Symantec
A Division of **Broadcom**

Client Management Suite 8.6
Security. Versatility. Productivity.

At A Glance

Client Management Suite 8.6 alleviates many of these day to day operational challenges by consolidating the functions found within the endpoint management life-cycle in a single, easy to use solution.

Discovery and Inventory

• Discover any resource that responds to network communications

• Collect and report information about computer hardware, operating systems, software, and users in your network.

Imaging and Deployment

• Reduce the cost of deploying and managing desktops, laptops and thin clients from a centralized location in your environment.

• Manage OS deployment, configuration, PC personality migration, and software deployment across hardware platforms and OS types.

Patch Management

• Scan managed computers to determine the software updates (patches) that they require.

• Automatically download updates from software vendors and install on computers that require them.

Software Distribution

• Control software configurations and distribution to your client computers through automated policies

• Ensures that the required software remains installed, is in a working state, and is correctly configured on client computers.
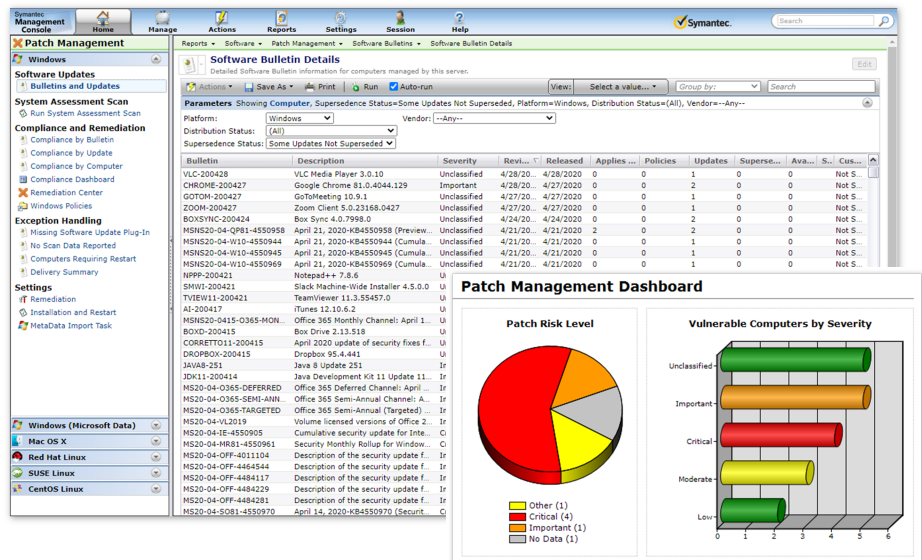
Overview

Symantec Client Management Suite (CMS) helps manage, patch, and remediate application and OS configurations for desktops, laptops and thin-clients throughout their life-cycle to strengthen endpoint security and maximize user productivity. CMS supports all major operating systems, provides both real-time and persistent management of endpoints inside and outside the perimeter, and has extensive deployment and patch management capabilities.

Patch Management

An effective patch management strategy is critical for distributing software updates and, more importantly, for detecting and remediating security vulnerabilities. Many successful attacks are perpetrated against previously known vulnerabilities in which a patch or secure configuration standard was already available from the software vendor. Patches are only effective if they have been deployed.

CMS centralizes and simplifies patch management. With this solution you can detect and remediate security vulnerabilities for Windows, Mac, and Linux operating systems as well as Microsoft and commonly used third-party applications. Patch automation can further streamline the process to ensure patches are applied as quickly as possible. Real-time compliance and detailed reports help ensure smart, fast decisions can be made to keep endpoints protected and maximize productivity. Key Patch Management features include:

• Support for Windows, Mac, and Linux operating systems

• Support for Office 365 and Windows 10 updates

• Support for commonly used third-party applications

• Cloud enabled management for computers used by remote workers

• Peer-to-peer downloading for sites with limited bandwidth

Deployment

CMS helps reduce the cost of deploying and managing desktops and laptops from a centralized location in your environment. The solution offers OS deployment, configuration, PC "personality" migration, and software deployment across hardware platforms and OS types to reduce end-user downtime and increase IT efficiency through automated, repeatable deployment processes.

