ManageEngine

Security Specifications of

Patch Manager Plus

Contents

Abstract

Data confidentiality is much spoken about in the current IT arena. Software vending companies must ensure they make foolproof products that can withstand malicious attacks & comply to IT regulations. These software must be hardened on security against data theft. Security becomes all the more a priority when the software applications access and/or process confidential data in large enterprises. Any compromise on the data can cause serious implications ranging from a temporary outage to a major financial loss. ManageEngine's Patch Manager Plus is a an automated patch management application, with presence on premise and on-demand. It helps maintain the network computers secure while itself is secure on various fronts. This white paper helps you learn the security specifications of Patch Manager Plus for both cloud and on-premise editions.

Security Specifications of Patch Manager Plus

1

Secured communication over HTTPS:

Patch Manager Plus helps in a secured gateway communication, allowing servers and agents to communicate using HTTPS protocol. Since the communication deals with essential corporate data, HTTP must be changed to HTTPS communication. When you choose a secured communication, Patch Manager Plus chooses HTTPS ports over insecure ports. You need to make appropriate changes to your firewall to allow the HTTPS port and disable the other ports. For more ports related security please refer here. Also a local authentication mechanism with SHA 256 algorithm adds to the security.

The Patch Manager Plus console thoroughly validates all inputs in the GUI. Usage of special characters and HTML code are filtered, and the application is guarded against common attacks like SQL injections, cross-site scripting, buffer overflows and other attacks.

A secure HTTPS connection and SSL Certificates help in mitigating attacks (like MITM) byplacing an overcoat of encryption to the data communicated.

2

Secured Socket Layer (SSL) Certificates:

If enterprises feel that communication via HTTPS is not secure enough to transmit data, Patch Manager Plus provides for a certificate based encryption between the machines in network. User can import third party SSL certificates in Patch Manager Plus server which will encrypt all data transferred between client and server. This rules out the possibility of an intercepting attack. Also even if an attacker gains an intermediate access can not crack the encrypted communication. However, the communication may not be secure post expiry of certificates.

3

Securing the ports used for Communication:

A set of ports need to be opened in the computer in which Patch Manager Plus Server is installed. If Windows firewall is being run, then the ports can be opened from Patch Manager Plus console, or if third party firewall (antivirus software) is run they need to be allowed manually. By default only HTTP port is enabled, and this can be disabled from the port settings. 8383 is the default HTTPS port for Agent/Distribution Server and Patch Manager Plus server communication. For a list of all ports used by Patch Manager Plus please refer https://www.manageengine.com/patch-management/lan-architecture.html

It is recommended to configure the firewall settings to disallow the unwated ports when not in use. Patch Manager Plus allows the manual configuration of firewall for target machines in the network.

4

Secure Authentication: Password policy

Patch Manager Plus comes with a complex Password policy that helps overcome security loopholes. This is in addition to Windows Active Directory credentials to ensure that your organization is hack-proof. One can customize the password policy to be more efficient by requiring that passwords incorporate one or more of the following:

- A minimum length
- Both upper and lower cases
- Special characters
- Numbers
- User account lockout for more than a specified number of invalid attempts

In the cloud-based edition, there additional parameters can be configured like:

- Password Expiry period
- Minimum number of special characters and numerals
- Mixed passwords

For more on the best practices, please refer to Zoho's cloud based password policy.

Stricter or more lenient requirements can be worked upon, depending on the environment. Furthermore, you can set the number of complexity requirements the user must adhere to while setting passwords. A strong password policy helps remain secure against brute force attacks. A strong password policy not withstanding Patch Manager Plus allows for a two factor/multi factor authentication.

5

Two factor Authentication:

Two Factor Authentication enables secured access to Patch Manager Plus web console. Apart from the default Patch Manager Plus password, users will have an additional layer of protection via the One Time Password (OTP). This OTP can be received either through email or Google authentication. If this option is enabled, user will not be prompted for OTP for a specified number of days which can be configured by the user himself. User can also choose the mode for two factor authentication, which could be via businessemail or Google Authenticator. In case of e-mail authentication, OTP will be sent via email to only those users mapped with Patch Manager Plus. You can set the browser to remember your OTP for a specified number of days.

6

Multi factor Authentication (only in cloud edition):

Multi factor authentication encompasses two or more of the following authentication modes:

- Touch ID
- Push notification
- Scan QR
- Time-based OTP

For more details on Multi factor authentication, please refer here.

