

An automated method for at least attempting to update software in a system having a first target computer in a non-update state connected across a network to an update server in a pre-update state, the system also having a package computer which is inaccessible to the first target computer but accessible to the update server, and a repository component accessible to the first target computer and the update server, the method comprising the steps of:

## Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (**ConfigMgr** and **Intune**) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**

Patch My PC is an application that automates updating software in a system.

Users have target computers (including mobile devices) that are in a pre-update state. Patch My PC has update servers that connect to the target computers through Agents. Agents used are part of Microsoft Endpoint Manager either System Center Configuration Manager for computers or Intune for mobile devices both of which are Agents.

Through use of its servers, PatchMyPC attempts and performs updates to software of devices that are in a non-update state from a server accessible by Patch My PC but not the target device. These servers are PatchMyPC's package computers.

Client machines scan using Microsoft Endpoint Manager's agents or Intune agents and the target computer or mobile device doing the scan is then in a non-update state. The user is in communication with the PatchMyPC servers (the update server) and the update server is in communication with one or more package computers that contain the actual updates identified as relevant to the target computer or mobile device through the agent scan and processing of the update server.

<sup>1</sup> Notes are provided as a **courtesy only** and for settlement purposes only subject to Federal Rule of Evidence 408 and any applicable state equivalent. Notes are not intended to be exhaustive nor indicate specific support for any claim element, nor is support for any claim element limited to that indicated in the Notes. Moreover, nothing in the Notes shall constitute an admission of any kind with respect to, or have any other legal bearing on the scope and breadth of, the claims. Nothing herein should be regarded as the provision of legal counsel, and recipients are welcome and encouraged to consult with qualified legal counsel regarding claim interpretation matters. For purposes of complete clarity, nothing herein is intended narrow or otherwise limit the scope or breadth of the claims as issued.

[Type here]

US 6,990,660 Claim 1	Patch My PC	Notes <sup>1</sup>
-------------------------	-------------	--------------------

(a) putting at least one patch fingerprint which defines a specific software update into the repository component, the patch fingerprint comprising:

a patch signature and an existence test, wherein the patch signature is ~~used~~ configured to request target computer information from the first target computer, and

wherein the existence test is configured to request target computer information provided via the patch signature to determine whether the specific software update is needed on the first target computer;

wherein the repository component is at least located at the update server and includes recommended configuration information for the first target computer

## Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (**ConfigMgr** and **Intune**) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**

Patch Fingerprints consist of a combination of Patch Signatures and Existence Tests. Both InTune (for mobile devices) and SCCM or Endpoint Manager (for computers) have software that over time requires updates including application software.

Patch My PC using either InTune or SCCM/Endpoint Manager scans devices to determine if software patches are applicable to a device and if that patch has already been installed or not. The first element of the fingerprint, the signature, determines if a potential update is applicable to a particular instance of software/hardware and therefore applicable to a device or its installed software. The second element, the existence test, is if that update has already been installed or not.

The repository component contains the recommended configuration information for the target computer. This includes what version and/or update of applications or drivers or other any other software on the target computer/device.

Patching and application management by scanning and determining whether a specific software update is needed on a particular device that has been scanned includes both the steps of applying a patch signature and an existence test to determine what updates are applicable to a program or device and if that update has already been performed or not.

[Type here]

[Type here]

US 6,990,660 Claim 1	Patch My PC	Notes <sup>1</sup>
-------------------------	-------------	--------------------

b) gathering the target computer information about the first target computer and sending the information back to the repository component] via a discovery agent located on the first target computer; wherein the discovery agent utilizes the patch signature to gather the target computer information; wherein the target computer information includes at least hardware configuration information, registry information, software presence information, and software version information relative to the first target computer; wherein the target computer information defines current configuration information of the first target computer;

(c) sending the target computer information back to the repository component located on the update server;

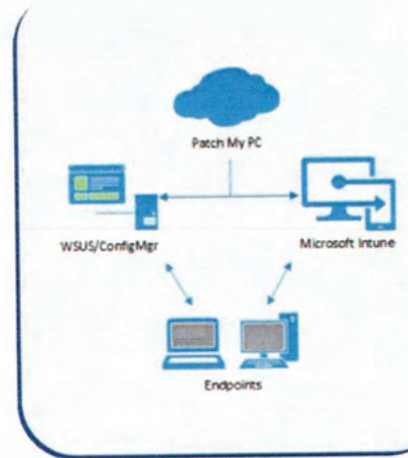
(d) storing the target computer information in the repository component located on the update server;

## Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (ConfigMgr and Intune) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**



## Product Features



### Automate Third-Party Updates

- Third-party updates automatically published to SCCM and Intune
- Use existing processes to deploy updates, including ADR's
- Report on non-compliance for third-party updates in the same way as Microsoft updates
- Automatically scan your SCCM or Intune inventory to auto-enable product for publishing
- Our application feature allows you to rollback third-party updates if needed
- Third-party updates typically released the same day as the vendor makes it available



### Automatically Create Applications

- Create base applications for SCCM and Intune
- Eliminate manual packaging of applications
- Auto-update applications to the latest version
- Ensure new machines always receive the most secure version of an application
- Use existing deployment mechanisms: task sequences, collections, or Intune assignments
- Applications include vendor icons, descriptions, and keywords

Target computer information is gathered by a discovery agent. PatchMyPc uses Endpoint Manager (previously known as System Center Configuration Manager or SCCM) or Intune. Both Endpoint Manager and Intune include agents that collect configuration data from Microsoft operating system devices. Intune is used with Windows Mobile devices and Endpoint Manager (or SCCM) for Windows PC and Server devices.

SCCM and Intune are discovery agents both use patch signatures to gather information about the system subject to being updated and existence tests to determine if the patch has already been installed or not. Both return all of the listed data to ensure a patch can be successfully installed and is needed. Discovery agents are also used to determine the hardware and software that is installed in the system and this target computer information is also provided to the repository component.

This information then defines the current configuration of the target computer.

[Type here]

[Type here]

US 6,990,660  
Claim 1

Patch My PC

Notes<sup>1</sup>

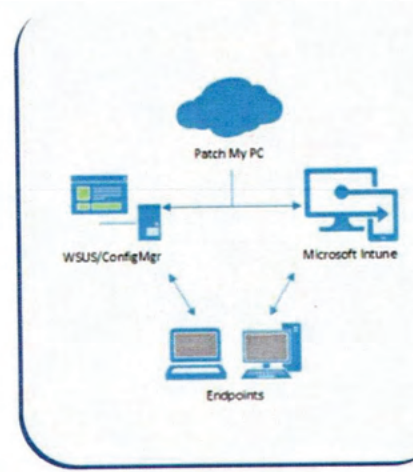
(e) comparing, at the update server, at least a portion of the gathered target computer information with the patch fingerprint using the existence test to determine whether the recommended configuration information of the first target computer matches the current configuration information of the first target computer and to determine whether the specific software update is absent from the first target computer and whether the specific software update has a dependency on at least one of another specific software update, a specific software, and a specific hardware [and if the specific software update is absent from the first target computer];

### Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (ConfigMgr and Intune) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**



Patch My PC claims to identify on average more than 1,300 updates that are needed and Patch My PC released 2,915 third-party updates in 2020. Identification of needed updates is accomplished by comparing gathered target computer information using the patch fingerprints using the existence test to determine whether the recommended configuration of the device matches the current configuration of the device and whether specific software updates are missing. And, whether one update is dependent upon another update or a specific hardware configuration.