For example, you can build a reference system with your standard OS and applications and then mass-deploy a hardware-independent image of the reference system to your new and existing systems. Because every system is unique, you can assign security IDs (SIDs) and configure user names, IP addresses, and other network settings.

In addition to supporting a wide variety of hardware types, CMS also supports multiple operating systems, including Windows, Mac OS X, and Linux. Deploying desktops, thin clients and laptops has never been easier. Key Deployment features include:

- Web console well suited for distributed access and detailed security models
- Support for Windows PE and Linux pre-boot images
- Supports for PXE and iPXE environments
- Support for hardware independent image deployments
- Hands-free migration
- Ability to configure new systems using imaging, scripting, or a combination of both

Cloud-Enabled Management

The number of people working remotely significantly increased as a result of the COVID-19 pandemic and is expected to significantly exceed pre-pandemic levels going forward.

Cloud-enabled management, a long-time feature of CMS, directly addresses this challenge by ensuring that inventory, patches and software (including Symantec Endpoint Protection) stay current on Windows and Mac devices even when they are disconnected from the corporate network.

Cloud-enabled management utilizes an Internet gateway in the DMZ to provide certificate-based trusted communication over the Internet between remote clients outside the firewall and the Symantec management server inside the corporate firewall. It ensures management is "always on" even when remote users are not connected through VPN.

When people are working remotely and their devices are connected via VPN, cloud-enabled management provides a means to optimize the flow of traffic, enabling the VPN tunnel to be reserved for critical business traffic while routing less essential management traffic to be routed over the Internet outside the VPN tunnel.
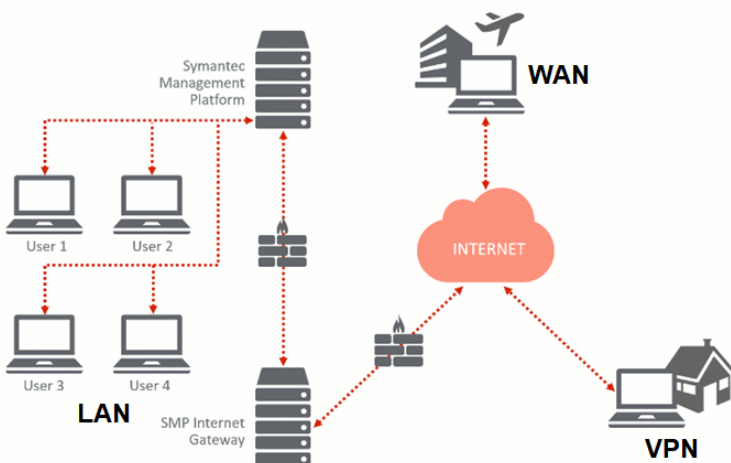
Comprehensive Inventory

Inventory Solution provides a comprehensive assessment of your discoverable assets supporting virtually any platform. The solution provides the foundation to achieve your management goals by aggregating data across your environment. so that you can quickly and easily generate software audit reports, assess security vulnerabilities, and more accurately determine hardware needs and availability.

Inventory Solution allows you to easily track comprehensive hardware information, installed software packages, and operating system settings for all IT assets throughout their life-cycle. Data is normalized, consolidated, and secured in a central repository, enabling detailed reporting of asset information from the convenience of a web console

Self-service Software Portal

CMS features a modern software portal that provides an "app store like" user experience for requesting and installing software with little or no administrator involvement. The software portal can be customized with your organization's logo and brand and is accessible across all browsers.

