Whitepaper Ver. 4.9

General Release - Subject to Change

Cloudbric Executive Team

https://www.cloudbric.com/blockchain-security support@cloudbric.com

TABLE OF CONTENTS

Current Cybersecurity Reality

As the world shifts to a more interconnected and internet driven society, the need to secure private online data is becoming increasingly paramount. The open flow of information between various online channels makes both users and organizations highly vulnerable to cyber hacking. Critical online data breaches are now reaching record highs with millions of personal records being stolen each and every year.

Cyber attacks are also expanding their reach into new and emerging markets, such as cryptocurrency assets and exchanges. In the past year alone, multiple cryptocurrency funds, worth over hundreds of millions, were hijacked by online criminals. This makes protection for digital assets found within the cryptocurrency market a new top priority for all users.

In order to counteract the growing cybersecurity concern, users must take action by safeguarding private data flowing across all communications protocols (i.e. email, websites, mobile devices, cryptocurrency exchanges, etc.). However, the implementation and management of multiple security solutions can be an extremely difficult task due to fundamental issues present in the market, which ultimately inhibits users from fully embracing the widespread adoption of cybersecurity.

Issues Facing End Users

The information security market as a whole is in need of a major paradigm shift with an emphasis on efficiency, transparency, and trust. This is due to a variety of issues that users face within the cybersecurity market.

Oversaturation of Security Solutions

The need to secure data across numerous online channels has led to the oversaturation of solutions made available to users. Currently, there are more than 1,600 solutions offered in the cybersecurity market worldwide, which makes the selection process for each security solution overly complicated. Users are usually left to their own devices to properly test, judge, and select from a sea of providers that offer similar solutions. Also, the management of these diverse solutions can be quite burdensome as users are forced to adapt to drastically different security platforms, software, settings configurations, pricing, etc.

The idea of taking a layered approach to cybersecurity, as outlined above, is simply inefficient and outdated. Studies show that some organizations use up to 70 different vendor made security solutions in order to solve a host of information security related issues. Deploying more security solutions does not necessarily lead to higher security. In fact, utilizing an excess of solutions could leave users even more susceptible to hackers as users must be cognizant of system upgrades and security bugs found in each respective software.

For many users, cybersecurity is a very foreign and complicated subject. This leads to vendors taking advantage of users' lack of knowledge by flooding the market with an overabundance of security solutions. Security providers should no longer look to profit off user naivety and instead should focus on building consolidated solutions that allows users to truly feel secure online.

Centralized Threat Intelligence Data

Another issue present in the information security market is the lack of transparency over threat intelligence data. By providing servicing to end users, cybersecurity vendors are able to collect vast amounts of emerging cyber threat information, such as attack patterns and behaviors, malicious IP addresses, identification of malware infected files, etc. However, threat intelligence data compiled through security servicing is not made accessible for public use.

Vendors typically privatize this information and use it for their own personal gain. For instance, cyber threat data is used to help develop new market solutions, issue pertinent software updates, create industry reports and analytics, etc., all of which can be valuable sources of revenue. On the other hand, users who help generate this data for vendors are left with little to no compensation and are forced to continue paying for vendor made services. This uneven centralization of threat data and lack of compensation must come to an end.

Rather than profiting from the security community, cybersecurity vendors must become active leaders on behalf of the community by making security intelligence open and accessible to all. Also, users should be encouraged and incentivized to secure their digital assets to promote a more trusted online society.

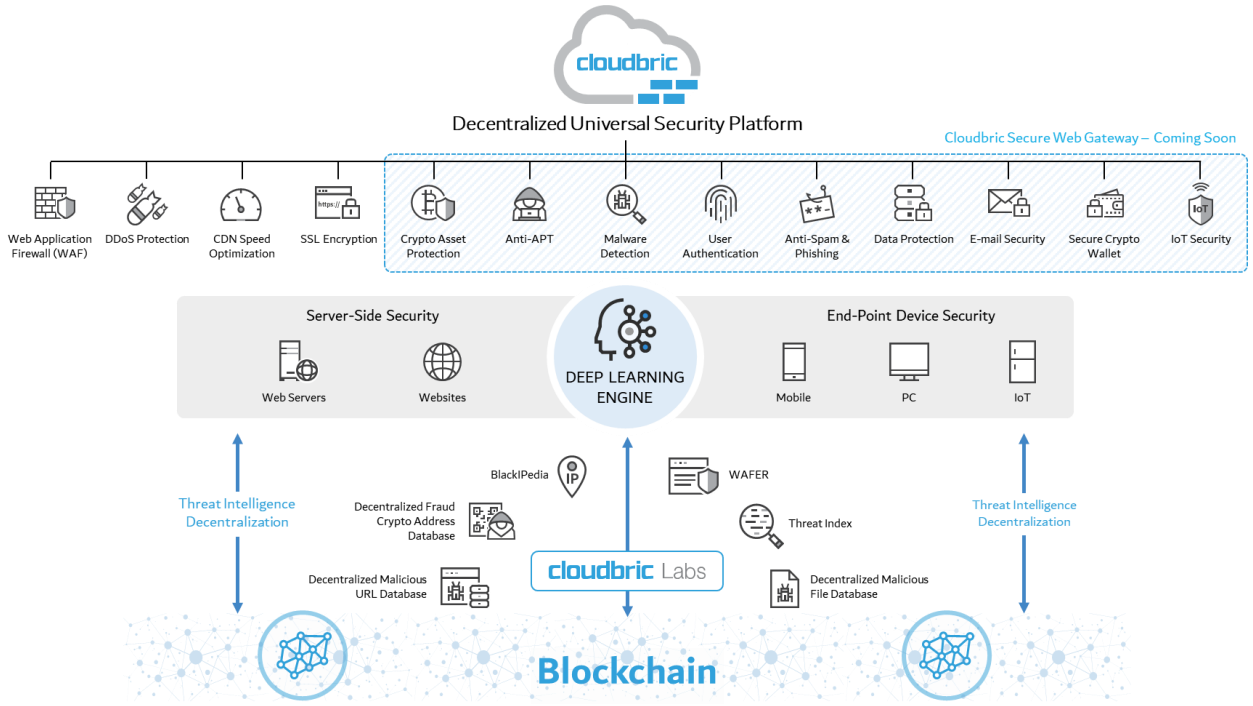
Uncertainty of Security Performance

Lastly, the current organization of the cybersecurity market makes it very difficult to discern the effectiveness of various vendor made solutions. As mentioned above, the market is highly saturated with an excess of information security vendors and solutions. The only way for users to properly distinguish vendor performance is through direct testing of these solutions. However, this can be an extremely resource intensive and costly ordeal.