### Product Features

#### Automate Third-Party Updates

- Third-party updates automatically published to SCCM and Intune
- Use existing processes to deploy updates, including ADR's
- Report on non-compliance for third-party updates in the same way as Microsoft updates
- Automatically scan your SCCM or Intune inventory to auto-enable product for publishing
- Our application feature allows you to rollback third-party updates if needed
- Third-party updates typically released the same day as the vendor makes it available

#### Automatically Create Applications

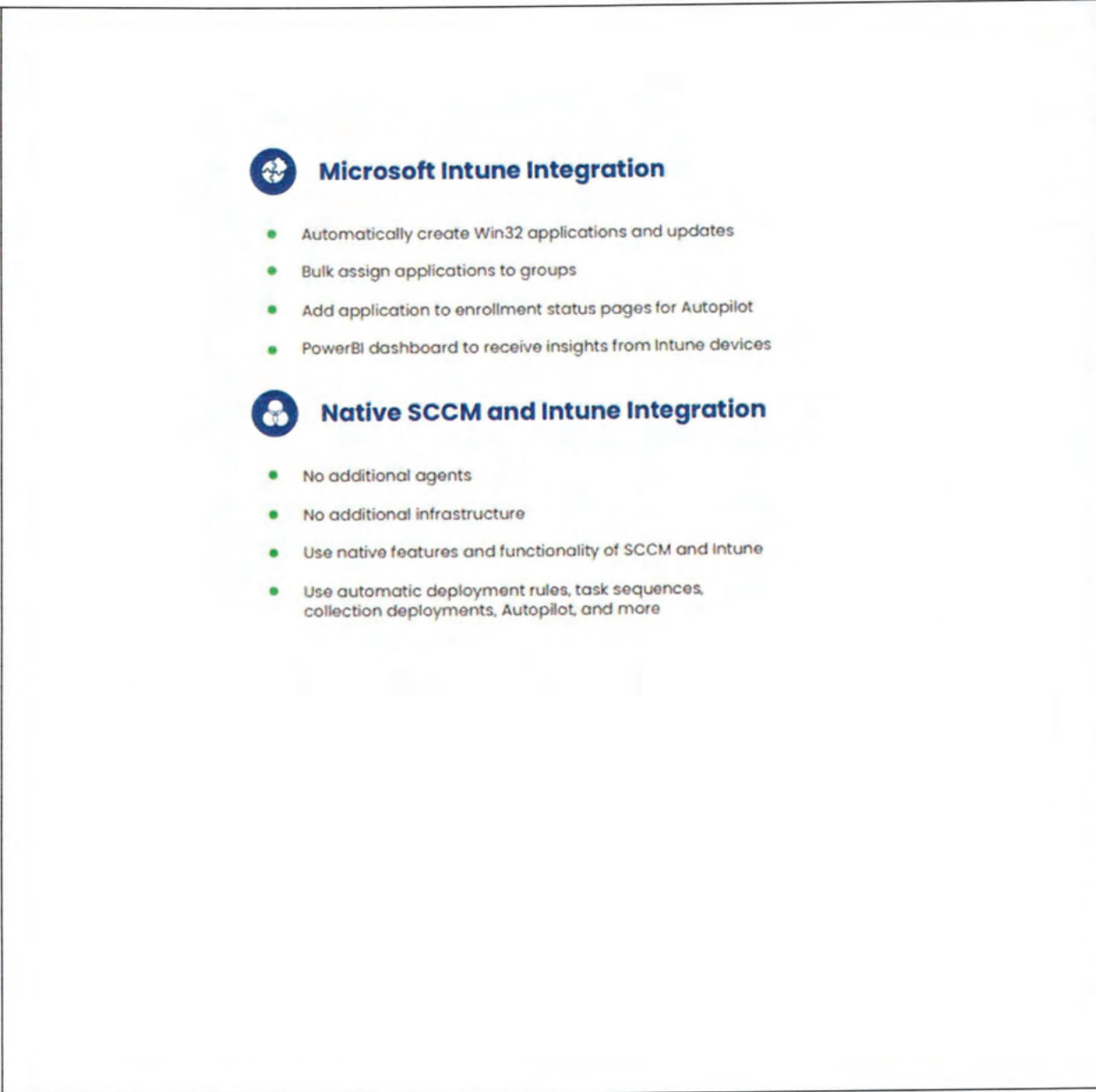
- Create base applications for SCCM and Intune
- Eliminate manual packaging of applications
- Auto-update applications to the latest version
- Ensure new machines always receive the most secure version of an application
- Use existing deployment mechanisms: task sequences, collections, or Intune assignments
- Applications include vendor icons, descriptions, and keywords

[Type here]

[Type here]

<b>US 6,990,660 Claim 1</b>	<b>Patch My PC</b>	<b>Notes<sup>1</sup></b>
---------------------------------	--------------------	--------------------------

(f) if a known condition is met, then placing at least one task identifier on an update task list, the task identifier specifying the first target computer, the update task list stored at the update server, the task identifier also specifying at least one download address which references a location on the package computer that contains a software update for the first target computer;



**Microsoft Intune Integration**

- Automatically create Win32 applications and updates
- Bulk assign applications to groups
- Add application to enrollment status pages for Autopilot
- PowerBI dashboard to receive insights from Intune devices

**Native SCCM and Intune Integration**

- No additional agents
- No additional infrastructure
- Use native features and functionality of SCCM and Intune
- Use automatic deployment rules, task sequences, collection deployments, Autopilot, and more

If a known condition requiring an update is determined to exist, tasks are created to automatically update the target computer and the task identifier specifies the location from which to download the software update for the target computer. This can be seen in Automatically creating updates in Intune and use of automatic deployment rules, task sequences, collection deployments, and more in SCCM/Endpoint Manager.

[Type here]

[Type here]

<b>US 6,990,660 Claim 1</b>	<b>Patch My PC</b>	<b>Notes<sup>1</sup></b>
---------------------------------	--------------------	--------------------------

(g) starting a task in response to the task identifier, the task attempting a first download of the *specific* software update from the package computer to the update server;



### Microsoft Intune Integration

- Automatically create Win32 applications and updates
- Bulk assign applications to groups
- Add application to enrollment status pages for Autopilot
- PowerBI dashboard to receive insights from Intune devices



### Native SCCM and Intune Integration

- No additional agents
- No additional infrastructure
- Use native features and functionality of SCCM and Intune
- Use automatic deployment rules, task sequences, collection deployments, Autopilot, and more

Tasks are started to download specific updates from the package computer to the update server in support of automatically creating updates and deploying updates to mobile devices and computers. This uses native features and functionality of SCCM/Endpoint Manager and Intune to use automatic deployment.

[Type here]

[Type here]

US 6,990,660 Claim 1	Patch My PC	Notes <sup>1</sup>
<p>(h) if the first download completes successfully, then attempting a second download of the <i>specific</i> software update from the update server to the first target computer, <i>wherein during the attempting a second download step, the first target computer is inaccessible to the package computer via a firewall</i>; and</p> <p>(i) monitoring the attempted downloads for an outcome.</p>	<div data-bbox="619 357 672 406"></div> <h3 data-bbox="693 365 1092 397">Microsoft Intune Integration</h3> <ul data-bbox="630 438 1207 592" style="list-style-type: none"><li>● Automatically create Win32 applications and updates</li><li>● Bulk assign applications to groups</li><li>● Add application to enrollment status pages for Autopilot</li><li>● PowerBI dashboard to receive insights from Intune devices</li></ul> <div data-bbox="619 633 672 682"></div> <h3 data-bbox="693 641 1197 673">Native SCCM and Intune Integration</h3> <ul data-bbox="630 714 1197 885" style="list-style-type: none"><li>● No additional agents</li><li>● No additional infrastructure</li><li>● Use native features and functionality of SCCM and Intune</li><li>● Use automatic deployment rules, task sequences, collection deployments, Autopilot, and more</li></ul>	

[Type here]

[Type here]

US 6,990,660 Claim 1	Patch My PC	Notes <sup>1</sup>
-------------------------	-------------	--------------------

#### NOTES<sup>1</sup>

Note on claim language: Claim language in *italics* was added to the claims during an ex-parte re-examination published as Certificate number US 6,990,660 C2 issued August 3, 2010 with the additions and deletions as shown in this chart. Claim language with ~~strike throughs~~ was removed from the claims and no longer form part of the patent's claims. Claim language in italics was added and form part of the patent's claims as shown. The deletions and additions are provided for context, clarity, and full disclosure.

Claim Language references to Specification: Citations to the specification for certain terms identified below are provided solely for convenience. The provision of these references in no way waives any argument that the claims have any meaning other than their plain and ordinary meaning to one of ordinary skill in the art in light of the specification. These citations are only provided to direct the reader to those portions of the specification for your information.

