

Product Brief

At a Glance

Unify endpoint and server management to strengthen security, improve visibility and control, and automate IT lifecycle operations at scale.

Business Outcomes

- Reduce security risk and exposure.
- Improve operational predictability.
- Lower operational costs and tool sprawl.
- Strengthen compliance and audit readiness.

Capabilities

- Centralized deployment and patching
- Lifecycle asset visibility
- Real-time operational control
- Remote and hybrid endpoint management
- Process automation and self-service

Symantec[®] IT Management Suite

Unified Endpoint and Server Management for Secure, Predictable IT Operations

Overview

Organizations now manage a mix of endpoints and servers across data centers, clouds, and remote locations, while attackers use automation and AI-assisted tools to find misconfigurations and unpatched systems faster than traditional processes can respond. Even with strong identity controls and threat detection, many teams struggle to maintain a consistent view of what they have, how it is configured, and whether it is protected against current threats.

Symantec[®] IT Management Suite (ITMS) is designed to address this gap by providing a unified platform for endpoint and server management. It brings together deployment, patching, configuration, asset tracking, and policy-based control so IT teams can see the state of their environment and orchestrate the changes needed to keep systems secure and compliant. This unified approach helps reduce reliance on disconnected tools and manual checks, making it easier to run IT operations with confidence as environments grow and evolve.

Endpoint Management Must Go Beyond Basic Policy and Patching

Most organizations already use tools to enroll devices, apply baseline policies, and deliver routine updates, but risks extend far beyond basic configuration and occasional patch cycles. Complex estates with a mix of endpoints and servers, remote and low-bandwidth locations, and diverse application stacks create more opportunities for misconfigurations, missed updates, and unmanaged systems to slip through.

At the same time, attackers are using automation and AI-assisted techniques to discover exposed services, missing patches, and weak configurations faster than traditional, batch-oriented processes can react. In this landscape, simply having a patch catalog or a cloud-based policy engine is not enough. Effective endpoint and server management requires trusted, real-time inventory, deeper lifecycle visibility, and precise control over when and how changes land; so urgent fixes, planned maintenance, and compliance-driven updates can all be executed with confidence.

Introducing Symantec ITMS

Symantec ITMS unifies endpoint and server management on a single platform, giving IT teams a consistent way to see, control, and update their environments. It combines OS deployment, software distribution, patch management, configuration, and asset tracking so organizations do not have to rely on disconnected tools or manual checks to understand what is deployed and in what state.

By integrating asset, client, and server management, ITMS provides accurate lifecycle inventory, real-time operational control, and scalable automation for desktops, laptops, and physical or virtual servers. This unified approach helps teams respond faster to emerging threats, coordinate maintenance windows with greater precision, and support security and compliance requirements across complex, hybrid environments.

Solution Capabilities

Symantec ITMS delivers a set of core capabilities that help IT teams see, control, and automate their endpoint and server environments. Together, these capabilities replace disconnected point tools with a unified approach to deployment, patching, asset visibility, and day-to-day operations.

- **Centralized deployment and patching:** Automated OS deployment, software distribution, and multiplatform patch management for endpoints and servers.
- **Lifecycle asset visibility:** CMDB-backed discovery, inventory, and asset tracking including contracts, warranties, and license usage.
- **Real-time operational control:** Time-critical management, on-demand patch assessment, and Patch Now actions for predictable remediation.
- **Remote and hybrid endpoint management:** Cloud-enabled management for devices outside the corporate network.
- **Process automation and self-service:** Workflows, content distribution, and a modern software portal to reduce manual effort and help desk load.
- **Supporting remote and hybrid workers at scale:** Keep remote and hybrid users' devices visible, patched, and up to date, even when they are frequently off the corporate network. Cloud-enabled management helps ensure Windows and Mac endpoints receive inventory, software, and security updates without relying exclusively on VPN connectivity.
- **Improving patch precision and vulnerability response:** Use real-time inventory, time-critical management, and Patch Now capabilities to react quickly when new vulnerabilities are disclosed. Organizations apply targeted updates to affected systems, coordinate maintenance windows with business owners, and verify that remediation has completed successfully.
- **Strengthening compliance and audit readiness:** Maintain a trusted view of hardware, software, contracts, and license usage to support security and regulatory requirements. ITMS helps teams answer audit questions faster, demonstrate patch and configuration compliance, and align asset data with internal and external reporting needs.
- **Optimizing IT operations and reducing manual work:** Automate recurring tasks such as inventory gathering, OS deployment, patch rollouts, and software distribution. When combined with a self-service software portal, these capabilities reduce help desk volume and free IT staff to focus on higher-value initiatives rather than repetitive maintenance.

Enterprise Use Cases

- **Managing mixed endpoint and server environments:** Standardize deployment, patching, and configuration across desktops, laptops, and physical or virtual servers. IT teams use ITMS to maintain consistent builds, control change windows, and reduce the risk of misconfigurations in heterogeneous estates.

- **Improve operational predictability:** Coordinate deployments, updates, and maintenance windows with greater confidence through centralized control and clear rollout status, reducing surprises for both IT teams and business stakeholders.
- **Lower operational effort and tool sprawl:** Replace manual processes and multiple point tools with policy-driven automation in a unified platform, helping IT teams reclaim time for higher-value initiatives while simplifying day-to-day management.
- **Strengthen compliance and audit readiness:** Use accurate lifecycle inventory, configuration data, and reporting to demonstrate patch and asset compliance more easily, respond to audit requests faster, and support internal and regulatory requirements.

Why Symantec Solutions?

Symantec ITMS is built on decades of experience managing complex endpoint and server environments, combining proven Altiris technology with the scale and investment of the Broadcom® cybersecurity portfolio. It offers deeper lifecycle management, inventory, and operational control than basic, policy-only tools, helping organizations unify deployment, patching, configuration, and asset visibility in a single, enterprise-ready platform.

By integrating with other Symantec solutions and aligning with modern security models, ITMS helps customers strengthen security and compliance while simplifying day-to-day operations. For organizations facing fast-moving threats and growing hybrid estates, Symantec solutions deliver a management platform that is comprehensive, mature, and designed to evolve alongside their broader IT and security strategy.

Business Outcomes

- **Reduce security risk and exposure:** Lower the likelihood and impact of incidents by maintaining trusted, real-time visibility into endpoints and servers, and by automating patching and configuration changes across the environment.



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

Copyright © 2026 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.
Symantec-ITMS-SB104 June 22, 2026