The software portal helps reduce help desk calls related to software requests by simplifying the process of delivering and installing software in a way that most users have grown accustomed to on their mobile devices. Users can quickly and easily access the software portal from any Windows or Mac computer on which the Symantec management agent is installed.
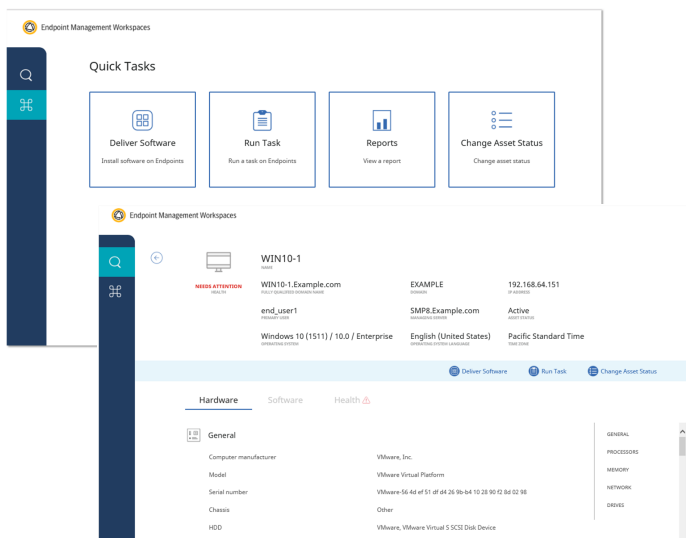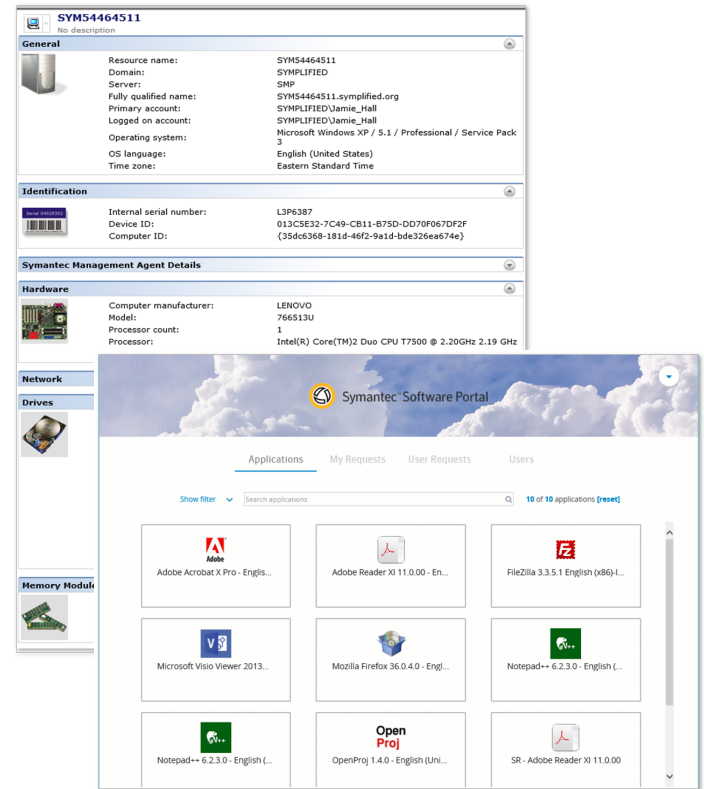
Modern UI Workspaces

CMS includes a modern UI for performing common everyday tasks. These "workspaces" use a web-based console based on HTML 5 that is browser agnostic and can be accessed from any device including Mac OS.

The workspaces are simple to use and specifically designed for technicians with little or no experience and without the need for special training. Technicians using the modern UI workspaces will only see what they need to do their job. The modern UI workspaces provide an optimized user experience designed to reduce the number of screens and clicks required to perform tasks by as much as 50%.