#### TARGET COMPUTER:

Any computer (for instance an end-user computer or a network server) that has its software updates managed by an Update Server where typically many Target Computers are managed and provided updates by a single Update Server. See Figures 5, 6 and 7. Co 4 Lines 4-6, Col 8 Lines 28:33, Col 8 lines 59:62 Col 9 Lines 7:19, Col 10 Lines 4:6, Lines 14-17, Lines 27:29, Lines 57:63, Col 12 Lines 17-21, Lines 33-40, Col 11 Line 66 - Col 12 line 2, Col 12 Lines 17:21, Col 12 Lines 33:40, Col 12 Line 65 - Col 13 Line 2, Col 13 Line 3:6, Col 13 Line 14:17, Col 14 Line 9:20, Col 14 41:47, Col 14 Lines 58:62, Col 14 Line 65 - Col 15 Line 1, Col 15 Lines 6:14, Col 15 Lines 23:27, Col 16 Lines 30:49, Col 16 Lines 57-65, Col 17 Lines 2-4, Col 17 Lines 12:20, Col 17 Lines 21:26, Col 17 Lines 31:33, Col 17 Lines 50-52, Col 18 Lines 32:39, Col 18 Lines 57:63, Col 18 Line 66:Col 19 Line 4, Col 20 Lines 10:12, Col 20 Lines 16:19, Col 20 Lines 54:61, Col 21 Lines 63:66

REPOSITORY COMPONENT: A database that contains a variety of information about managed devices (including but not limited to Patch Fingerprints) that is used for various purposes in determining if a particular Target Computer needs a particular software update given information that is obtained from the Target Computer by use of the Patch Fingerprint(s). It may also encompass a database of locally stored patches and their may be one or many repository component locations not all of which have to have all of the different types of information. Some may have patch fingerprints and other similar information, others may have stored copies of patches. The Repository Component is the component in communication with installed Agents. Col 3 Lines 56-57, 63-66, Col 4 Lines 8-10, Col 12 Lines 44-48, 55-61, Col 13 Lines 17-20, 26-31, 47-49, 49-51, 62-65, Col 13 Line 67- Col 14 Line 3, Col 14 Lines 9-10, 41-47, Col 15 Lines 18-20, Col 15 Line 66 – Col 16 Line 3, Col 16 Lines 29-30, 44-47.

#### UPDATE STATE. PRE-UPDATE STATE NON-UPDATE STATE:

Col 3 Lines 29-31, Col 8 Lines 16-26, Col 8 Lines 28:33 FIGS 3, 4, 5, 5-500, Col 10 Lines 46:53 Lines 30:39

#### UPDATE SERVER

Fig 2-220 Fig 5-528, Col 3 Lines 37:40, 49:51, Col 4 Lines 18:20, 30:31, 39:54, Col 5 Lines 2:5, Col 8 Lines 33:35, 37:40, Col 9 Lines 7:8, 14:19. 20:23, 36:39, 52:54, 62: Col 10 :6, Col 10 Lines 8:10, 11:14, 26:29, Col 11 Line 66:Col 12 Line 4, Col 12 Lines 17-26, 49-54, Col 13 Lines 49:50, Col 14 Lines 10-13, Col 15 Lines 39-41, 44-46, Col 16 Lines 59-60, 65-67 Col 17 Lines 4:11, 16:20, 25:29, 30:34, 45:52, 57:59, 63:67 Col 18 Lines 1:3, 9:14, 14:16, 17:21, 21:26, 27:31, 32:33, 33:39, 41:43, 59:63, Col 18 Line 66:Col 19 4, Col 19 Lines 54:57, Col 20 Lines 10:12, 43:45, 45:47, 47:52, 58:61 Col 21 Lines 55:56 Col 24 Lines 13:15, 38:39

#### PACKAGE COMPUTER

FIGURES 2,3,5 Col 3 Lines 44:48, Col 4 Lines 41:48, Col 9 Lines 20:23, 52:57, 62:64, Col 10 Lines 1:4, 12:14, Col 12 Lines 49:54, Col 16 Lines 58:60, Col 17 Lines 1:11, 53:57, 60:65

[Type here]



[Type here]

<b>US 6,990,660 Claim 1</b>	<b>Patch My PC</b>	<b>Notes<sup>1</sup></b>
---------------------------------	--------------------	--------------------------

**PATCH FINGERPRINTS**

FIGURES 8, 9 Col 3 Lines 56:59, Col 3 Line 66 - Col 4 Line 3, Col 4 Lines 10:14, 15:18, 23:25, Col 12 Lines 41 - Col 13 Line 2, Col 13 Line 38 - Col 14 Line 7, Col 14 Lines 56:58, Col 14 Line 63 : Col 15 Line 5, Col 15 Lines 6:21, 22:32, 33:38, Col 16 Lines 13:20, 21:26, 27:30, 44:47, Col 31 Lines 25:35

**EXISTENCE TEST**

FIGURE 9 Col 12 Line 65 - Col 13 Line 2, Lines 26:32, Col 15 Lines 22:32 Col 15 Line 63 : Col 16 Line 3, Col 16 Lines 6:12

**DISCOVERY AGENT**

Figure 5, Col 4 Lines 4:8, 10:14, Col 13 Lines 14:25, Col 14 Lines 10:20, Col 15 Line 6:21, Col 15 Line 63 : Line 66, Col 20 Lines 1:5, 16:19, Col 30 Line 52 : Col 31 Line 12

[Type here]

A system comprising:

(a) a package computer having a plurality of patch fingerprints;

(i) wherein the plurality of patch fingerprints includes at least a first patch fingerprint and a second patch fingerprint, different than the first patch fingerprint;

(i) wherein at least the first and second patch fingerprints each comprises at least one Extensible Markup Language (XML) metadata query,

wherein the first patch fingerprint includes a first XML metadata query, and

wherein the second patch fingerprint includes a second XML metadata query, different than the first XML metadata query;

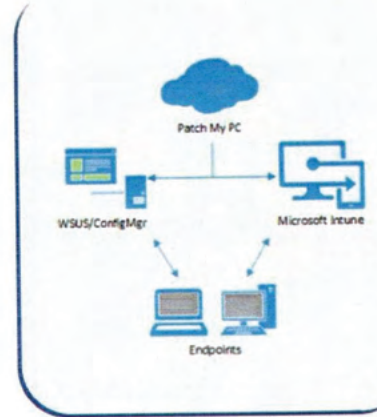
(ii) wherein at least the first and second patch fingerprints are both associated with a specific software update;

## Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (**ConfigMgr** and **Intune**) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**



## Product Features

### Automate Third-Party Updates

- Third-party updates automatically published to SCCM and Intune
- Use existing processes to deploy updates, including ADR's
- Report on non-compliance for third-party updates in the same way as Microsoft updates
- Automatically scan your SCCM or Intune inventory to auto-enable product for publishing
- Our application feature allows you to rollback third-party updates if needed
- Third-party updates typically released the same day as the vendor makes it available

### Automatically Create Applications

- Create base applications for SCCM and Intune
- Eliminate manual packaging of applications
- Auto-update applications to the latest version
- Ensure new machines always receive the most secure version of an application
- Use existing deployment mechanisms: task sequences, collections, or Intune assignments
- Applications include vendor icons, descriptions, and keywords

<https://patchmypc.com/freeupdater/definitions/definitions.xml>

Located at the cloud image in the diagram, PatchMyPC has its package computers/servers which have a plurality of patch fingerprints. As noted in the text in 2020 PatchMyPC released 1329 new updates and applications each of which would have at least one patch fingerprint

Patch Fingerprints consist of a patch signature and an existence test. The patch signature is designed to extract information about the specific computer being updated which includes both the identity and existence of specific hardware, registry, and software version information. Because there can be several different combinations of these items that all apply to the same patch, there will be a first and a second patch fingerprint that apply to the same patch but have different XML metadata queries. Hence the first and second (and perhaps more) metadata queries that are both associated with a specific software update. For instance, a particular application may require certain types of graphics hardware or processor hardware or versions of other software. Therefore, there would be multiple metadata queries to determine if at least one of the required combinations is present that satisfies the requirement of the specific software update. The graphic states "Automatically scan you SCCM or Intune inventory to auto-enable product for publishing" meaning that all of the combinations of hardware and software needed to support a particular patch would be subject to the patch fingerprints that determine if a required hardware/software combination is present in the device to be updated. The hyperlink provided is not intended to show the communications of fingerprints and existence test but shows that communication with device uses XML format.

<sup>1</sup> Notes are provided as a **courtesy only** and for settlement purposes only subject to Federal Rule of Evidence 408 and any applicable state equivalent. Notes are not intended to be exhaustive nor indicate specific support for any claim element, nor is support for any claim element limited to that indicated in the Notes. Moreover, nothing in the Notes shall constitute an admission of any kind with respect to, or have any other legal bearing on the scope and breadth of, the claims. Nothing herein should be regarded as the provision of legal counsel, and recipients are welcome and encouraged to consult with qualified legal counsel regarding claim interpretation matters. For purposes of complete clarity, nothing herein is intended narrow or otherwise limit the scope or breadth of the claims as issued. In addition, to the extent JSON is used as a language for querying device agents or supplying device agents with data, JSON is a well-known equivalent to XML and performs the same function in the same way with the same results and therefore would satisfy the Doctrine of Equivalents test.