Users typically need to invest both time and money in order to learn about a particular security solution, measure its respective performance, then decide whether it will be easy to manage and deploy. However, general end users and small businesses may not have the necessary resources and capabilities to test multiple security solutions all at once. This leaves enterprise organizations as the only target audience that can enjoy access to the full spectrum of security that every user needs.

Additionally, cybersecurity vendors tend to excessively promote their security capabilities, but many lack industry experience or high performance working products to become a trusted security vendor. This is especially true within the ICO arena where many fraudulent companies and vendors with limited security expertise run rampant.

Proposed Solution



Cloudbric's primary mission is to revolutionize the cybersecurity market by making information security open and accessible to all users through the introduction of a new **Decentralized Universal Security Platform.** This AI-based cybersecurity platform will be powered by Cloudbric's patented deep learning module known as VISION and will provide an all-inclusive suite of cybersecurity solutions, as well as the development of a new decentralized security ecosystem.

Furthermore, users will be able to train the very technology that helps protect their online digital assets by contributing anonymous cyber threat logs to advance the accuracy and learning capabilities of Cloudbric's deep learning module. For their continued security contributions, users will be rewarded through the free distribution of Cloudbric cryptocurrency (CLB) tokens directly to their user account.

CLB can then be redeemed to activate Cloudbric's suite of security services. A minimum balance of CLB tokens must be deposited or accumulated within each user account wallet in order to utilize all security services. Additionally, users may utilize CLB to gain access to exclusive offers from Cloudbric's extensive global partnership network known as the Secure Web Alliance.

Security Efficiency

Cloudbric will consolidate multiple security solutions into one unified platform to provide easy to manage cybersecurity for a diverse range of users. Solutions to be offered within the platform will focus on three (3) primary security components: server-side security (websites), end-point security (PC, mobile, and IoT connected devices), and cryptocurrency asset protection (including a secure CLB crypto wallet). This will enable all users to enjoy enterprise level website security, CDN speed optimization, intelligent malware protection, spam/phishing prevention, cryptocurrency fraud protection, and much more.

Data Transparency

All cyber threat information (i.e. malicious IP detection, spam URL listings, fraud crypto addresses, etc.) detected by Cloudbric's security system and deep learning attack recognition algorithm will be made accessible through the development of a decentralized security ecosystem.

The first facet of the new decentralized security ecosystem will revolve around Cloudbric Labs (beta version available at https://labs.cloudbric.com). Cloudbric Labs is an award winning security resource community to make threat intelligence open and accessible to the masses in the form of free-to-use security resources and tools. Cloudbric's goal of decentralizing previously withheld cyber threat information will help spark innovation and widespread awareness for cybersecurity for future developers, organizations, and the general security community.

The second component of the decentralized security ecosystem will focus on the launch of Cloudbric's Security Rewards Program. Users will be empowered to help advance the Cloudbric deep learning engine through anonymous cyber attack log contributions, which will benefit the wider security community. In addition, contributions to Cloudbric's deep learning machine will serve as a decentralized rewards system to incentivize users to adopt cybersecurity best practices. Users will be eligible to participate in the new "Secure to Earn" rewards program and receive free CLB token distributions for their contributions. Distribution of all CLB tokens, as well as user CLB transaction history, will be recorded on the blockchain for open and trusted verification.

User Trust

Cloudbric will look to expand on its security capabilities by developing new user focused technologies and solutions to help empower the security community and usher in the next evolution of cybersecurity. With over 30 years of cumulative cybersecurity experience, the Cloudbric team brings a wealth of knowledge and first-hand security service experience to the ICO market. Cloudbric is also unlike any other typical ICO cybersecurity vendor on the market. Cloudbric is also a current award winning and trusted global web security vendor based out of Singapore. To be more specific, Cloudbric's web security technology is recognized as the no. 1 solution in the APAC region and no. 5 in globally rankings by security analysts, such as Gartner and Frost & Sullivan.

Cloudbric Background

In early FY 2015, Cloudbric started as an in-house venture of Penta Security Systems, Inc., the no. 1 enterprise web security and data encryption firm in South Korea and the APAC region. Cloudbric was initially released as a cloud based Security-as-a-Service offering of Penta Security's market leading hardware appliance Web Application Firewall (WAF) known as WAPPLES.

Cloudbric quickly began to carve a strong niche market by targeting small and medium businesses, as well as general website owners, interested in utilizing an all-inclusive WAF solution. Cloudbric's solution helped first time users become more acclimated to the idea of cybersecurity by offering an enterprise level solution that truly catered to their needs.

Establishment of Cloudbric Pte. Ltd.

