TANGIBLE IP LLC

Aligning IP With Business ™

The Gold Standard for Patent Brokerage™

A proven record of success with more than 2500 patents sold.

· Full Patent Brokerage · Strategic IP Advisory

EXECUTIVE SUMMARY FOR THE SALE OF

Enterprise Malware Removal & Restoration Solutions

By GOOGLE

29 TOTAL ASSETS

TANGIBLE IP LLC
Aligning IP With Business ™

EXECUTIVE SUMMARY FOR THE SALE OF

Enterprise Malware Removal & Restoration Solutions

12 Families, 13 US Patents & their 16 family members in 8 other Jurisdictions

Patent Number	Patent Title	Priority Date	Issue Date	Expiry Date	Bwd/ Fwd Citations
FAMILY 1					
US 6748544	Discrete, background determination of the adequacy of security features of a computer system	Aug 19, 1999	Jun 8, 2004	Aug 18, 2019	10/41
FAMILY 2					
US 7114184 (This patent has been mapped against representative industry offerings)	System and method for restoring computer systems damaged by a malicious computer program	Mar 30, 2001	Sep 26, 2006	Oct 27, 2022 (PTA 576)	15/85
EP1374017	System and method for restoring computer systems damaged by a malicious computer program	Mar 30, 2001	Aug 23, 2006		
DE60214147	System and method for restoring a computer system which has been damaged by a malicious computer program	Mar 30, 2001	Jul 26, 2007		
ZA 200306411	System and method for restoring a computer system which as been damaged by a malicious computer program	Mar 30, 2001			
IL157542	System And Method For Restoring Computer Systems Damaged By A Malicious Computer Program	Mar 30, 2001	Dec 3, 2007		
IL157542D0	System And Method For Restoring Computer Systems Damaged By A Malicious Computer Program	Mar 30, 2001			
FAMILY 3					
US 7865723	Method and apparatus for multicast delivery of program information	Aug 25, 2004	Jan 4, 2011	Oct 26, 2028(PTA1 172)	6/17
DE102005039361	Method and apparatus for multicast transmission of program information	Aug 25, 2004	Jan 26, 2017		2/0
FAMILY 4					
US 8266684	Tokenized resource access	Sep 30, 2008	Sep 11, 2012	Sep 19, 2030	18/35

Patent Number	Patent Title	Priority Date	Issue Date	Expiry Date	Bwd/ Fwd Citations
				(PTA719)	
US 8522361	Tokenized resource access	Sep 30, 2008	Aug 27, 2013	Sep 29, 2028	21/4
FAMILY 5					
US 8374338	Transport packet decryption testing in a client device	Feb 20, 2009	Feb 12, 2013	Dec 28, 2030 (PTA 313)	4/4
CA2693749	Transport packet decryption testing in a client device	Feb 20, 2009	Apr 1, 2014		
MX2010002011	Transport packet decryption testing in a client device	Feb 20, 2009	Aug 19, 2010		
FAMILY 6					
US 8392702	Token-based management system for PKI personalization process	Jul 27, 2007	Mar 5, 2013	Jun 19, 2031 (PTA 1067)	17/38
CN101816140	Token-based management system for PKI personalization process	Jul 27, 2007			
MX2010001059	Token-based Management System For Pki Personalization Process	Jul 27, 2007			
FAMILY 7					
US 8873760	Service key delivery system	Dec 21, 2010	Oct 28, 2014	Dec 21, 2031 (PTA365)	29/0
CA2824809	Service key delivery system	Dec 21, 2010	Jun 21, 2016		
KR101528990	Service key delivery system	Dec 21, 2010	Jun 15, 2015		1/0
EP2656536	Service key delivery system	Dec 21, 2010			
FAMILY 8					
US 8898469	Software feature authorization through delegated agents	Feb 5, 2010	Nov 25, 2014	Mar 11, 2032 (PTA401)	17/19

Patent Number	Patent Title	Priority Date	Issue Date	Expiry Date	Bwd/ Fwd Citations
EP2531950	Software feature authorization through delegated agents	Feb 5, 2010			
MX2012009025	Software feature authorization through delegated agents	Feb 5, 2010	May 13, 2014		
FAMILY 9					
US 8990221	Device and method for updating a certificate	May 30, 2008	Mar 24, 2015	Feb 15, 2033 (PTA1605)	7/5
FAMILY 10					
US 9054879	Method and apparatus for delivering certificate revocation lists	Oct 4, 2005	Jun 9, 2015	Nov 10, 2033 (PTA 2701)	32/16
FAMILY 11					
US 9177114	Method and apparatus for determining the proximity of a client device	Oct 4, 2005	Nov 3, 2015	Oct 2, 2032 (PTA2297)	19/17
FAMILY 12					
US 9313214	Enhanced security using service provider authentication	Aug 6, 2004	Apr 12, 2016	Jan 23, 2029(PTA1631)	24/25
EP1776799	Enhanced security using service provider authentication	Aug 6, 2004	Nov. 1, 2017		
GB EP1776799	Enhanced security using service provider authentication	Aug 6, 2004			
FR EP1776799	Enhanced security using service provider authentication	Aug 6, 2004			
NL EP1776799	Enhanced security using service provider authentication	Aug 6, 2004			
DE602005052983.7	Enhanced security using service provider authentication	Aug 6, 2004			

Evidence of Use:

This portfolio is believed to cover the following products/services under the Enterprise Malware Removal and Restoration domain:

1. Computer Security Solutions
2. Computer Backup, Disaster Recovery and Computer Restore Solutions
3. Software Licensing / Certification Solutions
4. Token / Key Management Solutions
5. Proximity Detection Software Solutions
6. Solutions for Secured / Encrypted Data Communication over Network
7. Streaming Solutions

Industry Representative claim charts will be provided under NDA to serious buyers only.