[Type here]

<p><b>US 7,823,147 Claim 1</b></p>	<p><b>Patch My PC</b></p>	<p><b>Notes<sup>1</sup></b></p>
--	---------------------------	---------------------------------

(b) an update server in communication with the package computer;

(i) wherein the update server stores at least the first and second patch fingerprints of the package computer;

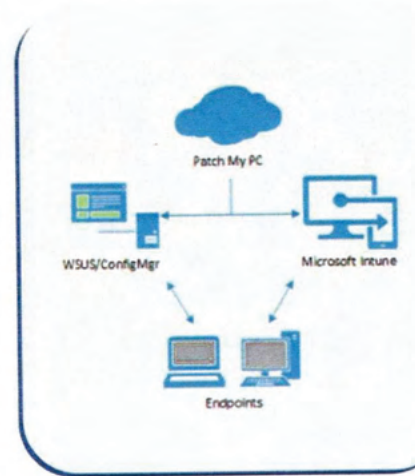
(ii) wherein the update server is located remote from the package computer; and

## Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (ConfigMgr and Intune) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**



## Product Features

### Automate Third-Party Updates

- Third-party updates automatically published to SCCM and Intune
- Use existing processes to deploy updates, including ADR's
- Report on non-compliance for third-party updates in the same way as Microsoft updates
- Automatically scan your SCCM or Intune inventory to auto-enable product for publishing
- Our application feature allows you to rollback third-party updates if needed
- Third-party updates typically released the same day as the vendor makes it available

### Automatically Create Applications

- Create base applications for SCCM and Intune
- Eliminate manual packaging of applications
- Auto-update applications to the latest version
- Ensure new machines always receive the most secure version of an application
- Use existing deployment mechanisms: task sequences, collections, or Intune assignments
- Applications include vendor icons, descriptions, and keywords

In the graphic, the Patch My PC cloud is where the update server(s) reside along with the package computer. Under the heading "Automate Third-Party Updates" it discloses that updates that must come from a third party (the third party's server is the package server for those updates) Patch My PC's update server communicates with the package computer of the third party to deliver the patch to the Endpoint device.

The update server (the Patch My PC cloud) communicates with the package computer (either its own package computer or a third-party package computer)

On information and belief, even the Patch My PC update servers that communicate with the agents (Intune or ConfigMgr in the graphic) are separate from the Patch My PC package computers to more effectively manage bandwidth and response to Endpoints by the update server.

[Type here]

[Type here]

US 7,823,147 Claim 1	Patch My PC	Notes <sup>1</sup>
-------------------------	-------------	--------------------

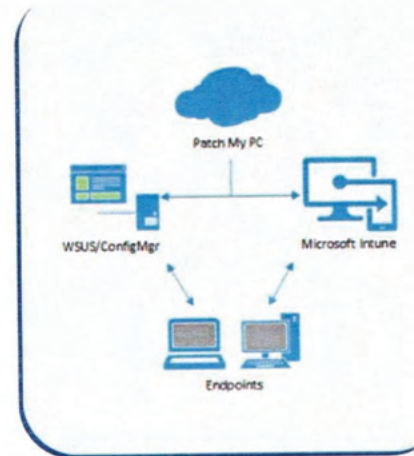
c) a discovery agent configured to separately interact with both the first XML metadata query and the second XML metadata query to produce first target computer information relating to the first target computer;

## Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (**ConfigMgr** and **Intune**) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**



The Endpoints have either Intune or ConfigMgr installed on the endpoint that are agents that then communicate with both the update server and the endpoint managed device. Every XML metadata query is separate and distinct from every other metadata query (each having their own Patch Signature and Existence test, together a Patch Fingerprint).

## Product Features

### **C** Automate Third-Party Updates

- Third-party updates automatically published to SCCM and Intune
- Use existing processes to deploy updates, including ADR's
- Report on non-compliance for third-party updates in the same way as Microsoft updates
- Automatically scan your SCCM or Intune inventory to auto-enable product for publishing
- Our application feature allows you to rollback third-party updates if needed
- Third-party updates typically released the same day as the vendor makes it available

### **W** Automatically Create Applications

- Create base applications for SCCM and Intune
- Eliminate manual packaging of applications
- Auto-update applications to the latest version
- Ensure new machines always receive the most secure version of an application
- Use existing deployment mechanisms: task sequences, collections, or Intune assignments
- Applications include vendor icons, descriptions, and keywords

[Type here]

[Type here]

**US 7,823,147  
Claim 1**

**Patch My PC**

**Notes<sup>1</sup>**

wherein the system is configured to:

(A) send the first XML metadata query and the second XML metadata query of the first and second patch fingerprints from the update server to the discovery agent to gather the first target computer information;

(I) wherein the first target computer information is related to at least registry information, software presence information, and software version information relative to the first target computer;

(II) wherein a first portion of the first target computer information is associated with the first patch fingerprint and the first XML metadata query;

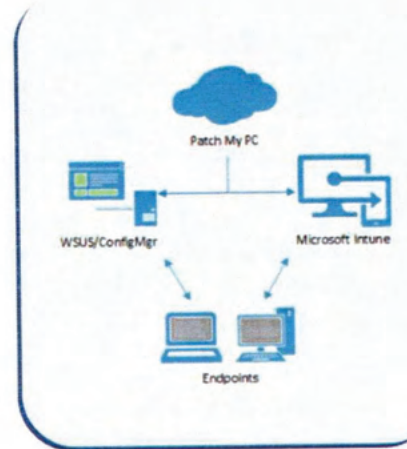
(III) wherein a separate second portion of the first target computer information is associated with the second patch fingerprint and the second XML metadata query;

## Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (**ConfigMgr** and **Intune**) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**



## Product Features

### Automate Third-Party Updates

- Third-party updates automatically published to SCCM and Intune
- Use existing processes to deploy updates, including ADR's
- Report on non-compliance for third-party updates in the same way as Microsoft updates
- Automatically scan your SCCM or Intune inventory to auto-enable product for publishing
- Our application feature allows you to rollback third-party updates if needed
- Third-party updates typically released the same day as the vendor makes it available

### Automatically Create Applications

- Create base applications for SCCM and Intune
- Eliminate manual packaging of applications
- Auto-update applications to the latest version
- Ensure new machines always receive the most secure version of an application
- Use existing deployment mechanisms: task sequences, collections, or Intune assignments
- Applications include vendor icons, descriptions, and keywords

On information and belief, Patch My PC's system is configured to send alternative patch fingerprints for the same potential software update to the discovery agent (Intune or ConfigMgr) when there are acceptable alternative hardware and software combinations for the patch but other hardware or software combinations that are not acceptable. In this case there would be a first XML metadata query to gather target computer information and a second (or more) XML metadata query(ies) to gather an alternative set of target computer information each set consisting of registry information, software presence information, and software version information. Multiple queries for the same update may be sent (only one needs to be satisfactory) when there are multiple acceptable configurations of certain specifications but not all configurations are acceptable. To determine this multiple XML metadata queries may be used to discover if an update can or should be performed or not.

[Type here]

[Type here]

US 7,823,147  
Claim 1

Patch My PC

Notes<sup>1</sup>

(B) determine, at the update server based on the first target computer information, whether the specific software update is both applicable to and absent from the first target computer;

(I) wherein the determination step comprises:

(1) evaluating the first portion of the first target computer information to determine the applicability of the specific software update to the first target computer;

and

(2) if the specific software update is applicable to the first target computer, then evaluating the second portion of the first target computer information to determine the presence or absence of:

(a) the applicable files;

(b) the applicable registry keys; and

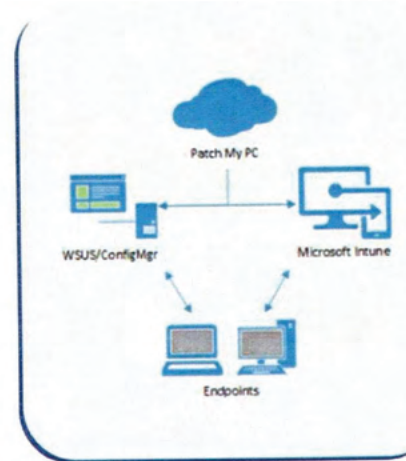
(c) the applicable configuration information of the specific software update;

## Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (ConfigMgr and Intune) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**



## Product Features

### Automate Third-Party Updates

- Third-party updates automatically published to SCCM and Intune
- Use existing processes to deploy updates, including ADR's
- Report on non-compliance for third-party updates in the same way as Microsoft updates
- Automatically scan your SCCM or Intune inventory to auto-enable product for publishing
- Our application feature allows you to rollback third-party updates if needed
- Third-party updates typically released the same day as the vendor makes it available

### Automatically Create Applications

- Create base applications for SCCM and Intune
- Eliminate manual packaging of applications
- Auto-update applications to the latest version
- Ensure new machines always receive the most secure version of an application
- Use existing deployment mechanisms: task sequences, collections, or Intune assignments
- Applications include vendor icons, descriptions, and keywords

On information and belief, the determination of (B) is performed for single, or each of two or more multiple, queries for the same patch until one is found applicable or all have been processed.

