of multi-product approaches.

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

BROADCOM®
connecting everything®

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

IDSP-PB100 January 16, 2026