Encumbrances: There are some minimal existing encumbrances on the portfolio, including obligations with respect to LOT Network (http://lotnet.com), and any sale is subject to a license back to the seller in accordance with industry standards. More details can be shared with serious buyers under NDA.

Pricing Guidance: We will be happy to share our pricing guidance for an all cash sale to interested buyers.

Submission Deadline: None. Offers will be treated in the order they are received.

Important Disclaimer: *This document includes information regarding the sale of a valuable patent portfolio. The information, data, and charts are provided only for each prospective buyer's use in independently evaluating the portfolio. The discussion of the use or applicability of the portfolio is only for illustrative purposes. This document and any documents exchanged during the sales process are not intended to be, and should not be interpreted as being, a notice of infringement, any form of accusation of infringement, or any opinion regarding the actual use of the patent portfolio.*

Table of Contents

EXECUTIVE SUMMARY

1. The Opportunity

Tangible IP, LLC is a leading patent brokerage firm focusing on high value, high quality portfolios with over 2500 assets sold since inception. We are Google LLC's exclusive agent for divesting the patent portfolio described in this document pertaining to the "**Enterprise Malware Removal & Restoration**" domain of the **cyber security market**. With this portfolio, we offer an unprecedented opportunity for interested parties. Commercial industry buyers may obtain strategic offensive and defensive positions with this portfolio.

2. Market Relevance and Trends

The patents/patent applications in the offered patent portfolio describe technologies and solutions for enterprise malware removal and restoration. More specifically the offered technologies are related to the solutions for:

- checking security of a computer network systems
- restoring computer systems
- checking licenses and certificates of applications or devices
- enabling multicast streaming
- secure transmission of digital content
- determining proximity of a device
- token/service-key management over a communications network.

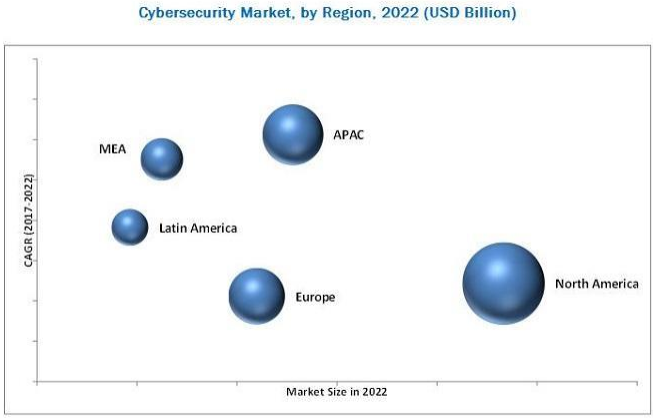
The technologies explained in the patent portfolio find applications in:

- computer security solutions
- data recovery or restoration solutions
- token & service-key management solutions
- solutions for secured and encrypted data communication over a network.

CYBER SECURITY

According to a 2015 report on cybersecurity by Zion Market Research, the global cyber security market was valued at **$105.45 billion USD** in 2015, is expected to reach **$181.77 billion USD in 2021**, and is anticipated to grow at a CAGR of 9.5% between 2016 and 2021. Cyber security focuses on securing IT infrastructure (computers, servers, confidential data, etc.) from cyber criminals and cyber attacks. With the increased penetration of the internet and the growth of connected devices (mobile and computers), the importance of various cyber security measures has increased significantly. Various types of cyber crime including hacking, software piracy, denial of service attack, and cyber terrorism, make cyber security an integral part of an enterprise's IT infrastructure. Robust cyber security measures offer numerous advantages, including enhanced security of cyberspaces, expanded digital safeguard and quicker reaction time in case of cyber attacks. These advantages enhance the value of a service given to the market end-users.

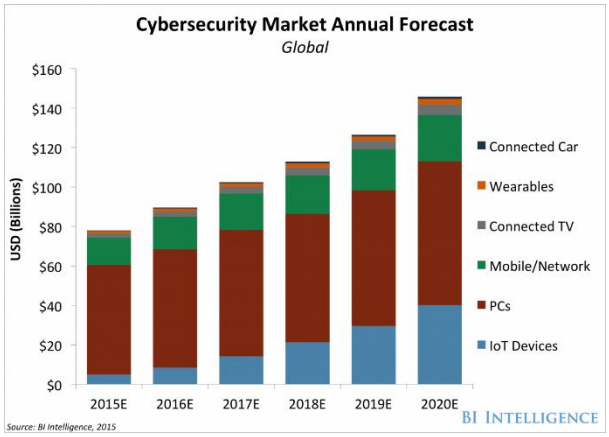
MarketsandMarkets, in its 2017 report on cybersecurity market, stated that the cyber security market is expected to grow from $137.85 billion USD in 2017 to **$231.94 billion USD by 2022**, at a CAGR of 11.0%. Strict data protection directives and cyber terrorism are the major driving forces of the cyber security market. The cyber security market is estimated to grow rapidly due to the growing security needs of the Internet of Things (IoT) and Bring Your Own Device (BYOD) trends, and increased deployment of web and cloud-based business applications. North America is estimated to hold the largest share of the cyber security market in 2017, due to technological advancements and early adoption of cyber security in the region. The market in APAC is expected to grow at its highest CAGR between 2017 and 2022.