Applicability is measured by the absence of the patch from the target computer and the presence of at least one hardware configuration that is required for the patch.

When a specific software update has been found to be applicable Patch My PC uses Intune or SCCM to deploy patches. That happens after the applicability of the patch to the target computer has been established.

[Type here]

[Type here]

US 7,823,147  
Claim 1

## Patch My PC

Notes<sup>1</sup>

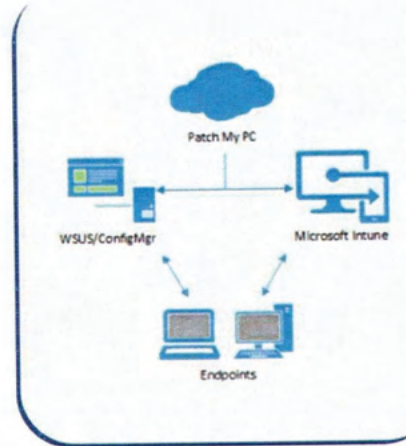
wherein the system is configured to, based on the determination (B), download the specific software update to one of (i) the update server and (ii) the first target computer

### Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (ConfigMgr and Intune) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**



### Product Features



#### Automate Third-Party Updates

- Third-party updates automatically published to SCCM and Intune
- Use existing processes to deploy updates, including ADR's
- Report on non-compliance for third-party updates in the same way as Microsoft updates
- Automatically scan your SCCM or Intune inventory to auto-enable product for publishing
- Our application feature allows you to rollback third-party updates if needed
- Third-party updates typically released the same day as the vendor makes it available



#### Automatically Create Applications

- Create base applications for SCCM and Intune
- Eliminate manual packaging of applications
- Auto-update applications to the latest version
- Ensure new machines always receive the most secure version of an application
- Use existing deployment mechanisms: task sequences, collections, or Intune assignments
- Applications include vendor icons, descriptions, and keywords

Once Patch My PC servers determine that a particular patch can be used and is missing from the target computer, the patch is downloaded to the update server (if the patch resides in the package computer) or to the first target computer if the patch resides on a third-party server (see third-party updates).

[Type here]

[Type here]

<b>US 7,823,147 Claim 1</b>	<b>Patch My PC</b>	<b>Notes<sup>1</sup></b>
---------------------------------	--------------------	--------------------------

Claim Language references to Specification: Citations to the specification for certain terms identified below are provided solely for convenience. The provision of these references in no way waives any argument that the claims have any meaning other than their plain and ordinary meaning to one of ordinary skill in the art in light of the specification. These citations are only provided to direct the reader to those portions of the specification for your information.

US 7,823,147 is a continuation application of US 6,990,660 filed on September 20, 2001 (as amended by ex-parte reexamination Certificate Number US 6,990,660 C1 issued May 12, 2009) and claims priority to US Provisional Application No. 60/234,680 filed on September 22, 2000

**TARGET COMPUTER:**

Figures 2, 3, 5, 6, 7, and 8, Col 3 Lines 44:51, Lines 64:67, Col 4 Lines 1:5, 6:10, 16:19, 30:34, 55:59, 59:66, Col 5 Lines 10:17, Col 8 Lines 26:38, 55:59, 59:67, Col 9 Lines 3:4, 10:12, 13:15, 16:24, 26:32, 33:35 Col 10 Lines 1:3, 4:7, 12:16, 24:29, 33:38, 45:49, 52:55, 56:62, Col 11 Line 65 – Col 12 Line 1, Col 12 Lines 4:11, 16:32, 33:38, 48:54, Col 13 Lines 4:13, 15:18, 21:26, 27:32, 39:43, 49:52, Col 14 Lines 10:14, 14:21, 22:24, 42:48, 60:63 Col 14 Line 66 – Col 15 Line 2, Col 15 Lines 6:10, 10:14, 23:26, 34:38, 39:43, 63:66, Col 16 Lines 30:34, 34:39, 39:40, 42:44, 44:47, Col 16 Line 58 – Col 17 Line 30, Col 17 Lines 33:35, 41:46, 47:54, 55:61 Col 18 Lines 34:39, 42:46, 46:51, 52:56, 57:65, Col 18 Line 66 – Col 19 Line 4, Col 19 Lines 13:17, 49:52, 54:57, Col 20 Lines 1:5, 9:15, 15:18, 27:35, 51:57, Col 21 Lines 56:63

(references to specification of US Patent 6,990,660 which is incorporated by reference) See Figures 5, 6 and 7. Col 4 Lines 4:6, Col 8 Lines 28:33, 59:62 - Col 9 Lines 7:19, Col 10 Lines 4:6, 14:17, 27:29, 57:63, Col 12 Lines 17:21, 33:40, Col 11 Line 66 - Col 12 line 2, Col 12 Lines 17:21, 33:40, Col 12 Line 65 - Col 13 Line 2, Col 13 Line 3:6, 14:17, Col 14 Lines 9:20, 41:47, 58:62, Col 14 Line 65 - Col 15 Line 1, Col 15 Lines 6:14, 23:27, Col 16 Lines 30:49, 57:65, Col 17 Lines 2:4, 12:20, 21:26, 31:33, 50:52, Col 18 Lines 32:39, 57:63, Col 18 Line 66 - Col 19 Line 4, Col 20 Lines 10:12, 16:19, 54:61, Col 21 Lines 63:66

**UPDATE STATE. PRE-UPDATE STATE NON-UPDATE STATE:**

Col 8 Lines 25:27, Col 10 Lines 44:48, 48:51

(references to specification of US Patent 6,990,660 which is incorporated by reference) FIGS 3, 4, 5, 5-500, Col 3 Lines 29:31 Col 8 Lines 16:26, 28:33 Col 10 Lines 46:53, 30:39

**UPDATE SERVER**

Figs. 2, 5 Col. 3 Lines 40:43, 51:54, 61:64, Col. 4 Lines 19:21, 30:34, 39:45, 49:54, Col 5 Lines 2:5, Col 8 Lines 31:32, 35:38, 48:50, Col. 9 Lines 3:15, Col. 9 Line 65 - Col. 10 Line 3, Col 10 Lines 4:7, 9:12, 25:27, Col. 12 Lines 16:21, 21:23, 23:26 49:57, Col. 13 Lines 49:52, Col. 14 Lines 9:14, Col. 15 Lines 39:41, 44:46, Col 16 Lines 59:61, Col 16 Line 66 - Col 17 Line 1, Lines 5:7, 7:12, 17:21, 33:35, 47:54, 59:61, Col. 17 Line 62- Col. 18 Line 5, Lines 6:9, 11:18, 19:32, 33:41, 42:44, Col. 18 Line 66 - Col. 19 Line 4, Lines 49:57, 57:67, Col. 20 Lines 9:11, 38:50, 51:57, Col. 31 Lines 14:19

(references to specification of US Patent 6,990,660 which is incorporated by reference) Fig 2-220 Fig 5-528, Col 3 Lines 37:40, 49:51, Col 4 Lines 18:20, 30:31, 39:54, Col 5 Lines 2:5, Col 8 Lines 33:35, 37:40, Col 9 Lines 7:8, 14:19, 20:23, 36:39, 52:54, 62 - Col 10 Line 6, Col 10 Lines 8:10, 11:14, 26:29, Col 11 Line 66 - Col 12 Line 4, Col 12 Lines 17:26, 49:54, Col 13 Lines 49:50, Col 14 Lines 10:13, Col 15 Lines 39:41, 44:46, Col 16 Lines 59:60, 65:67 Col 17 Lines 4:11, 16:20, 25:29, 30:34, 45:52, 57:59, 63:67 Col 18 Lines 1:3, 9:14, 14:16, 17:21, 21:26, 27:31, 32:33, 33:39, 41:43, 59:63, Col 18 Line 66 - Col 19 Line 4, Col 19 Lines 54:57, Col 20 Lines 10:12, 43:45, 45:47, 47:52, 58:61 Col 21 Lines 55:56 Col 24 Lines 13:15, 38:39

[Type here]



[Type here]

<b>US 7,823,147 Claim 1</b>	<b>Patch My PC</b>	<b>Notes<sup>1</sup></b>
---------------------------------	--------------------	--------------------------

**PACKAGE COMPUTER**

Figures 2, 3, 5

Col 3 Lines 47:51, Col 4 Lines 39:46, Col 9 Lines 16:19, 49: 58, Col 9 Line 65: Col 10 Line 1, Col 10 Lines 9:12, Col 12 Lines 48:54, Col 16 Lines 59:61, Col 17 Lines 1:12, Col 17 Lines 55:61, 62:67, Col 18 Lines 6:9,

