ConnectWise Automate

What is ConnectWise Automate? Supports 6,500 MSP's and 100,000 devices

ConnectWise Automate is a remote monitoring and management tool (RMM) that allows us to actively track the health and performance of your IT network. We compile that data to proactively monitor computer performance, security levels and manage all the assets in your IT environment. This allows us to deliver streamlined reactive and proactive managed services, meaning we can stop putting out fires and start focusing on what matters most. In addition, this program gives our help desk immediate access to your IT problems.

ConnectWise also allows us to manage everything from one control center. This means their integration with hundreds of applications gives our team the tools to more quickly isolate, identify and resolve issues.

Several Integrated Products:

- Anti-Malware Software
- Anti-Virus Software
- Encryption
- Mobile Device Management (MDM)
- Patch Management
- Remote Control of your desktop
- Third Party Patch Management

Additional Features:

- Asset Management and Reporting
- Automatically Restart Devices
- Automatic Disk Cleanup (Windows Devices)
- Compliancy Reporting
- Software Blacklisting
- Software License Management

Anti-Malware Software:

Malwarebytes

Antivirus programs have traditionally focused on viruses. With the rapid rise of zero-hour malware, antivirus failures have become more prevalent and a layered security approach is encouraged. Malwarebytes was created as a result of one of these failures to specifically focus on new threats that escaped detection by traditional antivirus Layering antivirus or other security measures, such as a firewall, alongside Malwarebytes is recommended.

- Includes layered security.

- Delivers centralized deployment, reports, custom data views and policy management

Second Opinion Security Scanner:

HitmanPro

Today's malware is designed to bypass anti-virus defenses and effectively hide from both security software and the computer user. Anti-virus programs, blacklists and other security software that require prior knowledge of a threat are ineffective against zero-day malware. Our real-world statistics, covering millions of scanned computers, show that one out of three computers has become infected, despite real-time protection from up-to-date anti-virus software.

Anti-Virus Software:

For more than 25 years, ESET development teams have been engineering security solutions that focus on highly effective detection with a low system footprint. As the threat landscape evolves, ESET specialists continually come up with effective tools to fight the increasing volume, diversity and sophistication of malware. And, with the highest number of coveted “Virus Bulletin VB100” awards of any competitor product, ESET consistently outperforms other security providers.

ConnectWise Automate

Encryption:

DESlock+

DESlock+ by ESET, is a FIPS validated, enterprise-quality encryption solution that offers Full Disk Encryption (FDE) and encryption for removable media, files, folder, and email. DESlock+ is lightweight and easy to deploy. Built for companies of all sizes, DESlock+ is easily managed through a centralized remote console that leverages the cloud for all commands, updates, requests, and responses. The client side requires minimal user interaction, increasing user compliance and the security of your customers' data.

Mobile Device Management:

MaaS360 by Fiberlink

IBM MaaS360 is a secure mobility management platform that quickly and seamlessly deploys devices and delivers productivity apps while enabling secure content collaboration on a personal or corporate-owned mobile devices. As a fully integrated cloud platform, IBM MaaS360 is a trusted mobile security solution to thousands of customers worldwide—from Fortune 500 companies to small businesses. This award-winning platform streamlines the way IT professionals manage and secure the proliferation of mobile devices in the workspace throughout their entire lifecycle.

Patch Management:

Computer patches are designed to fix exploits in networks and computers after release. Without patching, these exploits could be abused by hackers to retrieve sensitive data or allow unauthorized control of a computer.

Patches are often categorized by the severity of the exploit they fix. There are a few major patch severity rating systems:

Microsoft Security Update Severity Rating System

Microsoft Severity Levels	Critical*	Important*	Moderate*	Low	Unspecified
Current Patch Compliance	94%	92%	100%	89%	86%
Target Patch Compliance	100%	100%	100%	50%	0%

Common Vulnerability Scoring System

CVSS Patch Priority	High* (10.0-7.0)	Medium* (6.9-4.0)	Low (3.9-0.0)
Current Patch Compliance	99%	99%	87%
Target Patch Compliance	100%	100%	75%

Note: * Asterisk implies the Target Patch Compliance is only acceptable at 100%

ConnectWise Automate

Remote Control:

ConnectWise Control

The ScreenConnect plugin creates seamless integration, enabling configuration, deployment and management from within ConnectWise. With support and access, IT professionals can remote into both managed and unmanaged devices. With remote meetings, they can conduct online seminars and presentations. The self-hosted model, coupled with central web application, provides numerous advantages over competitive products. In addition to cost savings, the centralized tools are easy to setup, deploy and manage.

Third Party Patch Management:

ConnectWise Automate™

ConnectWise's Third Party Patch Management solution extends your patching capabilities beyond Microsoft updates to third party applications such as Adobe Reader, Adobe Flash, Java Runtime, and more. Unpatched applications are highly vulnerable to exploits and malware, which costs your team time to find and remove. Natively built into ConnectWise Automate™ (formerly LabTech), Third Party Patch Management downloads necessary updates for devices and can push patches to computers to close security gaps in third party applications. This allows us to automate the process and schedule patch installation to occur on your terms.

ConnectWise Automate

Additional Features:

- Asset Management and Reporting
- Automatically Restart Devices
- Automatic Disk Cleanup (Windows Devices)
- Compliancy Reporting
- Software Blacklisting
- Software License Management

ConnectWise Automate

Compliancy Reporting:

Network / Security Compliancy:

Antivirus, updates – patching, malwarebytes, ISP network performance, and backup usage.

Hardware Compliancy:

Hard Drive Status, hard drive usage, memory usage, processor usage, processor speed, and computer age.

Software Compliancy:

Operating systems, Microsoft office, email, and domain logins.

Contract Compliancy:

Reports on expiration dates for your current contracts.