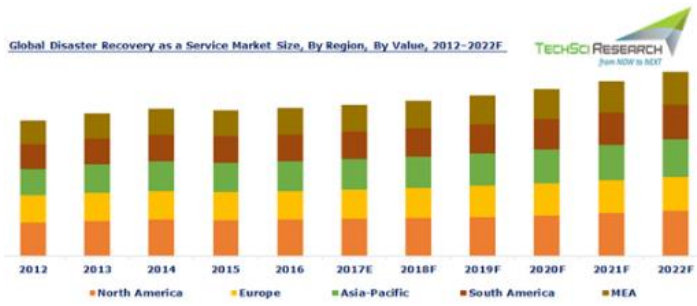
Additionally, a 2016 report from BI Intelligence — Business Insider's research service — estimated $655 billion will be spent on cyber security initiatives to protect PCs, mobile devices, and Internet of Things (IoT) devices between 2015 and 2020. BI breaks down the forecasted spending as follows:

- $386 billion spent on securing PCs;
- $172 billion spent on securing IoT devices;
- $113 billion spent on securing mobile devices.

Further, the hot areas for growth are cloud security, security analytics, threat intelligence, and mobile security.



According to a 2017 report by MarketsandMarketsDisaster Recovery as a Service (DRaaS) market size is estimated to grow from $2.19 billion USD in 2017 to **$12.54 billion USD by 2022**, at a CAGR of 41.8% during the forecast period. The demand for DRaaS is vastly driven by increased business flexibility and automation capabilities. The backup and recovery services are expected to have the major market share in the service type segment of the DRaaS market during the forecast period. The backup and recovery services play a key role in the DRaaS market, as it provides cost-effective, automated, reliable, secure, and scalable solutions to enterprises, ensuring business continuity in the event of disaster.



TechSci Research, in its 2017 report, projects the global DRaaS market to grow at a CAGR of over 43%, in value terms, during 2017-2022.

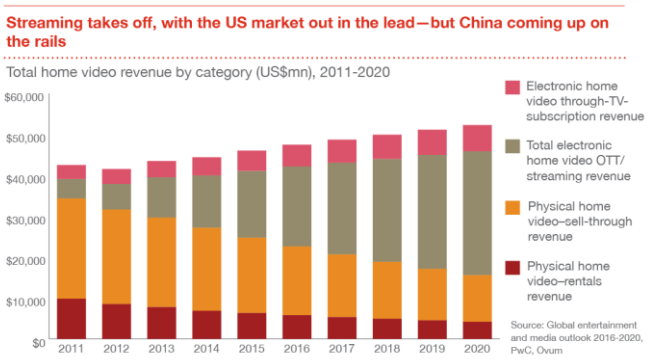
The report identifies a number of factors expected to drive demand for DRaaS over the next five years including:

- rapid expansion of the internet in developing economies,

- increased requirement for implementing disaster recovery backup plans to secure critical information and transactions,
- high flexibility and cost-effectiveness of DRaaS solutions,
- development of internal IT infrastructures across a number of industry verticals.

VIDEO STREAMING

A MarketsandMarkets forecasts the global video streaming software market size to grow from $3.25 billion USD in 2017 to **$7.50 billion USD by 2022**, at a CAGR of 18.2%. Increasing need for transcoding to deliver videos to a large number of end-users, the extensive growth of online videos, and growing demand for on-demand streaming are the major factors driving the growth of the market. Further, Technavio's market research analyst predicts the global streaming media device market to grow at a CAGR of more than 17% between 2016 and 2020. The growing integration of digital video content with streaming media devices will act as a major driving force for the growth of the global streaming media device market.



3. The Company

Google LLC (formerly, Google Inc.) holds all the patents in the offered patent portfolio. In 2015, Google reorganized its various interests, products, and services as a conglomerate called Alphabet Inc. Alphabet is listed on various stock exchanges and has revenue of over $90 billion.

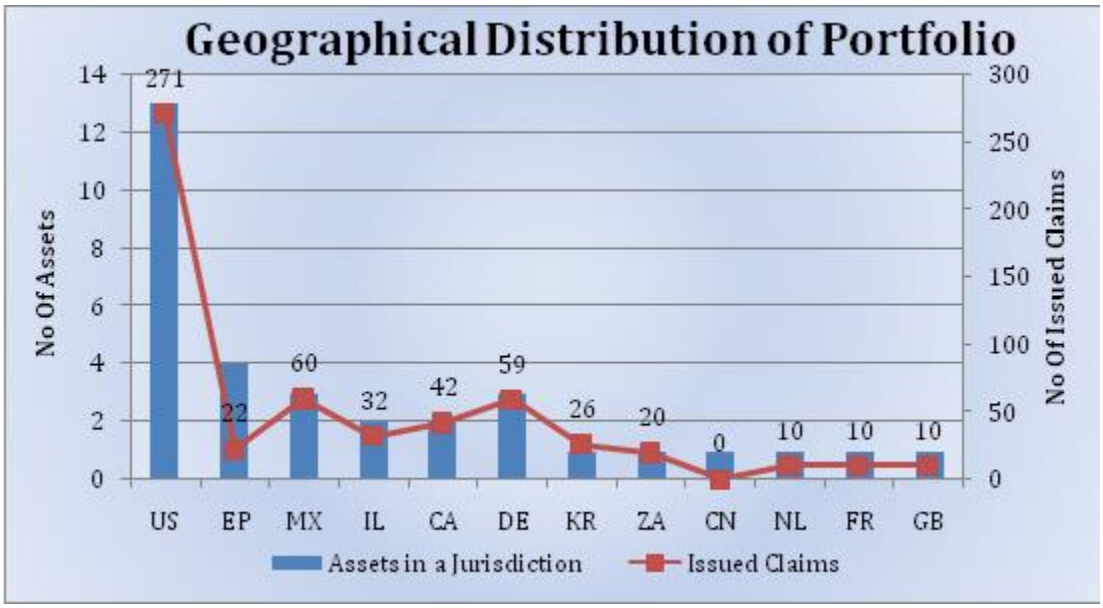
Google specializes in internet-related services and products. The company has a range of services and products related to email solutions, online advertising technologies, search, social networking solutions, productivity solutions, consumer services, cloud services, cloud computing, mobile OS and solutions, software, hardware, and others.