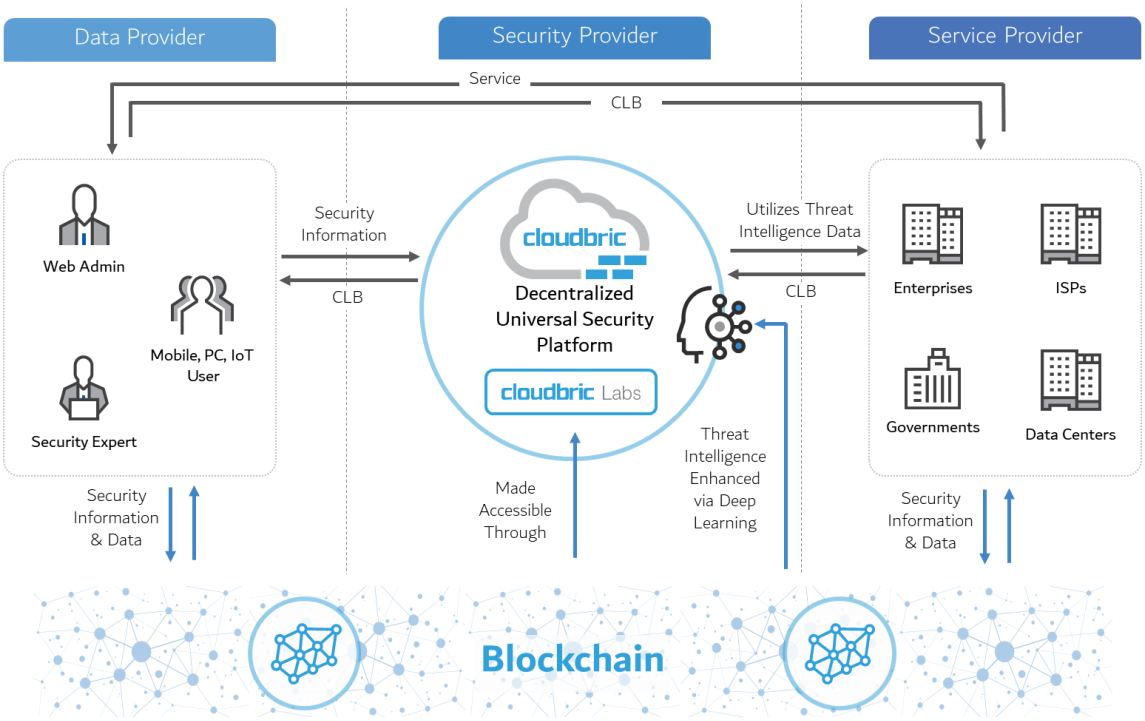
Within two years of operations, Cloudbric experienced considerable growth through sales and user acquisitions. Some notable accomplishments include: opening 25+ international points of presence (POP) or service regions, increasing user base to 10,000 members, and establishing over 50 global partnerships with infrastructure, web hosting, and value added resellers.

Cloudbric's continued success within the small business owner niche market also garnered recognition from industry leading analyst firms, such as Gartner (Magic Quadrant for Web Application Firewalls) and Frost & Sullivan. Cloudbric was also named the **'Best SME Security Solution'** and **'Hot Company in Web Application Firewall'** by SC Magazine Awards Europe and Cyber Defense Magazine, respectively.

In late FY 2017, fueled by Cloudbric's market success, the core executive Cloudbric team decided to create a new company independent from Penta Security Systems, Inc. called Cloudbric Pte. Ltd. This enabled the core Cloudbric team to focus on the development of a patented AI-based deep learning technology specifically designed for Cloudbric cybersecurity.

Cloudbric's goal is to help bridge the gap between cybersecurity and artificial intelligence in order to bring the most advanced user focused suite of security solutions to the market through the launch of a reverse ICO concept in FY 2018.

Reverse ICO Formation



Cloudbric's motivation to launch a reverse ICO is to empower all users to become the primary drivers of decentralized cybersecurity advancement and to become one of the first vendors to provide a suite of cybersecurity solutions powered by AI-based deep learning technology.

The cybersecurity market as a whole is expected to become a $165 billion dollar industry by 2023 with the fastest security adoption rates stemming from the APAC region. Due to Cloudbric's experience and eminence within the APAC security market, Cloudbric will be in a strong position to become a sustained market influencer with the expansion of its decentralized universal security platform.

Furthermore, Cloudbric will look to disrupt the security market by integrating deep learning technology into its core security technology to become the most technologically advanced security vendor in the arena. This will also enable Cloudbric to take advantage of one of the fastest growing technology markets today—the artificial intelligence sector. According to global forecasts, the AI market is expected to reach a size of $191 billion dollars by 2025.

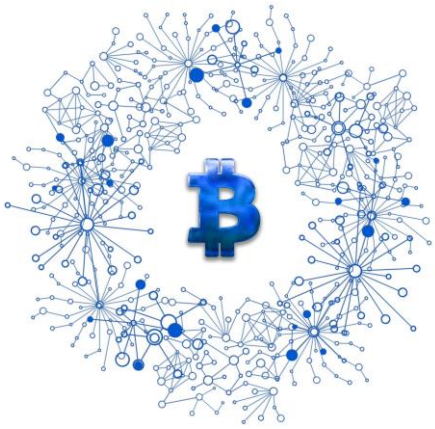
VISION: Deep Learning Technology

Although Cloudbric established its roots as an elite website security vendor, the need to provide a more autonomous and advanced range of data protection services to users helped fuel Cloudbric's plans to develop a new deep learning powered universal security platform.

Cloudbric's deep learning module, VISION, will soon offer the ability to more intelligently detect a new wave of cyber threat attacks targeting various end user devices, systems, and protocols. The integration of deep learning technology into Cloudbric's universal security platform will pave the way for Cloudbric to become one of the most accurate and low false positive rated solutions on the market. Furthermore, deep learning will be at the backbone of Cloudbric's plans to develop a decentralized cybersecurity ecosystem including a user powered security rewards system, cybersecurity resource tools for developers, extensive partnership network featuring complementary solutions and services, etc.

Cloudbric's patented deep learning module, VISION, will be powered by a Convolutional Neural Network (CNN) learning model that extracts patterns of behavior using a diverse set of attack inputs and data. More detailed information regarding Cloudbric's deep learning technology can be found in the technical overview section of the Appendix.

The next phase of Cloudbric's service evolution will come from the development of a new mobile/PC device security client known as the Cloudbric Secure Web Gateway. The Cloudbric Secure Web Gateway will enable all internet connected users to secure their data communications in a variety of ways. For instance, users who download the Cloudbric security client will automatically receive 24/7 real time security against malicious spam/phishing URLs, downloading of malware infected files, e-mail protection, etc.



Additionally, a major benefit of the new Secure Web Gateway client will be a focus on cryptocurrency digital asset protection. It is no secret that the transfer, storage, and access to cryptocurrency assets are vulnerable to hacking attempts. Over the past year or so, hackers were able to successfully steal millions of dollars worth of cryptocurrencies directly from users or trading exchanges.

