PRODUCT BRIEF

The Risks of the Ever-Expanding Enterprise Network Landscape

KEY FEATURES

Symantec® IT Management Suite focuses on three critical areas:

- **Security:** Improve your security posture by providing visibility into your environment's hardware and software, 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 unified console.

KEY CAPABILITIES

The following automated patch management capabilities enhance security:

- **Automated vulnerability detection:** Identify and remediate known vulnerabilities, install updates to address security flaws, fix bugs, and introduce new features.
- **Accurate patch management:** Eliminate false positives by identifying superseded updates, locate vulnerabilities, and remediate them through a centralized console.
- **Schedule-based monitoring and on-demand visibility:** Ensure compliance and security with consistent endpoint monitoring.

Overcome the Challenges of Modern Endpoint Management

As organizations expand and evolve their IT infrastructure, enterprise networks become more decentralized and complex. IT management teams face the critical challenge of safeguarding and optimizing these dynamic environments. However, traditional endpoint management methods often fail to keep pace. The following challenges are common:

- Difficulty tracking the numerous moving parts of the network.
- Reactive responses to demands and threats instead of proactive strategies.

These challenges result in unpatched vulnerabilities, leaving systems exposed to threats and missing opportunities to enhance network performance.

Patch It or Pay the Price: The Risks of Neglecting Vulnerabilities

Failure to patch IT systems can have catastrophic consequences. Consider these alarming statistics:

- High-risk vulnerabilities exist in 84% of companies. Half of these vulnerabilities could be resolved with a software update (Get Astra Blog, 35 Cyber Security Vulnerability Statistics, January 9, 2025).
- There were 40,000 new vulnerabilities identified in 2024 alone (National Institute of Standards and Technology).
- Breaches resulting from exploited vulnerabilities increased by 180% in 2023 (Verizon 2024 Data Breach Investigation Report).
- The median time for organizations to scan for non-CISA KEV vulnerabilities is 68 days (Verizon 2024 Data Breach Investigation Report).
- A year after patches are available, 8% of those vulnerabilities remain unresolved (Verizon 2024 Data Breach Investigation Report).

Unpatched IT systems with known vulnerabilities pose significant risks to organizations, exposing them to cyber attacks, data breaches, and operational disruptions. These vulnerabilities allow attackers to exploit security gaps, deploy malware, steal sensitive data, or disrupt critical services.

Delays in patching amplify the likelihood of attacks, as cybercriminals often exploit vulnerabilities within days of discovery. Beyond security concerns, unpatched systems can result in compliance violations, financial penalties, and irreparable reputational damage. In today's complex IT environments, timely and effective patch management is no longer optional; it is essential for safeguarding the modern enterprise.

Mind the Gaps: Challenges in Closing the Vulnerability Door

Organizations struggle to patch their IT systems because of three key challenges.

Lack of Visibility into the IT Environment

Organizations often struggle to view their network assets comprehensively. Identifying which systems need patching becomes difficult without accurate and real-time visibility into all endpoints, applications, and devices. This gap allows vulnerabilities to remain unnoticed and unaddressed.

Remote Workforce and Disruption Risks

The number of people working remotely has increased significantly and is expected to remain at high levels for the foreseeable future. This environment challenges organizations. Remote desktops and laptops may fall behind in updates, and IT may hesitate to disrupt user productivity by forcing them to self-patch.

Resource Constraints and Patch Overload

The sheer volume of vulnerabilities identified each year makes it challenging for IT teams to keep up. With limited staff and competing priorities, patch management often becomes reactive instead of proactive, exposing organizations to attack. Additionally, prioritizing which patches to deploy first is difficult without effective tools or processes.

Modern IT teams need a robust endpoint management platform.

Introducing Symantec® IT Management Suite

Symantec IT Management Suite (ITMS) includes a versatile set of tools that provide powerful real-time management and patch capabilities to strengthen security posture, while maximizing end-user productivity. Symantec ITMS securely manages devices both inside and outside the perimeter by focusing on three critical areas:

- Security: Improve your security posture by providing visibility into your environment's hardware and software, 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 unified console.

