SOLUTION BRIEF

IT Management Suite

In a world with expanding threats and vulnerabilities, a wider range of endpoints, and rapid expansion of remote workers, the Symantec® IT Management Suite (ITMS) automates common IT processes to reduce costs and improve security posture.

KEY BENEFITS

- **Improves security posture:** Identifies and remediates known vulnerabilities.
- **Increases productivity:** Automates hardware and software deployment and configuration.
- **Reduces costs:** Centrally manages multiple endpoint platforms from one unified console.
- **Avoids vendor penalties and fines:** Compares software inventory and usage data with license agreements to support compliance and optimization.

KEY FEATURES

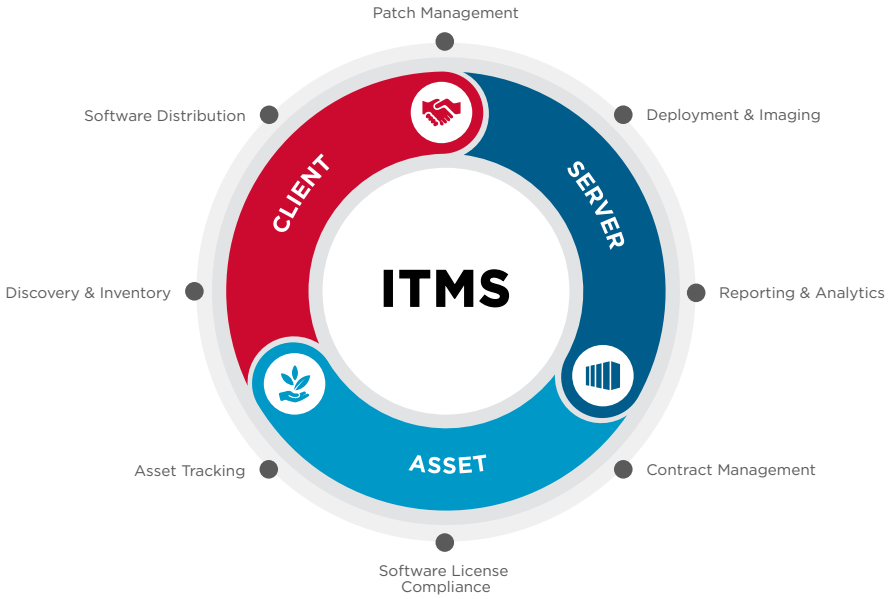
- Endpoint deployment and provisioning
- Network discovery and collection of hardware/software inventory data
- Patch management
- Software distribution
- Software license compliance and optimization
- Asset and contract management

Overview

Organizations are implementing stronger authentication mechanisms to distinguish legitimate users from fraudulent ones, but what about the end users' devices? External attackers have learned to target end users and their devices, with the most successful attacks exploiting known vulnerabilities simply because endpoints were not properly configured or patched. These weaknesses exist because many organizations lack real-time visibility into the state and usage of their own endpoints and software. One of the tenets of Zero Trust is to verify every identity and device requesting access. The Symantec® IT Management Suite (ITMS) enables you to meet this challenge.

The versatile ITMS suite of tools provide powerful real-time management and patch capabilities to strengthen security posture, while maximizing end-user productivity by simplifying and accelerating operating system deployment and migration, providing end user self-service capabilities, and helping organizations track and manage IT assets. ITMS securely manages devices both inside and outside the perimeter by focusing on three critical areas:

- **Security:** Improve security posture by providing visibility into the hardware and software in your environment, identifying and remediating vulnerabilities, and ensuring compliance.
- **Productivity:** Increase productivity by automating the deployment and configuration of hardware and software while minimizing costs and optimizing operational efficiency.
- **Versatility:** Efficiently manage and secure hardware and software across multiple platforms from a single, unified console.



GAIN REAL-TIME VISIBILITY INTO THE STATE AND USAGE OF YOUR ORGANIZATION'S ENDPOINTS AND SOFTWARE

ITMS combines the capabilities and features of three powerful products into one comprehensive solution:

- **Asset Management Suite**
- **Client Management Suite**
- **Server Management Suite**

Security

Real-Time Management

The foundation of secure and successful server management is an accurate picture of what you have. ITMS provides network discovery and inventory tools that automatically collect this information and populate it into the Configuration Management Database. The solution can also perform inventory actions on-demand and in real-time using a feature called Time Critical Management (TCM). This provides immediate intelligence about what is happening in your environment to help make the right decisions faster than ever. Additionally, TCM also includes Patch Now support, which can be used to identify and remediate zero-day vulnerabilities by initiating the execution of a patch system assessment scan and installation of software updates on demand.

Patch Management

Many successful attacks exploit previously-known vulnerabilities for which a patch was already available from the software vendor. However, patching endpoints often requires longer implementation cycles due to the necessary demands of pretesting to minimize potential service disruptions. ITMS improves overall security by providing automated, robust patch management, including the following capabilities:

- Support for Microsoft, macOS, RedHat, CentOS, and SUSE updates
- Support for laptops, workstations, and servers
- Support for security and non-security related updates
- Support for commonly used third-party applications
- Cloud-enabled management for remote users who are not connected to your organization's network
- Peer-to-peer downloading for sites with limited bandwidth

ITMS patch management enables organizations to successfully combat threats by providing the means to easily detect vulnerabilities throughout your environment and quickly remediate them from a central console.