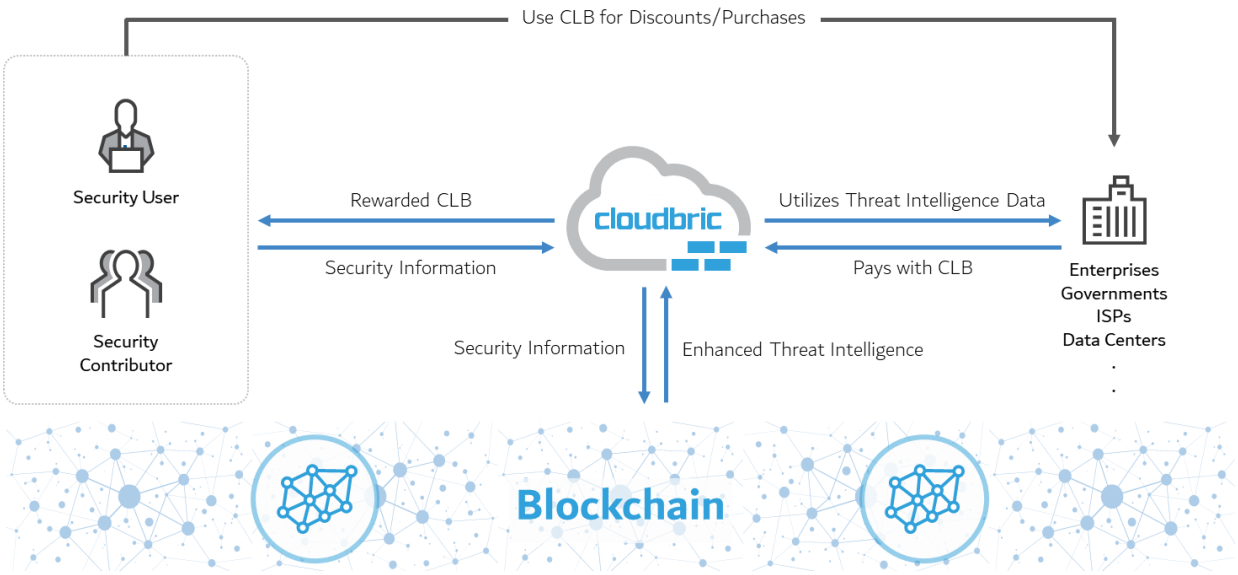
Cloudbric's planned Secure Web Gateway client will allow users who own various cryptocurrency assets to receive real time protection against crypto centric hacking attempts. For example, PCs or mobile devices infected with malicious software, such as CryptoShuffler, can manipulate wallet addresses for users that are looking to transfer cryptocurrencies to their friends and family. The Secure Web Gateway client will be able to identify and prevent the installation of malicious cryptocurrency hijacking software to user devices.

Furthermore, one persistent issue plaguing the cryptocurrency market is the expansion of clone websites that look, feel, and act like authentic cryptocurrency exchanges. Unsuspecting cryptocurrency traders can easily fall prey to these hacking tactics by logging into fake websites with their usernames and passwords. The only way to prevent this issue is to pay particular attention towards the URL address or look for other hacking symptoms that could be very difficult to identify. However, Cloudbric's Secure Web Gateway will automatically recognize and block access to these crypto phishing exchange websites through the power of Cloudbric's deep learning module and decentralized cyber threat intelligence database.

Lastly, users who utilize Cloudbric's upcoming secure cryptocurrency wallet (early FY 2019 development) will be able to enjoy automated protection against transferring digital assets to fraud cryptocurrency addresses. All data concerning fraud crypto wallet addresses, spam crypto URLs, or crypto centric malware infected files will be compiled by the Cloudbric security user community and made accessible on Cloudbric Labs.

In order to activate the Cloudbric end-point security, users will need to download the official Cloudbric Secure Web Gateway desktop client or a mobile application. For technical information regarding Cloudbric's Secure Web Gateway technology, please refer to the Appendix below.

Cloudbric Security Rewards Program



The Cloudbric Security Rewards Program will be a major component of Cloudbric's decentralized security ecosystem. The rewards program will be a blockchain-based compensation system to help incentivize users to participate in the active growth of Cloudbric's deep learning security detection capabilities, which in turn will provide more accurate and advanced security for all Cloudbric users. Users who participate in the Cloudbric Security Rewards Program will be able to automatically train VISION's deep learning capabilities by feeding anonymous Cloudbric generated attack logs back into the deep learning engine itself. This will play an integral role in the increased intelligence, recognition, and learning of the very security technology that protects users from global cyber attacks.

By participating in the Cloudbric Security Rewards Program, users will be eligible to receive complimentary CLB cryptocurrency distributions through two (2) primary contribution methods: Threat Data Contribution and/or Resource Community Contribution.

Method 1: Threat Data Contribution Method

By utilizing any of the solutions available in the Cloudbric universal security platform, users will automatically generate anonymous Cloudbric attack logs based on the attack behaviors detected by Cloudbric's web application security system and deep learning module. Users are given the option to distribute these attack logs by automatically submitting them back into the artificial intelligence engine for increased attack pattern recognition.

Cloudbric will then reward users with free CLB token distributions as a form of compensation for actively contributing towards the growth of the Cloudbric security ecosystem.

All security users who register and utilize Cloudbric security services will automatically be assigned a default CLB distribution rate. The distribution rate of CLB can be compounded, increased, or given bonus subsidies based on a variety of factors. For instance, users can increase CLB rewards by registering multiple websites, email accounts, mobile devices, and PCs directly to their personal Cloudbric universal security dashboard. Bonus CLB distributions will also come in the form of user referrals or length of Cloudbric account registration. Recurring distribution of end user CLB will be made on either a daily, weekly, or monthly basis (to be determined) and will be posted to a distributed blockchain ledger for verification of user distribution.

Method 2: Resource Community Contribution Method

Users who do not wish to utilize the Cloudbric suite of security solutions can still be eligible to receive CLB token distributions through their contribution towards Cloudbric Labs. Cloudbric Labs is a decentralized security resource community with various free security tools, data analytics, and discussion forums made accessible to the public.