Improving Visibility and Prioritizing Vulnerability Remediation

Effective endpoint management begins with clearly and accurately understanding your IT environment. Symantec ITMS simplifies this process by providing powerful network discovery and inventory tools that automatically gather critical asset data and populate it into a configuration management database. Additionally, Symantec ITMS features Time Critical Management, enabling real-time, on-demand inventory actions. This feature provides immediate insights into your environment, empowering IT teams to make faster, more informed decisions.

Automated Patch and Vulnerability Management

Symantec ITMS enhances security by automating patch management across a wide array of platforms, devices, and applications:

- Supports updates for Microsoft, macOS, RedHat, CentOS, SUSE, and third-party applications.
- Covers laptops, workstations, and servers, including remote users with cloud-enabled management.
- Addresses both security and non-security updates, with peer-to-peer downloading for bandwidth-constrained sites.

Symantec ITMS has the following capabilities:

- **Automated vulnerability detection:** Identify and remediate known vulnerabilities, install updates to address security flaws, fix bugs, and introduce new features.
- **Accurate patch management:** Eliminate false positives by identifying superseded updates, locating vulnerabilities, and remediating vulnerabilities through a centralized console.
- **Schedule-based monitoring and on-demand visibility:** Ensure compliance and security with consistent endpoint monitoring.

Enhancing Remote User Security and Productivity

Symantec ITMS ensures remote desktops and laptops receive timely updates through Cloud-Enablement Management (CEM). CEM establishes trusted communication with remote clients outside the firewall, eliminating the need for VPN connections. CEM keeps inventory, patches, and software current, even when devices are disconnected from the corporate network. Additionally, when users connect through VPN, CEM optimizes traffic flow by routing only critical business traffic over the VPN, reducing network congestion.

Enhancing Remote User Security and Productivity (cont.)

Symantec ITMS also features a modern software portal that offers a familiar, app-store-like experience. This portal allows users to request and install software with minimal administrator involvement, significantly reducing help desk calls related to software requests. Customizable with your organization's branding, the portal is accessible from any Windows or Mac computer running the Symantec ITMS agent, delivering a seamless and user-friendly software distribution experience.

Streamlining IT Operations and Reducing Patch Management Burden

Symantec ITMS streamlines IT and business operations by automating critical processes such as inventory data collection, software distribution, and patch deployment. Policies can be executed based on a schedule, while tasks can be executed on-demand or on a schedule across multiple endpoints from a unified management console. Symantec ITMS also enables the creation of custom workflows to automate Symantec ITMS-related actions and integrate seamlessly with other systems.

With advanced features like Patch Now support, Symantec ITMS addresses zero-day vulnerabilities by initiating immediate patch scans and software updates. Real-time, actionable compliance reports empower organizations to make swift, informed decisions to maintain a secure environment.

Automation further enhances efficiency, eliminating the need for time-consuming emergencies during software audits by providing quick access to asset inventory and status. Symantec ITMS also facilitates compliance reporting and the creation of software update policies based on CVE-IDs for vulnerabilities.

By combining robust automation, real-time visibility, and powerful reporting tools, Symantec ITMS enables organizations to proactively detect and resolve vulnerabilities, safeguarding IT environments with minimal disruption.

Benefits of an Automated, Cost-Efficient Endpoint Management Platform

Symantec ITMS delivers a comprehensive, modern endpoint management solution designed to empower organizations in today's complex IT environments. By combining real-time visibility, automation, and robust features, Symantec ITMS helps organizations.

Gain Immediate Network Insights

Discover and inventory all devices to maintain an accurate, up-to-date network view.

Improve Security Posture

Identify and remediate vulnerabilities proactively to safeguard endpoints against evolving threats.

Boost End-User Productivity

Provide employees with self-service access to IT resources and software, increasing efficiency and satisfaction.

Optimize Operations

Automate deployment, provisioning, and migration, reducing operational overhead and costs.

Streamline IT Management

Automate routine tasks and deliver comprehensive asset lifecycle management to simplify IT operations.

Software and Hardware License Management

Oversee hardware warranties, leases and software license management to ensure cost control, compliance, and accountability across IT assets.

Minimize Total Cost of Ownership

With fast deployment, scalability, and user-friendly features, Symantec ITMS optimizes costs and adapts to the needs of even the largest enterprises.

Symantec ITMS equips IT teams to meet the challenges of decentralized networks, diverse endpoints, and growing remote workforces with efficiency, security, and confidence.

BROADCOM®
connecting everything®

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