7

AES Encryption for credentials:

Patch Manager Plus requires credentials like user name and password to perform various desktop management activities inside the product,for adding a domain or workgroup, for deploying certain configurations etc., These credentials details are collected at different points, Credential Manager provides a unified solution to store and manage all these credentials globally from a centralized location using AES encryption. Also, the HTTPS communications happen over AES encryption adding to the security hardening of Patch Manager Plus. Every sensitive information is protected using AES encryption.

8

Windows Active Directory Authentication:

Patch Manager Plus on premise's web console is the management interface for exclusive patching activities. If a disgruntled person gets access to this interface, he/she can perform any undesirable activities using Patch Manager Plus. Moreover, with the increase in software applications, each with their own authentication and password complexity levels, it becomes very difficult to remember all the passwords.Patch Manager Plus addresses these problems with Active Directory Authentication, enabling quick user importation. Active Directory's authentication and single sign-on capabilities can be extended to Patch Manager Plus letting users log on with their AD credentials. The database constantly synchronizes with the directory, and is automatically updated whenever users are added or removed in AD. This will greatlyminimize the risk of unauthorized users accessing Patch Manager Plus Web interface. The scope of authorization for users is dealt with in "Role Based administration" head. Similarly it is possible to generate reports for computers in all sites, domains,organizational units, groups of the AD. This helps in auditing purposes.

9

Single Sign-on (SSO) using SAML for Patch Manager Plus Cloud:

SSO has a major role to play in cloud security and saves you from juggling with multiple usernames and passwords of cloud/web applications you use. Security Assertion Markup Language(SAML) is a XML-based, open-standard data format for exchanging authentication and authorization data between an identity provider and a service provider. Simply put, this means you can use a third-party identity provider or create your own identity provider to pass credentials to the service provider in the form of a digitally signed XML document. Hence you have no need to key in the credentials, no need to remember any passwords, ensure a strong password being in place. You can automatically get logged in and start accessing your console. To know more on SAML, please click here.

10

Role-based Administration:

In mid-size and larger networks, it is quite an impossible task for a single person to cover all the aspects of system administration. Patch Manager Plus helps to overcome this concern using its Role Based Administration' module. 'Role Based Control' feature notjust helps the administrator shed his work load but also adds an additional layer of network security by restricting the access of systems to only authorized personnel. Tailor-made roles like Guest, Technician, Auditor, etc. can be created and givencustomized access permissions (read, write, no access, full control) based on needs. Target computers defined for the users can be static unique groups, remote offices or all computers. Also, by defining the scope of computers managed by each user, they can not take unduly advantage of the permission.

11

Roaming users connecting over Security Gateway Server:

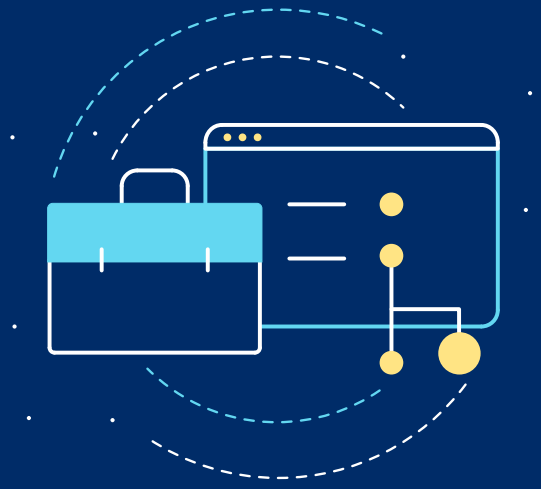
Security Gateway Server helps roaming agents (on the mobile devices and desktops) access the server securely through the HTTPS protocol. It prevents the exposure of Patch Manager Plus Server directly to the internet by serving as an intermediate server between the Patch Manager Plus server and roaming agents. This ensures that the Patch Manager Plus Server is secure from risks and threats of vulnerable attacks. Patch Manager Plus Security Gateway Server is a component that will be exposed to the internet. . All communications from the roaming agents will be navigated through the Security Gateway Server. Thus Security Gateway Server acts a security frontier for remote users' agents and Patch Manager Plus server.

12

Demilitarized network security:

Certain networks are kept totally disconnected from the internet to prevent network breaches, often using a demilitarized zone to isolate the private network from the internet. Patch Manager Plus can patch computers protected by demilitarized zones to ensure they're up-to-date. Since neither the server nor the agents are connected to the internet in a demilitarized network, admins need to adjust their proxy settings before patching with Patch Manager Plus.