4. The Patent Portfolio

The offered patent portfolio, which is currently owned by Google, consists of **12** distinct patent families. The patents in the offered patent portfolio describe technologies and solutions for:

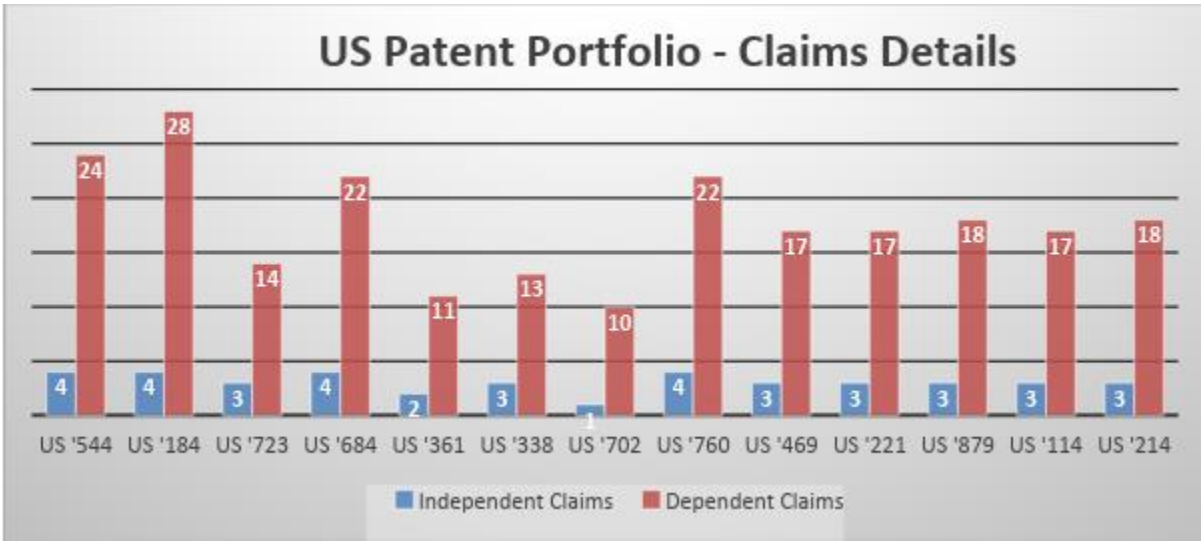
- checking security of computer/network systems,
- recovering/restoring computer systems,
- checking licenses / certificates of applications/devices,
- enabling multicast streaming,
- secure transmission of digital content,
- determining proximity of a device, and
- token / service-key management in a communications network.

The twelve distinct patent families of the offered patent portfolio, presently, comprise **29 active patents** and patent applications, distributed over nine jurisdictions. The following chart shows the distribution of the active assets and their number of issued claims in each jurisdiction:

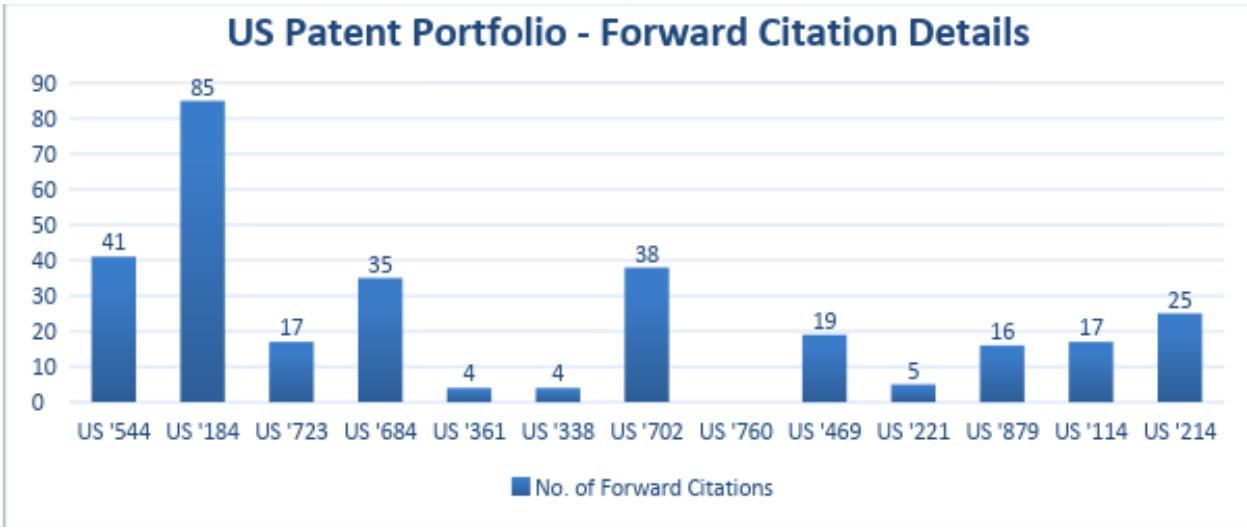


There are four active patent applications out of 29 active assets of the portfolio. The four active patent applications include two patent applications in EP jurisdiction and one pending patent