Risk Mitigation

ITMS provides real time, actionable compliance reports so you can make the smart and fast decisions required to ensure your environment remains protected, while automation allows you to further streamline the process. These tools can be leveraged to quickly gather an inventory and status of assets to avoid a time-consuming IT fire drill during a software audit. In addition, for those software updates that remediate vulnerabilities, you can even report on compliance and create software update policies based on the CVE-IDs assigned to the vulnerabilities.

Additionally, ITMS allows organizations to apply patches as part of the deployment process when provisioning new computers. This equips customers to use a standard image that does not need to be constantly updated and ensures new computers are not vulnerable as soon as they come online.

Productivity

ENABLEMENT AND AUTOMATION ARE THE KEYS TO SUPPORTING A REMOTE WORKFORCE, ENSURING PRODUCTIVITY WITHOUT SACRIFICING SECURITY.

Deployment, Provisioning, and Migration

IT administrators leverage ITMS to deploy and manage desktops, laptops, and servers, whether physical or virtual, across a broad array of platforms. The solution provides OS deployment and configuration, PC personality migration, and software distribution capabilities that can be used to create automated, repeatable processes which reduce the cost of provisioning desktops, laptops, and servers.

You can build a reference system with your organization's standard operating environment, including both OS and apps, and then mass-deploy a hardware-independent image to new and existing systems. These deployment capabilities ensure consistent configurations across large numbers of endpoints. Additionally, because each system is unique, you can assign Security IDs (SIDs) and configure user names, IP addresses, and other network settings.

EMPOWERING END USERS REDUCES THE BURDEN ON IT AND IMPROVES END USER SATISFACTION.

End User Self-Service

ITMS features a modern software portal that provides a familiar app store-like experience and allows users to request and install software with little or no administrator involvement. In addition, the portal can be customized with your organization's logo and branding, and is accessible across all browsers from any Windows or Mac computer on which the Symantec Endpoint Management agent is installed. By simplifying the process of delivering and installing software, ITMS can significantly reduce help desk calls related to software requests.

Asset Management

Organizations often do not have an accurate picture of their assets. The results of this inaccuracy can include paying support and maintenance for software that is installed on machines but not being used, or penalties and fines for using more software than you are licensed for. ITMS addresses this concern through three core features, which provide accountability and cost control of discoverable and fixed assets:

VISIBILITY INTO INVENTORY AND USAGE DATA, AND THE ABILITY TO CORRELATE IT TO CONTRACTS AND LICENSES, OPTIMIZES IT SPENDING AND SUPPORTS COMPLIANCE.

- **Configuration Management Database (CMDB).** Discover, inventory, and track all hardware and software assets in your organization. Information about these assets are stored in the CMDB, which manages the relationships between assets and configuration items, users, locations, departments, cost centers, and associated contracts.
- **Contract Management.** Minimize the burden of managing vendor contracts related to hardware warranties and leases, as well as software maintenance and support agreements. The integration of contract and financial cost data allows you to effectively forecast hardware and software needs while avoiding penalties and late fees.
- **Software License Management.** Robust software license management capabilities not only support per-device and per-user license models, including site-based and enterprise definitions, but also support per-CPU and per-processor models often used for server applications.

CRITICAL DIFFERENTIATORS

ITMS offers the following competitive differentiators:

- **Management throughout the asset lifecycle**: Automate and streamline IT and business processes across multiple endpoints and ensure they are properly retired at end of life.
- **Ease of use**: A modern, web-based centralized management console helps manage heterogeneous environments with scalable architecture.
- **Meaningful insights:** Comprehensive asset inventory provides better visibility for software compliance audits.
- **Automated risk mitigation:** Automatically identify known vulnerabilities and remediate them through patch management.
- **Best-in-class total cost of ownership:** Quick to deploy, easy to use, and scalable.

Versatility

Remote Endpoint User Management

The number of people working remotely has increased significantly and is expected to remain at high levels for the foreseeable future. This presents a challenge for organizations as remote desktops and laptops may fall behind in updates. ITMS addresses this with Cloud-Enabled Management (CEM). CEM utilizes a gateway to provide trusted communications with remote clients outside the firewall when users are not connected through VPN, and ensures that inventory, patches, and software stay current even when devices are disconnected from the corporate network. When users are working remotely and their devices are connected via VPN, cloud-enabled management provides a means to optimize traffic flow so only critical business traffic is routed over the VPN.

Modern Device Management

The paradigm for endpoint management is evolving. As vendors have added management capabilities to operating systems, Modern Device Management (MDM) simplifies the process of managing devices by leveraging protocols built into the operating system rather than an agent. In the case of macOS, some important management settings can only be configured via MDM. ITMS includes native MDM capabilities and specifically provides the ability to enroll macOS devices, configure the value of numerous management-related properties, install applications, and perform actions such as collecting inventory data and shutting down, restarting, locking, and erasing devices.

Process Automation and Efficient Content Distribution

One of the many strengths of ITMS is its ability to streamline IT and business practices. ITMS tasks and policies automate the collection of inventory data, the distribution of software, and the rollout of patches on a predefined schedule or on-demand, across multiple endpoints from a unified management console. In addition, ITMS enables you to build workflow processes to automate ITMS-related actions or build integration with other systems.

In addition to securely managing endpoints, ITMS optimizes content distribution with built-in resiliency, peer-to-peer, and bandwidth-throttling features. These features reduce content delivery time, minimize bandwidth consumption, and improve the reliability of content delivery. You will benefit from these features when you distribute cumulative updates and large software packages to client computers, especially to devices at sites with low-bandwidth connections and no dedicated site servers.

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

BROADCOM®
connecting everything®

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

Symantec-ITMS-SB102 November 17, 2023