Cloudbric Labs is also recognized as the **"Cybersecurity Project of the Year – Gold Winner"** by the Cybersecurity Excellence Awards for its continued efforts in decentralizing threat information as easy to use tools for the security community. A beta version of these tools can be found at the Cloudbric Labs resource page. The three (3) security tools currently available in the Cloudbric Labs community are: BlackIPedia, WAFER, and Threat Index.

- **BlackIPedia** serves as a real time listing of all globally malicious and blacklisted IP addresses detected by the Cloudbric security system.
- **WAFER**, also known as the WAF Evaluator, is a unique tool that allows users to "test hack" any website to gauge their web security performance.
- **Threat Index** serves as a worldwide listing of newly discovered web exploits and vulnerabilities found on the internet.

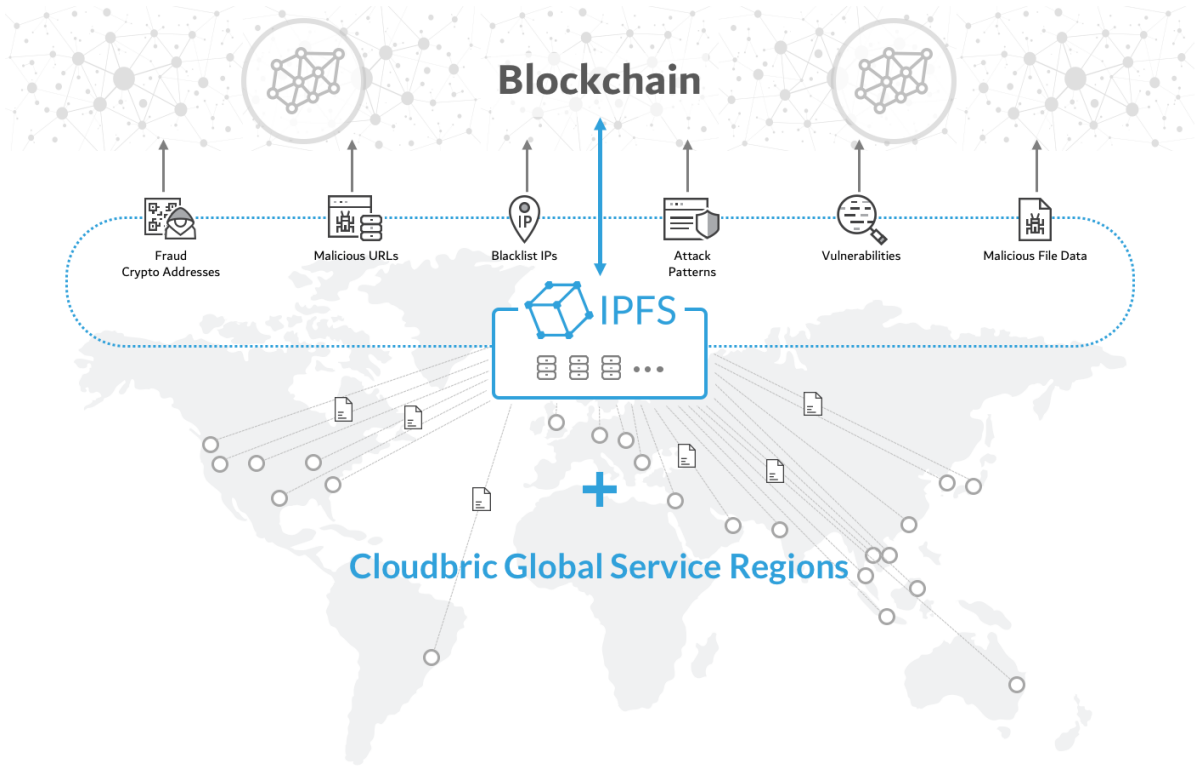
Users will be able to earn free CLB token distributions by contributing new information to the Cloudbric Labs community. For example, security contributors can help provide additional malicious IP information to the BlackIPedia community, suggest new test hacking rulesets or patterns for the WAFER community, or help alert users in the Threat Index community about newly discovered web vulnerabilities that need to be patched. Furthermore, security contributors can also participate in any of the upcoming Cloudbric discussion boards and forums to promote cybersecurity awareness, answer community related questions, etc. for potential CLB token distribution bonuses.

Cloudbric will also work to expand the Cloudbric Labs database by end of FY 2018 to include spam and phishing URL information, malware infected file sources, fraud cryptocurrency wallet addresses, etc. Users will be able to continually contribute this new and emerging threat data information to Cloudbric Labs and become eligible for increased CLB security reward distributions.

It is important to note that no personally identifiable information (PII) is stored or recorded in the Cloudbric generated attack logs. In addition, it is not mandatory for users to participate in the Cloudbric Security Rewards Program. Users who do not wish to have their attack logs distributed into the deep learning module can still enjoy Cloudbric universal security, but will forfeit the right to earn CLB tokens. Attack logs generated by Cloudbric will still be anonymously housed on Cloudbric servers (as per the standard terms of security service) and will be permanently deleted on a bi-annual basis.

Cloudbric will also provide the option for users to utilize a new secure in-house cryptocurrency wallet or have tokens transferred to a wallet of the user's choice. Cloudbric's native cryptocurrency wallet will feature encryption and secure authentication for all Cloudbric users and can be accessed via the Cloudbric universal security dashboard. Users will be able to log into their personal dashboards directly online or through a pending Cloudbric mobile application. Recurring distribution of end user CLB tokens will be made on either a daily, weekly, or monthly basis (to be determined) and will be posted to a distributed blockchain ledger for verification of user distribution.

Decentralization of Threat Intelligence



One of the key aspects of the Cloudbric reverse ICO will be the decentralization of all threat intelligence information onto the blockchain. Cloudbric's universal security platform will compile large amounts of anonymous user generated attack logs for collective transparency and open verification. The goal is to develop the world's largest cyber threat database across various protocols (i.e. web, mobile, and cryptocurrency threats) and to make this information accessible to the general public through the development of new interactive Cloudbric Labs resource tools and custom APIs.