application in each of Israel and China. The offered patent portfolio has five hundred sixty two **(562) issued claims** in the above-mentioned geographies. The US portfolio of the offered patent portfolio has **two hundred seventy-one (271) issued claims**, which include **forty** independent claims and two hundred thirty-one dependent (231) claims. The following chart provided below depicts the no. of claims of each active US patent in the offered patent portfolio.



The thirteen US patents in the offered patent portfolio have **three hundred six (306) forward citations** by patents and patent applications from other companies. Several companies, e.g. Microsoft, IBM, Apple, Sony, Ericsson, Samsung, and others have cited the patent portfolio multiple times. The chart provided below depicts the number of forward citations of each active US patents of the offered patent portfolio.



The priority date of the offered patent portfolio ranges from August 1999 to December 2010.

5. Detailed Portfolio Review

The patent portfolio comprises **twelve distinct patent families** which include the following active patents - thirteen enforceable US patents, three MX patents, two CA patents, two DE patents, one EP patent, one IL patent, one KR patent, one ZA patent, three EP pending patent applications, one IL patent application and one CN patent application.

The following shows the technologies claimed by various patent families of the portfolio:

Family Number	Family Technology Description
1	Methods and systems for discretely and efficiently checking the level of security on PC systems and data processing systems
2	Various embodiments for restoring a computer system which has been modified by a malware
3	Solutions which enable multicast stream of digital content from a multicast address to several client devices

Family Number	Family Technology Description
4	Multiple methods and systems for unlocking debugging functionality of a hardware device for a user
5	Methods and systems for testing a transport packet decrypting module of a client device
6	Multiple embodiments of a system for token-based management of a PKI (public key infrastructure) personalization process
7	Multiple embodiments of an invention which describe the usage of a Service Key Delivery (SKD) system for delivering service keys to client devices in a communications network
8	Methods for enabling selected features of a software product residing on an end user electronic device with a license delivered from a licensing provider to a service provider of the end user electronic device
9	Methods and systems for updating certificates for the potential recipients of the certificate
10	Methods for delivering a revocation list over a one-way broadcast network to receivers with limited memory capabilities.
11	Methods and systems for determining proximity of a device.
12	Methods for providing enhanced security using service provider authentication.

Family 1

The first family of the offered patent portfolio includes one active US patent:

- **US Patent 6,748,544** (Discrete, background determination of the adequacy of security features of a computer system) was filed on August 19, 1999 and has a priority date of August 19, 1999. The patent and its corresponding patent application have been **cited 41 times** by patents / patent applications from companies like IBM, Samsung, Nokia, Broadcom, Dell, BlackBerry (formerly, Research In Motion), Trend Micro, Ebay, Intel, Sandisk, and others.

US Patent '544 claims methods and systems for discretely and efficiently checking the level of security on PC systems and data processing systems. The claimed invention accesses the security password of the system via a dynamic call within the BIOS of the system. The dynamic call is initiated without any user input. The retrieved password is analyzed to determine if the security access available on the

system is adequate for protection of the system. The invention generates an alert asking the user to upgrade the security of the system in case the security password is not adequate as per the standards of the system. The claimed invention further ensures that the password is not provided outside the internal environment of the system.

Family 2

The second family of the offered patent portfolio includes the following active patents / patent applications:

- **US Patent 7,114,184** (System and method for restoring computer systems damaged by a malicious computer program) was filed on March 30, 2001 and has a priority date of March 30, 2001. The patent and its corresponding patent application have been **cited 85 times** by patents / patent applications from companies like MacAfee, BlackBerry, Microsoft, Symantec, Kaspersky, Airbus Operations, IBM, Lenovo, HP, Hitachi, and others.

US Patent '184 describes methods and systems for restoring a computer system which has been modified by malicious code. The claimed invention scans the computer system to identify the malicious code. Upon identification of the malicious code, the invention retrieves from a data file all relevant information related to the code. The retrieval process also involves gathering information related to a command which shall be used for restoring the computer to a state that existed prior to it being modified by the malicious code. The claimed invention then executes the said command to restore the system to the state that existed prior to modification by the malicious code. The restore operation ensures that the host file having the malicious code is not restored to its previous safe state.

- **EP Patent 1,374,017** (System and method for restoring computer systems damaged by a malicious computer program) was filed on March 26, 2002 and has a priority date of March 30, 2001.
- **DE Patent 60,214,147** (System and method for restoring a computer system which has been damaged by a malicious computer program) was filed on March 26, 2002 and has a priority date of March 30, 2001.
- **ZA Patent 200,306,411** (System and method for restoring computer systems damaged by a malicious computer program) has a priority date of March 30, 2001.
- **IL Patent 157,542** (System and method for restoring computer systems damaged by a malicious computer program) has a priority date of March 30, 2001.

- **IL Patent Application 157,542D0** (System and method for restoring computer systems damaged by a malicious computer program) has a priority date of March 30, 2001.