(references to the specification of US Patent 6,990,660 which is incorporated by reference) FIGURES 2,3,5 Col 3 Lines 44:48, Col 4 Lines 41:48, Col 9 Lines 20:23, 52:57, 62:64, Col 10 Lines 1:4, 12:14, Col 12 Lines 49:54, Col 16 Lines 58:60, Col 17 Lines 1:11, 53:57, 60:65

**PATCH FINGERPRINTS**

Figures 8, 9, Col 3 Lines 36:43, 58:67, Col 4 Lines 1:5, 12:15, 16:19, 24:29 Col 12 Lines 41:62, Col 12 Line 63: Col 13 Line 3, Col 13 Line 39: Col 14 Line 7, Col 14 Lines 42:49, 58-60, Col 14 Line 64 : Col 15 Line 5, Col 15 Lines 6:21, 22:32, 33:36, 39:62. Col 16 Lines 13:20, 21:26, 27:30, 42:49, Col 30 Lines 50: Col 31 Line 2,

(references to specification of US Patent 6,990,660 which is incorporated by reference) FIGURES 8, 9 Col 3 Lines 56:59, Col 3 Line 66 - Col 4 Line 3, Col 4 Lines 10:14, 15:18, 23:25, Col 12 Lines 41: Col 13 Line 2, Col 13 Line 38: Col 14 Line 7, Col 14 Lines 56:58, Col 14 Line 63: Col 15 Line 5, Col 15 Lines 6:21, 22:32, 33:38, Col 16 Lines 13:20, 21:26, 27:30, 44-47, Col 31 Lines 25:35

**EXISTENCE TEST**

Figure 9, Col 12 Line 63: Col 13 Line 3, Lines 27:32, Col 15 Lines 14:21, 22:23, 63:66, Col 16 Lines 6:12, Col 20 Lines 1:8,

(references to specification of US Patent 6,990,660 which is incorporated by reference) FIGURE 9 Col 12 Line 65: Col 13 Line 2, Lines 26:32, Col 15 Lines 22:32 Col 15 Line 63: Col 16 Line 3, Col 16 Lines 6:12

**DISCOVERY AGENT**

Figure 5, Col 4 Lines 6:15, Col 13 Lines 18:21, Col 14 Lines 9:21, 42:48, Col 14 Line 50: Col 16 Line 56, Col 19 Lines 57:61, Col 20 Lines 1:8, 15:18, Col 30 Lines 10:45

(references to specification of US Patent 6,990,660 which is incorporated by reference) Figure 5, Col 4 Lines 4:8, 10:14, Col 13 Lines 14:25, Col 14 Lines 10:20, Col 15 Line 6:21, Col 15 Line 63 : Line 66, Col 20 Lines 1:5, 16:19, Col 30 Line 52 : Col 31 Line 12.

**XML METADATA QUERY**

Col 14 Lines 27:29, Col 15 Lines 39:63, Col 23 Lines 50:55, Col 25 Line 39: Col 26 Line 1, Cols 27:30

(references to specification of US Patent 6,990,660 which is incorporated by reference) Col 14 Lines 26:28, 39:41, Col 23 Line 64: Col 24 Line 3, Col 26 Lines 11:39, Col 28 Lines 17:45, Col 30 Line 52: Col 31 Line 20

[Type here]

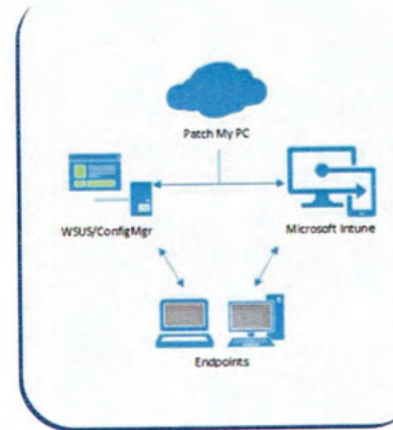
1. A method comprising:  
 (a) storing at least one patch fingerprint at a package computer; wherein each patch fingerprint comprises at least one extensible markup language (XML) metadata query; wherein at least one of the patch fingerprints is associated with a specific software update;  
 (b) downloading the at least one patch fingerprint from the package computer to a repository component of an update server; wherein the package computer is apart from the update server;

### Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (ConfigMgr and Intune) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**



### Product Features

#### Automate Third-Party Updates

- Third-party updates automatically published to SCCM and Intune
- Use existing processes to deploy updates, including ADR's
- Report on non-compliance for third-party updates in the same way as Microsoft updates
- Automatically scan your SCCM or Intune inventory to auto-enable product for publishing
- Our application feature allows you to rollback third-party updates if needed
- Third-party updates typically released the same day as the vendor makes it available

#### Automatically Create Applications

- Create base applications for SCCM and Intune
- Eliminate manual packaging of applications
- Auto-update applications to the latest version
- Ensure new machines always receive the most secure version of an application
- Use existing deployment mechanisms: task sequences, collections, or Intune assignments
- Applications include vendor icons, descriptions, and keywords

<https://patchmypc.com/freeupdater/definitions/definitions.xml>

Located at the cloud image in the diagram, PatchMyPC has its package computers/servers which have a plurality of patch fingerprints. As noted in the text in 2020 PatchMyPC released 1329 new updates and applications each of which would have at least one patch fingerprint.

Patch Fingerprints consist of a patch signature and an existence test and are stored on the Patch My PC servers in the cloud in the image. The patch signature is designed to extract information about a specific update for a specific computer being updated which includes both the identity and existence of specific hardware, registry, and software version information. Because there can be several different combinations of these items that all apply to the same patch, there will be a first and a second patch fingerprint that apply to the same patch but have different XML metadata queries. Hence the first and second (and perhaps more) metadata queries that are both associated with a specific software update. For instance, a particular application may require certain types of graphics hardware or processor hardware or versions of other software. Therefore, there would be multiple metadata queries to determine if at least one of the required combinations is present that satisfies the requirement of the specific software update. The graphic states "Automatically scan you SCCM or Intune inventory to auto-enable product for publishing" meaning that all of the combinations of hardware and software needed to support a particular patch would be subject to the patch fingerprints that determine if a required hardware/software combination is present in the device to be updated.

<sup>1</sup> Notes are provided as a **courtesy only** and for settlement purposes only subject to Federal Rule of Evidence 408 and any applicable state equivalent. Notes are not intended to be exhaustive nor indicate specific support for any claim element, nor is support for any claim element limited to that indicated in the Notes. Moreover, nothing in the Notes shall constitute an admission of any kind with respect to, or have any other legal bearing on the scope and breadth of, the claims. Nothing herein should be regarded as the provision of legal counsel, and recipients are welcome and encouraged to consult with qualified legal counsel regarding claim interpretation matters. For purposes of complete clarity, nothing herein is intended narrow or otherwise limit the scope or breadth of the claims as issued. In addition, to the extent JSON is used as a language for querying device agents or supplying device agents with data, JSON is a well-known equivalent to XML and performs the same function in the same way with the same results and therefore would satisfy the Doctrine of Equivalents test.

[Type here]

**US 8,407,687  
Claim 1**

**Patch My PC**

**Notes<sup>1</sup>**

(c) sending the at least one XML metadata query from the update server to a first target computer;

(d) scanning the first target computer via a discovery agent located on the first target computer,

wherein the scanning comprises utilizing the at least one XML metadata query in combination with the discovery agent to produce target computer information;

wherein the target computer information is related to at least hardware configuration information, registry information, software presence information, and software version information relative to the first target computer;

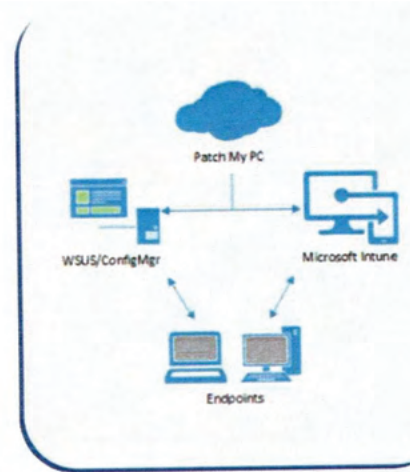
wherein the first target computer is separated from the package computer via a firewall;

## Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (**ConfigMgr** and **Intune**) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**



Patch MY PC sends metadata queries to managed devices through either SCCM or Intune in XML format which allow SCCM or Intune to scan the target computer (Endpoint) that produces target computer information regarding hardware configuration, registry, software presence, and software version information relative to the target computer. Patch My PC uses Intune and SCCM agents to facilitate communication between the target computer and Patch My PC servers in the cloud across a firewall between the two devices.