- Search and view inventory details for a selected endpoint
- Run tasks on one or more endpoints
- Deliver and install software on one or more endpoints

Time Critical Management

One of the many strengths of CMS is its ability to perform actions on a pre-defined schedule such as gathering inventory, updating software, and sending out patches. These persistent management capabilities are augmented by "Time Critical Management" (TCM) that performs actions on-demand and in real-time.

In the ITMS 8.6 release, TCM has been expanded to include "Patch Now" support that can be used to identify and remediate zero-day vulnerabilities by initiating the execution of the Windows patch system assessment scan and installation of software updates on-demand.
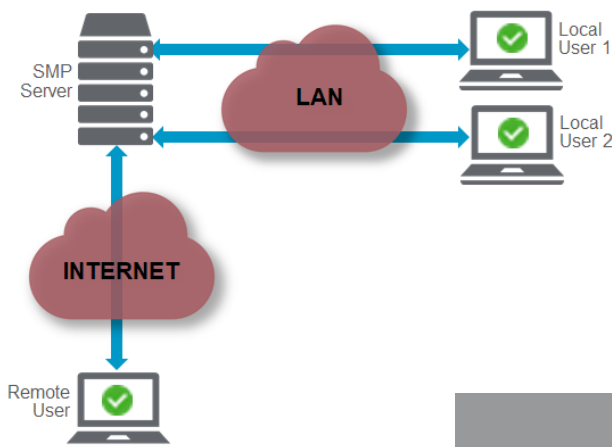
Endpoint Compliance and Quarantine

One exciting feature in CMS is made possible through integration with Symantec Endpoint Protection (SEP). During an outbreak of a critical vulnerability (i.e. WannaCry), there may be a delay between when a patch is available or when it is possible for all machines to be patched. This gap in time can be mitigated through using CMS and SEP together to block network access to any endpoint that fails a compliance scan.

SEP Agent Health

Another key integration point is the ability of CMS to monitor the health of the SEP agent in an on-premise installation, adding an additional layer of protection. Information gathered by CMS from SEP clients on Windows and Mac computers in your environment enables you to identify issues related to the health of the SEP agent.

Symantec Endpoint Protection Manager

Notification Server

User 1   User 2   User 3   User 4
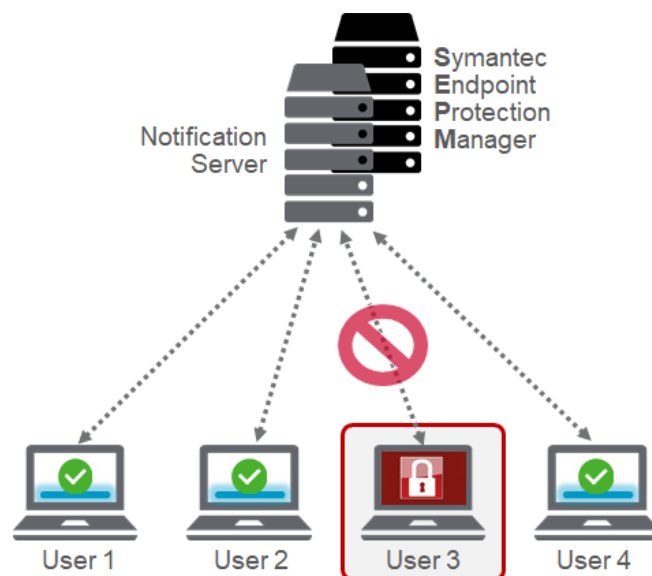
Summary

Managing an IT environment in today's world continues to become more complex. There are a wider range of devices and operating systems, more vulnerabilities and threats, and users who need to be able to work from any location using any device.

This requires IT to have immediate intelligence on what's happening in their environment and the ability to take instant action to ensure users are productive and protected. The key capabilities of Symantec Client Management Suite help strengthen endpoint security and maximize user productivity.

Learn more about Client Management Suite at https://go.symantec.com/manage

For the latest Platform Support Matrix and documentation, see https://techdocs.broadcom.com

Symantec™
A Division of **Broadcom**