Proposed tools to be added to Cloudbric Labs will center around various user generated decentralized databases, such as malicious URL and file identification and crypto fraud addresses. Users will be able to contribute to these tools by suggesting new malicious downloadable files found on the internet, suspicious phishing URLs that seek to pilfer user account information, and spam cryptocurrency wallet addresses used to trick users online.

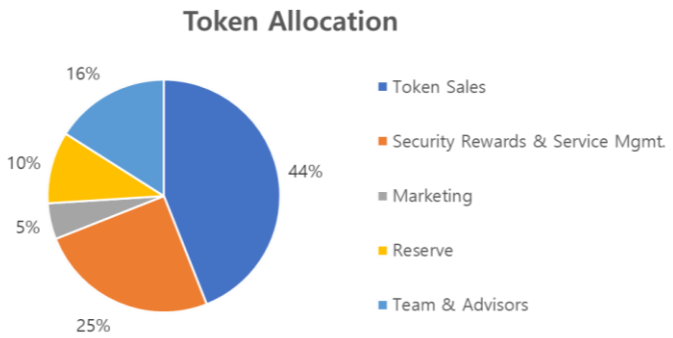
Due to the difficulty in storing vast amounts of data on the blockchain directly, Cloudbric plans to deploy an InterPlanetary File System (IPFS) in order to store and decentralize cyber threat information for public use. The actual threat data compiled by Cloudbric and its users will be housed within Cloudbric's secure global network of data centers (currently 25+ service regions). The hash values of Cloudbric's cyber threat data will be recorded on the blockchain, which will also allow users to openly access and utilize the threat information directly.

Cloudbric's vast network of data center regions will be used as separate IPFS nodes. This will ensure that all cyber threat information housed within Cloudbric's server network will be secured by Cloudbric WAF and will also provide a high speed decentralized database environment. Global users that wish to retrieve this information will be able to tap into the global network of Cloudbric's 25+ server regions to access databases that are closest in proximity to their respective locations. Cloudbric aims to expand its IPFS nodes to over 100 locations around the world by 2020.

All cyber threat information will also be made accessible through multiple interactive security research tools found on Cloudbric Labs. This information will remain free for personal and public use. However, enterprise organizations that wish to directly utilize this threat information for integration into preexisting security platforms or for the development of new security technologies may do so for an additional fee.

Token Distribution Plan

CLB tokens will be available for sales and distribution through both pre-sales and crowd sales events, which will account for 44% of the total CLB supply. Tokens will also be distributed amongst core Cloudbric executive team members and advisors, potential marketing efforts, and the Cloudbric Security Rewards Program.

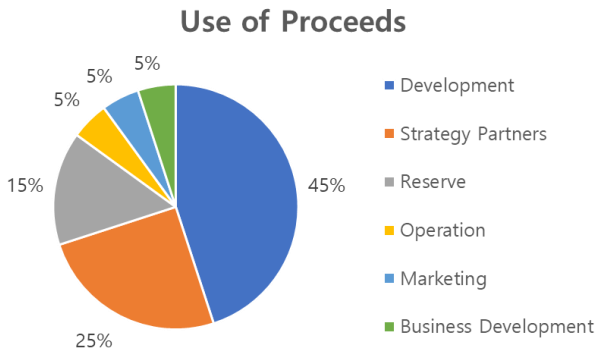


For a more detailed breakdown of CLB token allocation, please refer below:

- Cloudbric will create approximately 1,000,000,000 CLB (1 billion CLB) for maximum supply
- 44% or 440,000,000 CLB (440 million CLB) will be allocated for Token Sales events
- 25% or 250,000,000 CLB (250 million CLB) will be allocated for the Cloudbric Security Rewards Program, as well as additional internal service management or operational costs
- 16% or 160,000,000 CLB (160 million CLB) will be allocated for the core Cloudbric team and advisors
- 10% or 100,000,000 CLB (100 million CLB) will be allocated as an investment reserve (i.e. potential exchange listing, strategic partnerships, etc.)
- 5% or 50,000,000 CLB (50 million CLB) will be allocated for potential short and long term marketing efforts to help promote CLB tokens

Use of Proceeds

Total funds raised from the Cloudbric reverse ICO event will be allocated towards the development and global scalability of Cloudbric. A large portion of these funds will be reinvested for product development, blockchain integration, deep learning data integration, and global infrastructure expansion.



The remaining proceeds will be used to fund marketing, business development, and operational needs of the Cloudbric reverse ICO.

Token Staking & Governance

In order to activate Cloudbric's suite of security services, prospective users will participate in a new token staking program. Users will be required to deposit and maintain a minimum balance of CLB tokens within their respective accounts to gain full access to the universal security platform (i.e. website security, mobile device security, and cryptocurrency asset protection). Failure to maintain the minimum CLB activation balance will result in user accounts being placed on "bypass mode", which will temporarily deactivate all security measures until the minimum balance is restored.

Moreover, Cloudbric will implement a new user governance system in order to promote full decentralization of overall CLB token health and distribution. Users will be empowered to take full control over CLB minimum balance requirements, security rewards distribution rates, etc. via a voting based system. Cloudbric will set the initial minimum balance rates for account activation and security rewards program distributions. Afterwards, Cloudbric will help manage and deploy user voting systems on a quarterly basis to promote full implementation of a user governance ecosystem.

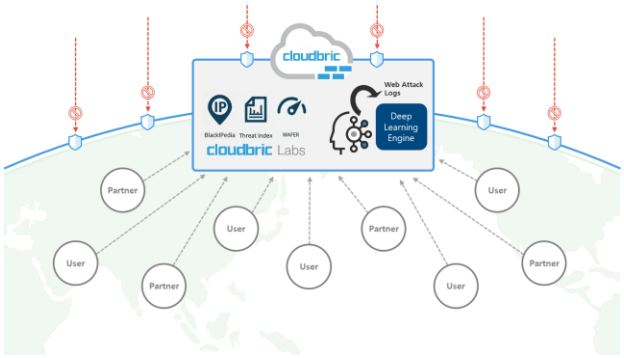
Token Utilization

Enterprise clients and organizations will be subject to paid security plans. However, Cloudbric will offer incentives for enterprise users who purchase their security plans using CLB.