## Product Features

### Automate Third-Party Updates

- Third-party updates automatically published to SCCM and Intune
- Use existing processes to deploy updates, including ADR's
- Report on non-compliance for third-party updates in the same way as Microsoft updates
- Automatically scan your SCCM or Intune inventory to auto-enable product for publishing
- Our application feature allows you to rollback third-party updates if needed
- Third-party updates typically released the same day as the vendor makes it available

### Automatically Create Applications

- Create base applications for SCCM and Intune
- Eliminate manual packaging of applications
- Auto-update applications to the latest version
- Ensure new machines always receive the most secure version of an application
- Use existing deployment mechanisms: task sequences, collections, or Intune assignments
- Applications include vendor icons, descriptions, and keywords

[Type here]

[Type here]

<b>US 8,407,687 Claim 1</b>	<b>Patch My PC</b>	<b>Notes<sup>1</sup></b>
---------------------------------	--------------------	--------------------------

(e) sending the target computer information to the repository component located on the update server,

(f) storing the target computer information in the repository component located on the update server,

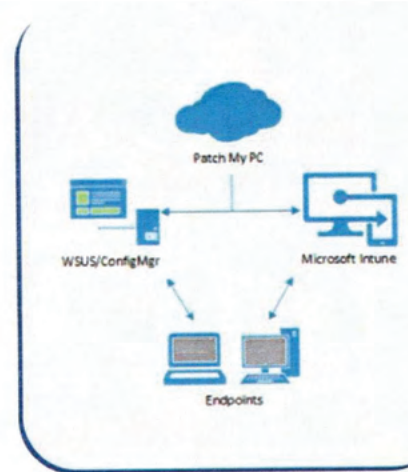
(g) comparing, at the update server, at least a portion of the target computer information with at least one of the patch fingerprints;

## Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (ConfigMgr and Intune) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**



Information gathered from target computers (Endpoint) is sent to the Patch My PC update server by the Intune or SCCM agent as appropriate for the type of Endpoint where the update server determines through a comparison of the received configuration of the hardware and software of the device if the device is eligible with respect to that configuration for a particular update.

## Product Features



### Automate Third-Party Updates

- Third-party updates automatically published to SCCM and Intune
- Use existing processes to deploy updates, including ADR's
- Report on non-compliance for third-party updates in the same way as Microsoft updates
- Automatically scan your SCCM or Intune inventory to auto-enable product for publishing
- Our application feature allows you to rollback third-party updates if needed
- Third-party updates typically released the same day as the vendor makes it available



### Automatically Create Applications

- Create base applications for SCCM and Intune
- Eliminate manual packaging of applications
- Auto-update applications to the latest version
- Ensure new machines always receive the most secure version of an application
- Use existing deployment mechanisms: task sequences, collections, or Intune assignments
- Applications include vendor icons, descriptions, and keywords

[Type here]

[Type here]

<b>US 8,407,687 Claim 1</b>	<b>Patch My PC</b>	<b>Notes<sup>1</sup></b>
---------------------------------	--------------------	--------------------------

(h) determining, at the update server, in response to the comparing step (g), whether the specific software update is absent from the first target computer;

(i) downloading, in response to the determining step (h), the specific software update to the update server; and

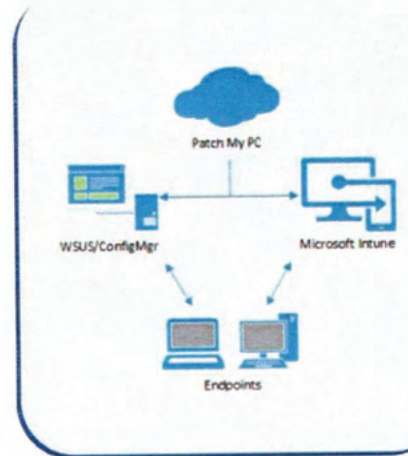
(j) downloading, in response to the determining step (h) or the downloading step (i), the specific software update from the update server to the first target computer.

## Simplified Third-Party Application Management

We help you extend Microsoft Endpoint Manager (**ConfigMgr** and **Intune**) capabilities by seamlessly integrating third-party patching and application management. Our average customer saves about **6,000 hours per year** and publishes over 1,329 updates and applications. This saves administrative time by eliminating the manual packaging of third-party products.

One of the most common ways computers are exploited is vulnerabilities in outdated third-party applications or libraries. A primary benefit of our product is **improved security** through patching vulnerable third-party applications. In 2020, we released a total of 2,915 third-party updates, which addressed **1,530 CVEs**.

By only focusing on application management, you can ensure you receive a team dedicated solely to this problem. **We're a small team passionate about what we do, why we do it, and who we do it for.**



Patch My PC servers determine if the specific update is absent from the Endpoint, and if it is absent downloads, in response to the determination, the specific software update to the update server. It then downloads in response to either the determining step or the downloading step, the specific software update from the update server or the package compute to the first target computer.

## Product Features

### Automate Third-Party Updates

- Third-party updates automatically published to SCCM and Intune
- Use existing processes to deploy updates, including ADR's
- Report on non-compliance for third-party updates in the same way as Microsoft updates
- Automatically scan your SCCM or Intune inventory to auto-enable product for publishing
- Our application feature allows you to rollback third-party updates if needed
- Third-party updates typically released the same day as the vendor makes it available

### Automatically Create Applications

- Create base applications for SCCM and Intune
- Eliminate manual packaging of applications
- Auto-update applications to the latest version
- Ensure new machines always receive the most secure version of an application
- Use existing deployment mechanisms: task sequences, collections, or Intune assignments
- Applications include vendor icons, descriptions, and keywords

[Type here]

[Type here]

US 8,407,687 Claim 1	Patch My PC	Notes <sup>1</sup>

Note on claim language: Claim language in *italics* was added to the claims during an ex-parte reexamination published as Certificate number US 6,990,660 C2 issued August 3, 2010 with the additions and deletions as shown in this chart. Claim language with ~~strike throughs~~ was removed from the claims and no longer form part of the patent's claims. Claim language in italics was added and form part of the patent's claims as shown. The deletions and additions are provided for context, clarity, and full disclosure.

Claim Language references to Specification: Citations to the specification for certain terms identified below are provided solely for convenience. The provision of these references in no way waives any argument that the claims have any meaning other than their plain and ordinary meaning to one of ordinary skill in the art in light of the specification. These citations are only provided to direct the reader to those portions of the specification for your information.

**TARGET COMPUTER:**

Figures 5, 6, 7, and 8, Col 3 Lines 50:57, Col 4 Lines 3:6, 7:11, 12:16, 22:25, 36:40, 61:65, Col 4 Line 65 : Col 5 Line 5, Col 5 Lines 16:24, Col 8 Lines 30:35, 35:42, 59:64, Col 9 Lines 3:6, 7:19, 20:23, 23:28, 30:35, 36:38, Col 10 Lines 4:6, 7:10, 15:18, 29:33, 37:42, 48:52, 52:58, 59:65, Col 9 Lines 3:4, 7:16, 16:19, 20:23, 23:28, 30:35, 36:38, Col 10 Lines 4:6, 7:10, 16:19, 29:30, 20:32, 37:42, 48:52, 52:58, 59:65, Col 12 Lines 1:4, 7:14, 19:28, 28:34, 35:40, 50:56, Col 13 Lines 5:10, 16:19, 22:26, 28:33, 40:43, 49:52, Col 14 Lines 10:20, 21:23, 41:48, 58:61, 62:67, Col 14 Line 67 – Col 15 Line 3, 4:8, 8:12, 20:24, 31:36, 39:41, 61:64, Col 16 Lines 28:39, 40:42, 42:45, 56:61, Col 17 Lines 10:19, 20:24, 30:32, 38:43, 49:51, 52:58, Col 18 Lines 31:36, 39:43, 43:48, 49:53, 54:56, 56:60, Col 18 Line 63 – Col 19 Line 1, Col 19 Lines 10:14, 45:50, 50:53, Col 19 Line 64 – Col 20 Line 1, 5:7, 11:14, 24:29, 39:42, 48:49, 50:54, Col 21 Lines 52:58,