When patching computers behind a demilitarized network, Patch Manager Plus uses a download manager tool installed on an internet-enabled machine outside the network to detect and download the missing patches. Once the patch database is updated, the patch database is copied to the Patch Manager Plus server in the closed network. Patch Manager Plus then scans for missing patches in the closed network; once the scan is complete, Patch Manager Plus exports the missing patch report to the machine connected to the internet and downloads the patches. The downloaded patches are finally copied to the specified path in the Patch Manager Plus server and pushed to the agents. Additional information about patching demilitarized networks can be found here.



13 Business Continuity Planning:

Patch Manager Plus allows enterprises to strategize for 'Business Continuity and Risk management' by providing uninterrupted patching solution even during an unforced downtime. This is made possible by a Fail over server being in place (only in case of on-premise edition)

Whenever a downtime is endured due to unforeseen circumstances, the agent's communication with Patch Manager Plus Server is locked down. This downtime can become a gateway to cyber attacks and your network may experience a breach. Resolving downtimes is a humongous task to IT department, as this can reduce enterprise productivity and also make your network vulnerable. To prevent this a Patch Manager Plus offers a 'Fail over server' which acts as the backup server for Patch Manager Plus server. Once downtime is endured, this backup server establishes connection through a pre-configured virtual IP address (available in the same network as primary server).

Patch Manager Plus provides for high availability by virtue of native mobile applications on iOS and Android platforms allowing maintenance on the go. The mobile apps also use a secure HTTPS connection.

Access can be granted or revoked for querying the database stored in the server from a remote computer, reducing the time lags in reporting. However, this feature is restricted to just reporting and disallows undesirable modifications to the database protecting the original data. If the server endures a hardware failure, there is provision for migrating server to a different machine without loss of data to keep the normal functioning intact. Similarly databases comprising of confidential data pertaining to the customers can be backed up and restored seamlessly

14

Compliance to cloud so ware's privacy policy

ManageEngine is a division of Zoho corp. Patch Manager Plus Cloud, being an offering of ManageEngine conforms to Privacy policies for Cloud software laid down by Zoho corp.

Data security is offered on multiple levels including the physical, software and people/process levels.

Physical: Patch Manager Plus Cloud's servers and infrastructure are located in the most secure types of data centers that have multiple levels of restrictions for access including: on-premise security guards, security cameras, biometric limited access systems, and no signage to indicate where the buildings are, bullet proof glass, earthquake ratings, etc.

Hardware: Patch Manager Plus Cloud employs state of the art firewall protection on multiple levels eliminating the possibility of intrusion from outside attacks Logical/software protection: Zoho deploys anti-virus software and scans all access 24 x7 for suspicious traffic and viruses or even inside attacks. All of this is managed and logged for auditing purposes.

Process: Very few staff have access to either the physical or logical levels of our infrastructure. Enterprise data is therefore secure from inside access; further regular vulnerability testing is performed and security is constantly enhanced at all levels. All data is backed up on multiple servers in multiple locations on a daily basis. This means that in the worst case, if one data center was compromised, your data could be restored from other locations with minimal disruption.

Zoho's privacy policy states that "the contents of your account will not be disclosed to anyone and will not be accessible to even employees of Zoho. Neither do we process the contents of your account for serving targeted advertisements." In addition, when payment is made by credit card for cloud based services, the card details are not stored by us, but is securely passed to the credit card companies and in use for that single transaction. Users can also access their personal information to make changes and remove themselves from the system". Both Zoho and ManageEngine ensure that the privacy of users' data and confidential corporate data are not compromised at any cost.

ManageEngine

Patch Manager Plus

Patch Manager Plus is an integrated and automated patching software that helps patch computers across platforms. It is a network-neutral solution that can be used to patch computers in Active Directory, Workgroups and Novell eDirectory. Patch Manager Plus helps secure the computers from vulnerabilities by applying automated patches of Windows, Mac and Linux as well as 250-plus third party applications. It can patch computers in multiple domains, workgroups and can also remotely patch computers across WAN (branch offices and users on travel). Patch Manager Plus is an easy-to-deploy, easy-to-use automated patching software allowing management from a single console. Patch Manager Plus is available both on-premise and on-demand(only for Windows).

Patch Manager is available
for immediate download/signup from:
https://patch.manageengine.com/free-trial.html

ManageEngine

ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need — more than 90 products and free tools — to manage all of your IT operations, from networks and servers to applications, service desk, Active Directory, security, desktops, and mobile devices.

Since 2003, IT teams like yours have turned to us for affordable, feature-rich software that's easy to use. You can find our on-premises and cloud solutions powering the IT of over 180,000 companies around the world, including three of every five Fortune 500 companies.

As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers. And as a division of Zoho Corporation, we'll continue pushing for the tight business-IT alignment you'll need to seize opportunities in the future.

www.manageengine.com