Enterprise clients that purchase monthly service plans using CLB tokens will **automatically receive a 50% discount** on the Cloudbric list price. For those that do not wish to purchase using CLB, they may still choose to proceed with standard payments with a valid credit card or PayPal account.

Secure Web Alliance

The Cloudbric Secure Web Alliance will serve as an additional method for users to utilize their CLB tokens. This alliance will be a global network of partners that protect their businesses using Cloudbric universal security and will provide exclusive offers directly to Cloudbric users through the acceptance of CLB tokens.



Users will be able to access newly updated Secure Web Alliance offers through a Cloudbric Marketplace or directly from the partner website.

Each partner will also be validated with a Secure Web Alliance web seal to be displayed on their company homepage. This will ensure that partnership transactions are secure and denote that a partner is officially licensed to receive payment in CLB tokens. All transactions made using CLB to partners and/or users will be verified and recorded on the blockchain.

Security Development Ecosystem

All decentralized cyber threat information will be made accessible as free-to-use interactive tools and resources on Cloudbric Labs for public use. A beta version of Cloudbric Labs is made available at https://labs.cloudbric.com.

Cloudbric will also look to promote a new security development ecosystem that will encourage complementary service providers, governmental agencies, or security developers to directly utilize Cloudbric's global threat database to create their own proprietary tools and software. This will help promote more widespread innovation, awareness, and adoption of cybersecurity best practices for the community.

Potential service providers can directly utilize Cloudbric Labs data via a custom API, which can be purchased using CLB tokens. Proceeds from enterprise API purchases will be used to replenish the existing Security Rewards token allocation pool for end users.

Appendix

Deep Learning Technical Overview

These days, the technology market is gradually becoming more and more enamored with industry buzzwords, such as artificial intelligence, machine learning, deep learning, etc. Proper utilization and integration of these technologies for specific purposes is an extremely difficult task. However, the benefits and market disrupting capabilities of AI technology is staggering, which is why Cloudbric's research and development team has been focused on developing a patented in-house deep learning engine focused on cybersecurity detection.

Despite having one of the lowest false positive rates for web attack detection in the market, Cloudbric always wondered if there was an even better way to further improve its accuracy rate. Cloudbric also realized that human intervention could sometimes better detect cyber attacks with the naked eye through constant traffic monitoring. However, since it is difficult logistically to expend human capital resources on constantly monitoring online traffic, Cloudbric's research and development team ultimately decided to build one of the world's first deep learning modules specifically designed for intelligent detection and differentiation of online traffic data.

Development History

Cloudbric's deep learning technology was developed by Cloudbric's internal team of machine learning developers and PhD scholars from the Korea Institute of Science & Technology (KAIST), Korea University, and the Massachusetts Institute of Technology (MIT).

In order to properly train the newly developed deep learning module, the team first had to overcome how to feed a deep learning machine with web traffic data. In the past, deep learning machines were successfully designed to accept data in pixels. This made the feeding of image data very convenient since all images are already comprised of thousands of pixels. However, all online requests, communications, and web addresses are presented via a

system of letters and phrases. This left the R&D team with a tough task to repurpose alphabetical characters into a deep learning machine for it to properly conceptualize the data and make sound judgements.

The Cloudbric team came to the conclusion that web traffic must be converted to a more easily digestible form of data for a deep learning machine to grasp. To explain better how the conversion works, each letter and symbol of the various components that make up online traffic was first converted into an image. The deep learning machine was then programmed to discover specific patterns or regularities/irregularities within these corresponding images. From there, the deep learning module was trained to differentiate between patterns found in legitimate and malicious online traffic.

Traffic Conversion

To put this in simpler context, Cloudbric researchers were able to convert a specific pattern of online traffic known as “DBFC” into the image shown below.

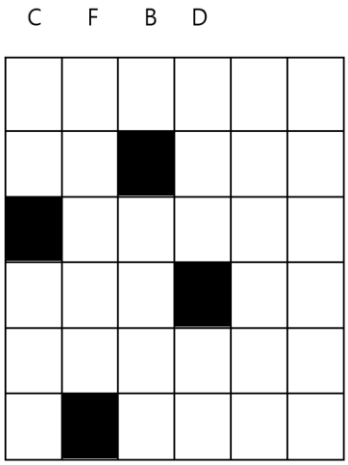


Figure 1: Deep Learning Image Conversion

The deep learning machine would then be trained to find the relation between other images or pieces of online traffic as a benchmark. Afterwards, based on its findings, the machine would accurately decide whether “DBFC” is legitimate traffic or malicious traffic.

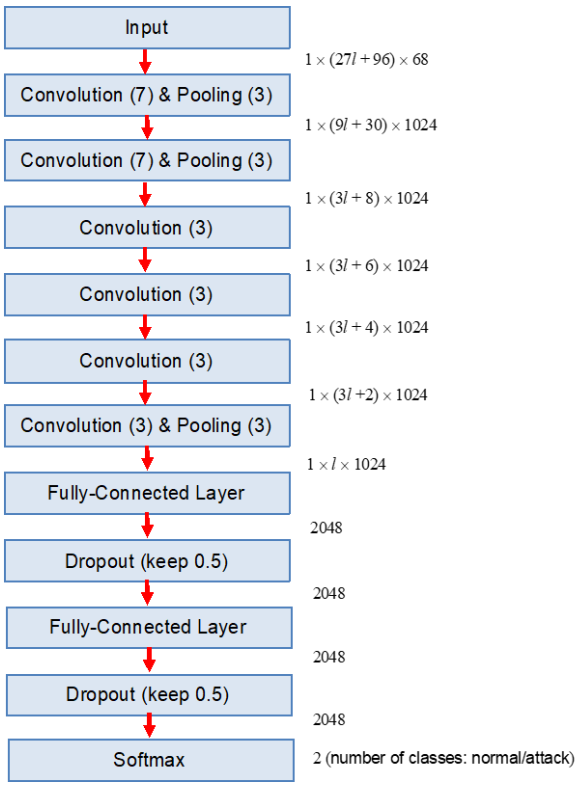


Figure 2: Basic Structure of Cloudbric Deep Learning

At the initial onset of Cloudbric's development, there were a lack of other deep learning modules out in the market that could properly convert characters into sets of distinguished images. Cloudbric was able to accomplish this feat by testing two (2) open source machines based on Convolutional Neural Network (CNN) structures that were apt for this task.