(references to specification of US Patent 7,823,147 which is incorporated by reference) Figures 2, 3, 5, 6, 7, and 8, Col 3 Lines 44:51, Lines 64:67, Col 4 Lines 1:5, 6:10, 16:19, 30:34, 55:59, 59:66, Col 5 Lines 10:17, Col 8 Lines 26:38, 55:59, 59:67, Col 9 Lines 3:4, 10:12, 13:15, 16:24, 26:32, 33:35 Col 10 Lines 1:3, 4:7, 12:16, 24:29, 33:38, 45:49, 52:55, 56:62, Col 11 Line 65 – Col 12 Line 1, Col 12 Lines 4:11, 16:32, 33:38, 48:54, Col 13 Lines 4:13, 15:18, 21:26, 27:32, 39:43, 49:52, Col 14 Lines 10:14, 14:21, 22:24, 42:48, 60:63 Col 14 Line 66 – Col 15 Line 2, Col 15 Lines 6:10, 10:14, 23:26, 34:38, 39:43, 63:66, Col 16 Lines 30:34, 34:39, 39:40, 42:44, 44:47, Col 16 Line 58 – Col 17 Line 30, Col 17 Lines 33:35, 41:46, 47:54, 55:61 Col 18 Lines 34:39, 42:46, 46:51, 52:56, 57:65, Col 18 Line 66 – Col 19 Line 4, Col 19 Lines 13:17, 49:52, 54:57, Col 20 Lines 1:5, 9:15, 15:18, 27:35, 51:57, Col 21 Lines 56:63 Col 16 Lines 28:32, 32:39, 40:45, 55:63, Col 17 Lines 10 – 19, 20:24, 30:32, 38:43, 49:51, 52:56, Col 16 Lines 31:36, 41:43

(references to specification of US Patent 6,990,660 which is incorporated by reference) See Figures 5, 6 and 7. Col 4 Lines 4:6, Col 8 Lines 28:33, 59:62 - Col 9 Lines 7:19, Col 10 Lines 4:6, 14:17, 27:29, 57:63, Col 12 Lines 17:21, 33:40, Col 11 Line 66 - Col 12 line 2, Col 12 Lines 17:21, 33:40, Col 12 Line 65 - Col 13 Line 2, Col 13 Line 3:6, 14:17, Col 14 Lines 9:20, 41:47, 58:62, Col 14 Line 65 - Col 15 Line 1, Col 15 Lines 6:14, 23:27, Col 16 Lines 30:49, 57:65, Col 17 Lines 2:4, 12:20, 21:26, 31:33, 50:52, Col 18 Lines 32:39, 57:63, Col 18 Line 66 - Col 19 Line 4, Col 20 Lines 10:12, 16:19, 54:61, Col 21 Lines 63:66

**UPDATE STATE. PRE-UPDATE STATE NON-UPDATE STATE:**

(references to specification of US Patent 7,823,147 which is incorporated by reference Col 3 Lines 29-31, Col 8 Lines 16-26, Col 8 Lines 28:33

(references to specification of US Patent 6,990,660 which is incorporated by reference) FIGS 3, 4, 5, 5-500, Col 10 Lines 46:53 Lines 30:39

[Type here]

[Type here]

<b>US 8,407,687 Claim 1</b>	<b>Patch My PC</b>	<b>Notes<sup>1</sup></b>
---------------------------------	--------------------	--------------------------

#### UPDATE SERVER

(references to specification of US Patent 7,823,147 which is incorporated by reference) Fig 2-220 Fig 5-528, Col 3 Lines 37:40, 49:51, Col 4 Lines 18:20, 30:31, 39:54, Col 5 Lines 2:5, Col 8 Lines 33:35, 37:40, Col 9 Lines 7:8, 14:19, 20:23, 36:39, 52:54, 62: Col 10 :6, Col 10 Lines 8:10, 11:14, 26:29, Col 11 Line 66:Col 12 Line 4, Col 12 Lines 17-26, 49-54, Col 13 Lines 49:50, Col 14 Lines 10-13, Col 15 Lines 39-41, 44-46, Col 16 Lines 59-60, 65-67 Col 17 Lines 4:11, 16:20, 25:29, 30:34, 45:52, 57:59, 63:67 Col 18 Lines 1:3, 9:14, 14:16, 17:21, 21:26, 27:31, 32:33, 33:39, 41:43, 59:63, Col 18 Line 66:Col 19 4, Col 19 Lines 54:57, Col 20 Lines 10:12, 43:45, 45:47, 47:52, 58:61 Col 21 Lines 55:56 Col 24 Lines 13:15, 38:39

(references to specification of US Patent 6,990,660 which is incorporated by reference) Fig 2-220 Fig 5-528, Col 3 Lines 37:40, 49:51, Col 4 Lines 18:20, 30:31, 39:54, Col 5 Lines 2:5, Col 8 Lines 33:35, 37:40, Col 9 Lines 7:8, 14:19, 20:23, 36:39, 52:54, 62 - Col 10 Line 6, Col 10 Lines 8:10, 11:14, 26:29, Col 11 Line 66 - Col 12 Line 4, Col 12 Lines 17:26, 49:54, Col 13 Lines 49:50, Col 14 Lines 10:13, Col 15 Lines 39:41, 44:46, Col 16 Lines 59:60, 65:67 Col 17 Lines 4:11, 16:20, 25:29, 30:34, 45:52, 57:59, 63:67 Col 18 Lines 1:3, 9:14, 14:16, 17:21, 21:26, 27:31, 32:33, 33:39, 41:43, 59:63, Col 18 Line 66 - Col 19 Line 4, Col 19 Lines 54:57, Col 20 Lines 10:12, 43:45, 45:47, 47:52, 58:61 Col 21 Lines 55:56 Col 24 Lines 13:15, 38:39

#### DISCOVERY AGENT

(references to specification of US Patent 6,990,660 which is incorporated by reference) Figure 5, Col 4 Lines 4:8, 10:14, Col 13 Lines 14:25, Col 14 Lines 10:20, Col 15 Line 6:21, Col 15 Line 63 : Line 66, Col 20 Lines 1:5, 16:19, Col 30 Line 52 : Col 31 Line 12.

(references to specification of US Patent 7,823,147 which is incorporated by reference) Figure 5, Col 4 Lines 6:15, Col 13 Lines 18:21, Col 14 Lines 9:21, 42:48, Col 14 Line 50 : Col 16 Line 56, Col 19 Lines 57:61, Col 20 Lines 1:8, 15:18, Col 30 Lines 10:45

#### PACKAGE COMPUTER

(references to specification of US Patent 7,823,147 which is incorporated by reference) Col 3 Lines 47:51, Col 4 Lines 39:46, Col 9 Lines 16:19, 49: 58, Col 9 Line 65 : Col 10 Line 1, Col 10 Lines 9:12, Col 12 Lines 48:54, Col 16 Lines 59:61, Col 17 Lines 1:12, Col 17 Lines 55:61, 62:67, Col 18 Lines 6:9,

(references to specification of US Patent 6,990,660 which is incorporated by reference) FIGURES 2,3,5 Col 3 Lines 44:48, Col 4 Lines 41:48, Col 9 Lines 20:23, 52:57, 62:64, Col 10 Lines 1:4, 12:14, Col 12 Lines 49:54, Col 16 Lines 58:60, Col 17 Lines 1:11, 53:57, 60:65

#### PATCH FINGERPRINTS

(references to specification of US Patent 7,823,147 which is incorporated by reference) Col 3 Lines 36:43, 58:67, Col 4 Lines 1:5, 12:15, 16:19, 24:29 Col 12 Lines 41:62, Col 12 Line 63 : Col 13 Line 3, Col 13 Line 39 :Col 14 Line 7, Col 14 Lines 42:49, 58-60, Col 14 Line 64 : Col 15 Line 5, Col 15 Lines 6:21, 22:32, 33:36, 39:62. Col 16 Lines 13:20, 21:26, 27:30, 42:49, Col 30 Lines 50: Col 31 Line 2,

(references to specification of US Patent 6,990,660 which is incorporated by reference) FIGURES 8, 9 Col 3 Lines 56:59, Col 3 Line 66 - Col 4 Line 3, Col 4 Lines 10:14, 15:18, 23:25, Col 12 Lines 41:Col 13 Line 2, Col 13 Line 38 : Col 14 Line 7, Col 14 Lines 56:58, Col 14 Line 63 : Col 15 Line 5, Col 15 Lines 6:21, 22:32, 33:38, Col 16 Lines 13:20, 21:26, 27:30, 44-47, Col 31 Lines 25:35

#### XML METADATA QUERY

(references to specification of US Patent 7,823,147 which is incorporated by reference) Col 14 Lines 27:29, Col 15 Lines 39:63, Col 23 Lines 50:55, Col 25 Line 39:Col 26 Line 1, Cols 27:30

(references to specification of US Patent 6,990,660 which is incorporated by reference) Col 14 Lines 26:28, 39:41, Col 23 Line 64 : Col 24 Line 3, Col 26 Lines 11:39, Col 28 Lines 17:45, Col 30 Line 52 : Col 31 Line 20

[Type here]