Family 3

The third family of the offered patent portfolio includes the following active patents / patent applications:

- **US Patent 7,865,723** (Method and apparatus for multicast delivery of program information) was filed on August 11, 2005 and has a priority date of August 25, 2004. The patent and its corresponding patent application have been **cited 17 times** by patents / patent applications from Microsoft, Cisco, General Instrument, Ericsson, China Mobile, Intel, Samsung, and others.

US Patent '723 describes methods and systems which are related to multicast stream of digital content from a multicast address to several client devices. The claimed invention generates session description messages for the multicast stream of digital content. The session description message includes at least one content access parameter which further includes DRM data and channel key identification data associated with the corresponding channel of the multicast stream. The channel key identification data also identifies channel key sets which are stored on a server and are used to derive content decryption keys for decryption of digital content being multicast in the channel. Each of the session description messages is signed using a cryptographic key which generates authentication data. The session description messages are then multicast to the client devices using a predefined multicast address.

- **DE Patent 102005039361** (Method and apparatus for multicast transmission of program information) was filed on August 19, 2005 and has a priority date of August 25, 2004.

Family 4

The fourth family of the offered patent portfolio includes following active patents:

- **US Patent 8,266,684** (Tokenized resource access) was filed on September 30, 2008 and has a priority date of September 30, 2008. The patent and its corresponding patent application have been **cited 35 times** by patents / patent applications from General Instrument, BlackBerry, Verizon, Microsoft, Qualcomm, Sony, Intel, Nvidia, IBM, Google, Ericsson, and others.

US Patent '684 claims multiple methods and systems for unlocking debugging functionality of a hardware device for a user. The claimed invention obtains a signed permission object from the user for the hardware device. The signed permission object is based on a user-selected product model and a user-authorized configuration of the product. The signed permission object includes a sequence number and an expiration counter which indicates a lifetime for the object. The claimed invention validates the signed permission object against the configuration stored on the hardware. If the object is valid, the expiration counter is updated to decrease the lifetime and the corresponding sequence number is stored as the last recorded sequence number in the hardware device. The claimed invention then unlocks the debugging functionality of the hardware for the user based on the validated signed permission object.

- **US Patent 8,522,361** (Tokenized resource access) was filed on August 9, 2012 and has a priority date of September 30, 2008.

US Patent '361 expands on the invention – unblocking debugging functionality of hardware devices for users – already claimed in the '684 patent. The claimed invention receives a login request from the user and authenticates the user based on his/her login credentials. The invention also receives a selection of a product model from the user and determines access control permissions of the user for the selected product model. The user's access control permissions are compared to the available permissions for the selected product model to determine the configurations of the product that are allowed for the user. The invention then generates a signed permission object which, if valid, unblocks the debugging functionality of the hardware device for the user.

Family 5

The fifth family of the offered patent portfolio includes the following patent and patent applications:

- **US Patent 8,374,338** (Transport packet decryption testing in a client device) was filed on February 18, 2010 and has a priority date of February 20, 2009. The patent and its corresponding patent application have been **cited 4 times** by patents / patent applications from companies like Cisco, Broadcom, and others.

US Patent '338 describes methods and systems for testing a transport packet decrypting module of a client device. The claimed invention first decrypts a transport packet decrypting module on an encrypted test word to derive a test control word. The invention, in the next step, again decrypts the transport packet decrypting module on multiple test transport packets by using the test control word,

derived in the first step, via a predetermined content decryption algorithm. Upon implementation of the two steps, the KIV (key integrity value) is derived from the decrypted transport packets. The derived KIV is then compared with a value stored in the client device to verify whether the transport packet decrypting module of the client device is functioning properly or not.

- **CA Patent 2,693,749** (Transport packet decryption testing in a client device) was filed on February 19, 2010 and has a priority date of February 20, 2009.
- **MX Patent 2,010,002,011** (Transport packet decryption testing in a client device) has a priority date of February 20, 2009.

The CA patent and MX patent application of this patent family also describe the exact same steps for testing a transport packet decrypting module of a client device. The claimed inventions implement a two-step decryption function to identify a KIV which is then compared to a stored value to verify the functioning status of the transport packet decrypting module.

Family 6

The sixth family of the offered patent portfolio includes following active patent and patent applications:

- **US Patent 8,392,702** (Token-based management system for PKI personalization process) was filed on July 17, 2008 and has a priority date of July 27, 2007. The patent and its corresponding patent application have been **cited 38 times** by patents / patent applications from companies like Motorola, Visa, Red Hat, Amazon, IBM, EMC, and others.

US Patent '702 claims a system for token-based management of a PKI (public key infrastructure) personalization process. The claimed system includes a token request management system (TRMS) which is configured to gather request information from a requestor. The system request information comprises a location-based trust domain, PKI data type and a workstation identifier. The claimed system also comprises a token personalization system (TPS) which is configured to personalize a hardware token such that usage of the hardware token is constrained by the request information. The hardware token is bound to a workstation which is configured to receive the hardware token. The workstation then uses credentials within the hardware token to request and download PKI data from a PKI server. The claimed system also monitors actual usage of the hardware tokens and the PKI data.

- **CN Patent Application 101,816,140** (Token-based management system for PKI personalization process) has a priority date of July 27, 2007.
- **MX Patent 2,010,001,059** (Token-based management system for PKI personalization process) has a priority date of July 27, 2007.

Family 7

The seventh family of the offered patent portfolio includes the following active patents and patent applications:

- **US Patent 8,873,760** (Service key delivery system) was filed on December 21, 2010 and has a priority date of December 21, 2010.

US Patent '760 claims methods and systems which describe the usage of a Service Key Delivery (SKD) system for delivering service keys to client devices in a communications network. The delivered service keys are used to decrypt an encrypted key which is further used to decrypt an encrypted digital content. The claimed invention receives a distribution time frame for the keys and a listing of client device identifications through a user interface. The claimed invention also includes a scheduling module which is used to partition the distribution time frame into a number of time slots. The number of time slots depends on a variety of factors, e.g. user preference, statistics associated with the usage data, configuration of device, etc. The scheduling module then assigns each client device to a different time slot to build a schedule / listing of the devices. The claimed invention, further, includes a message generator which is configured to send key delivery messages to each client device.

- **CA Patent 2,824,809** (Service key delivery system) was filed on December 15, 2011 and has a priority date of December 21, 2010.
- **KR Patent 101,528,990** (Service key delivery system) was filed on December 15, 2011 and has a priority date of December 21, 2010.
- **EP Patent Application 2,656,536** (Service key delivery system) was filed on December 15, 2011 and has a priority date of December 21, 2010.

Family 8

The eighth family of the offered patent portfolio includes the following active patents and patent applications:

- **US Patent 8,898,469** (Software feature authorization through delegated agents) was filed on February 4, 2011 and has a priority date of February 5, 2010. The patent and its corresponding patent application have been **cited 19 times** by patents / patent applications from companies like Google, Appcentral, Intel, Arris Technology, and others.

US Patent '469 claims methods for enabling selected features of a software product residing on an end user electronic device with a license delivered from a licensing provider to a service provider of the end user electronic device. The method includes means for requesting at least one license to authorize a first service provider. An encrypted installation key uniquely associated with the first service provider is received. Further, an authorization agent module for installation on one or more authorization agent devices associated with the first service provider is also received in the same step. The encrypted installation key and the authorization agent module are then installed on the authorization agent devices. A device-unique identifier (DUID) is generated for each authorization agent device based on hardware characteristics of the respective authorization agent devices. The DUID and the encrypted installation key are then sent from the authorization agent device to a licensing provider to obtain the requested license. The requested license is received by the authorization agent devices if the DUID and the encrypted installation key are validated by the licensing provider. The license on the authorization agent device authorizes and enables the selected features of the software product on the end user electronic device.

- **EP Patent Application 2,531,950** (Software feature authorization through delegated agents) has a priority date of February 5, 2010.
- **MX Patent 2,012,009,025** (Software feature authorization through delegated agents) has a priority date of February 5, 2010.

The EP and MX patent applications of the patent family also describe multiple embodiments for enabling selected features of software on an end user device with a license delivered from a licensing provider to a service provider of the end user device.

Family 9

The ninth family of the offered patent portfolio includes one active US patent:

- **US Patent 8,990,221** (Device and method for updating a certificate) was filed on September 24, 2008 and has a priority date of May 30, 2008. The patent and its corresponding patent application have been **cited 5 times** by patents / patent applications from companies like Microsoft, and others.

US Patent '221 claims methods and systems for updating certificates for potential recipients of the certificate. The claimed invention first determines whether any certificates require an update. If the certificates require an update, the invention determines the number of certificates that need an update. The invention then requests updates for each certificate that requires updating and simultaneously sets a timer for a fixed time duration. The time duration could be either of two values depending on whether the number of certificates that require an update is smaller or greater than a fixed preset number.

Family 10

The tenth family of the offered patent portfolio includes one active US patent:

- **US Patent 9,054,879** (Method and apparatus for delivering certificate revocation lists) was filed on June 19, 2006 and has a priority date of October 4, 2005. The patent and its corresponding patent application have been **cited 16 times** by patents / patent applications from companies like Panasonic, Red Hat, Motorola, Ericsson, and others.

US Patent '879 discloses an apparatus and method for delivering a revocation list over a one-way broadcast network to receivers with limited memory capabilities. The revocation list is partitioned to form a first certificate revocation list (CRL) sequence if the number of entries in the revocation list exceeds a predetermined value. Each partition of the CRL sequence includes a unique signature that can be verified independent of other partitions of the sequence. The claimed invention then assigns individual identification numbers belonging to a first identification number series to the partitions of the first CRL sequence. The individual identification numbers comprise a numerical value from which a client can determine whether the partitions are part of the same CRL sequence or not, and whether the CRL sequence has been received in its entirety or not. The first CRL sequence is, thereafter, interleaved into a first content transport stream which is sent across the broadcast network to the receivers.

Family 11

The eleventh family of the offered patent portfolio includes one active US patent:

- **US Patent 9,177,114** (Method and apparatus for determining the proximity of a client device) was filed on June 19, 2006 and has a priority date of October 4, 2005. The patent and its corresponding patent application have been **cited 17 times** by patents / patent applications

from companies like Freescale Semiconductor, Samsung, IBM, Hulu, Canon, Raytheon, and others.

US Patent '114 claims methods and systems for determining proximity of a device. The claimed invention acquires key management requests, which comprises requests to obtain a decryption key specific to the device, from a client device. A measurement request is then transmitted to the device. Upon receiving a reply to the measurement request, the invention determines whether a measurement parameter associated with the transmitting and the receiving signals exceeds a predetermined threshold. If the predetermined threshold is not exceeded, i.e. the device is proximate to an associated network, then a reply to the original key management request is transmitted to the device. The reply to the key management request allows the device to establish a secure session with the network server from which digital content can be acquired.

Family 12

The twelfth family of the offered patent portfolio includes the following active patent and patent applications:

- **US Patent 9,313,214** (Enhanced security using service provider authentication) was filed on August 6, 2004 and has a priority date of August 6, 2004. The patent and its corresponding patent application have been **cited 25 times** by patents / patent applications from companies like Nokia, Microsoft, Sony, Samsung, NEC, Motorola, Sony Ericsson, Huawei, AT&T, Apple, and others.
- **EP Patent 1,776,799** (Enhanced security using service provider authentication) was filed on August 5, 2005 and has a priority date of August 6, 2004. The issue date of the patent is November 1, 2017. EP patent is enforceable in Great Britain, Netherland, France and Germany jurisdictions.

US Patent '214 discloses methods and systems for providing enhanced security using service provider authentication. The claimed invention comprises a network interface for receiving an application suite over a communication network. The application suite includes an application, security information associated with the application and the carrier identification associated with the application. The carrier identification identifies the communications service provider whose customers are the intended recipients of the application. Upon receiving the application suite, a hardware processor of the claimed invention authenticates the received security information against a root certificate to identify whether the application belongs to a trusted domain or not. If the

application is found to belong to a trusted domain, the received carrier identification is compared with the stored carrier identification. The application is only allowed to access the data stored on the network or be installed on the network if the first and second carrier identification data are matched.

6. Foreign Counterparts

All twelve families of the offered patent portfolio have active US patents. The following table depicts the active patent families in other jurisdictions:

Jurisdictions	Active Patent Families
US	All Families
Europe	Families - 2nd, 7th, 8th and 12th
Germany	Families - 2nd, 3rd and 12th
Canada	Families - 5th and 7th
Mexico	Families - 5th, 6th and 8th
Israel	Family -2nd
South Africa	Family - 2nd
China	Family - 6th
Korea	Family - 7th
Great Britain	Family – 12th
Netherland	Family – 12th
France	Family – 12th

7. Power Rankings

A. Lack of Prior Art

The priority date of the offered patent portfolio ranges from August 1999 to December 2010. The first and second patent families have a priority date earlier than 2002. The seventh and eight families claim priority from 2010. The fourth and fifth patent families have a priority date in 2008 and 2009 respectively. The remaining patent families have a priority date between 2004 and 2008.

The majority of the patent families in the portfolio have a priority date dating to the period of time when the need and/or demand for solutions related to security of computer solutions, streaming of digital content over networks, mobile operating systems and secured/encrypted data communications over network had just started. The forward citations, include several prominent companies in the same technology space. Most of the biggest companies, e.g. Microsoft, Apple, Samsung, Intel, IBM, Sony, MacAfee, and others in related technology domains have cited multiple patents of the offered patent portfolio. This potentially denotes the early stage development of the offered patent portfolio in its technology domain.

B. Commercial Maturity

Security solutions for computer systems, solutions enabling secured data access, and data encryption technologies for transmission over network are some of the most important technologies in the present world where data and information is critical to the majority of the businesses across the globe. With an increase in hacking, phishing and other unsecured access to secure databases and computer systems, the demand and corresponding usage of security solutions continues to rise. Adoption of technologies for system or software restoration for computer devices (including mobiles and tablets) continues to increase as a result.

The increased penetration of cellular data transfer technologies, continuous increase of data transfer speeds, and adoption of several other network topologies has resulted in several services and solutions which offer streaming and online data access solutions. Verification of licenses and certificates of software/hardware or web-data is also more relevant in the present scenario due to increased cases of data piracy, the rapid growth of paid services for data streaming/transfer, and the launch of several subscription-based data services.

As such, the demand for the types of technologies, which have been claimed in the offered patent portfolio, has already taken a huge leap in comparison to its state about a decade ago and it is expected to continue to grow at a tremendous pace. As a result, it can safely be assumed that the offered patent portfolio will continue to appreciate over time as more and more companies adopt its underlying approach.

8. Encumbrances

All the patents in the offered patent portfolio were originally assigned to one of the five companies – Google Technology Holdings LLC, IBM Corp, Computer Associates Think Inc., General Instrument Corp or Motorola Mobility LLC. However, Google presently holds all the patents in the offered patent portfolio. There are some encumbrances on the portfolio, including obligations with respect to LOTNetwork (http://lotnet.com), and any sale is subject a license back to the seller in accordance with industry standards. More details can be shared with serious buyers under NDA.

9. Evidence of Use

Tangible IP's team of seasoned registered patent attorneys has prepared several industry representative claim charts for select patents in this portfolio. Any details as to evidence of use pertaining to a given patent in the portfolio on offer will be provided only to serious buyers under NDA.

10. Targeted Price

We will be happy to share our pricing guidance for an all cash sale to interested buyers.

11. Sale Structure and Submission Deadline

The portfolio is offered only to a limited number of potential buyers. There are no formal submission deadlines. Offers will be treated in the order received in writing. Assets will be taken off the market once a PPA has been executed and buyers will be given a reasonable period to complete the closing.

12. Contact Information

For all inquiries, please contact **Louis Carbonneau**, CEO of Tangible IP, LLC, at:

By Phone: +1-425-868-9280 (direct) or +1-425-213-7252 (mobile)
Via Skype: louis.carbonneau
By Email: louis@tangibleip.biz