Cloudbric tested both machines and found out that both have their advantages and disadvantages. For instance, one machine would be easier to train, but performed with less accuracy than the second machine. Cloudbric ultimately chose to utilize the faster module for web traffic detection because the latter machine was unable to process the extraordinary number of web traffic logs being updated on a continuous basis.

After the appropriate machine selection, the research and development team ran into another problem. When they tried to apply this machine specifically geared towards web attacks, the team quickly realized that certain characters in attack URLs could not be included in the conventional set of 68 letters (which is recognized by machine). This meant that the Cloudbric team had to find a way for the machine to accept any characters without any restriction due to the fact that web sites could be built in a variety of languages.

This led to the team implementing a patented technology, which helps read cyber attacks in UTF-8 hexadecimal format, and then feed it back into to the deep learning machine. This allowed the deep learning machine to accept any UTF-8 based characters, which eventually enabled the team to train the module geared specifically for web traffic recognition.

Accurate Traffic Detection

In regards to machine accuracy, the Cloudbric team came up with a primitive, yet effective solution known as incremental learning. Instead of having a single machine doing all the work, the Cloudbric team will initially establish four deep learning machines that have each been trained with four weeks worth of cyber attack data. The team would then assign weights to each of these machines depending on their error rates.

Type	Period of Trained Data	Final Result
Machine A	Week 1 to Week 4	$argmax_{c\in\{0,1\}} \sum_{n} W_n \mathbb{1}\{O_n = c\}$
Machine B	Week 2 to Week 5	Where W is defined as...
Machine C	Week 3 to Week 6	$\log \frac{1}{E_n}$
Machine D	Week 4 to Week 7	n = Machine A, B, C, D W = Weight O = Output of machine E = Error rate

The period and the final result above are subject to change depending on the accuracy of the Cloudbric testing results. However, current internal deep learning testing results have shown a stunning 85% accuracy rate increase compared to the standard logic-based Cloudbric Web Application Firewall (WAF) engine. For the sake of comparison, Cloudbric's WAF engine is regarded as one of the lowest false positive rated WAFs in the market by industry analysts.

In summary, Cloudbric had to overcome three (3) main hurdles in order to develop its proprietary deep learning engine – convert web traffic characteristics to pixels, seek efficiency of the chosen machine, and improve machine accuracy standards. The Cloudbric team was able to overcome these obstacles in early 2018, which paved the way

for the integration of Cloudbric's patented deep learning engine, VISION, into all pre-existing and planned Cloudbric security solutions.

End-Point Security Technical Overview

Although Cloudbric plans to expand security servicing for its reverse ICO project, Cloudbric's current Security-as-a-Service only provides server-side security for end users. This includes security solutions, such as WAF, CDN speed optimization, DDoS Protection, SSL encryption, etc., which is mainly used to protect a particular web server and is not applicable for the end-point devices.

The Cloudbric team understands that most general end users rarely interact with a web server, while mobile devices and PCs are part of their daily lives. The cybersecurity market currently does not integrate these two worlds (web security and mobile device security) under a unified solution, which is what Cloudbric hopes to make possible through its reverse ICO venture.

Secure Web Gateway

There are various ways to breach the security of an end-point device. However, by utilizing Cloudbric's extensive resource database and partnering with established end-point security providers, Cloudbric plans to take down each of these security risks and provide a universal platform that will protect all user end-point devices. In addition, the integration of Cloudbric's deep learning engine can be applied to better detect new and unknown malware sources, virus infected files, spam and phishing URLs, etc. This will ultimately be packaged into a consolidated end-point centric client known as Cloudbric's Secure Web Gateway.

The Secure Web Gateway client will be a downloadable client available for both PC and mobile phones. This client will function by automatically enabling Virtual Private Network (VPN) tunneling, which can connect users through Cloudbric's extensive network of service nodes strategically located all around the world.

While Cloudbric already has approximately 25 active service regions open, one key milestone of the Cloudbric reverse ICO will be to exponentially expand these service nodes (open 100+ service regions by 2020) to accommodate speed, stability, and performance from all user regions. The Secure Web Gateway will not only protect end-point devices from day-to-day threats, such as automated prevention of spam/phishing URL site visits, downloading of malware infected files, e-mail scanning protection, etc., but will also ensure the security of user owned cryptocurrency assets.

Cloudbric (CLB) Cryptocurrency Wallet

Security has always been an issue with cryptocurrency wallets. While online wallets are fast and easy to use, all information is transferred via the open internet. These types of wallets only provide one method of user authentication, and even two factor authentication (2FA) enabled wallets are usually done online. This means that a simple packet sniffer could easily gain unauthorized access to these credentials. Cold or hardware crypto wallets try to solve these security issues; however, the inconvenience of the wallet being offline and the possibility of losing the actual device itself is too high of a risk for many people.

Cloudbric will look to develop a more secure cryptocurrency wallet (initial development for early FY 2019) utilizing the backbone of its Secure Web Gateway technology to better store and prevent the risk of unwanted transfers to fraud addresses. The secure Cloudbric CLB crypto wallet will be available on both smartphones and PCs.

In addition, a key feature of the CLB crypto wallet will be the fact that the private key for the wallet will never be revealed. Instead, there will be twelve (12) user authenticated passphrases that would activate the wallet by the user. Once activated, users have the option of setting a secure password or using biometrics to re-access the wallet.

Not only would the CLB wallet be password protected, but mobile devices will also have the advantage of utilizing Fast IDentity Online (FIDO) authentication methods. In addition, the CLB wallet will use end-to-end encryption (E2EE) communications, which means that a stolen data packet would be of little use to a potential cyber criminal.

Lastly, the emergence of crypto asset thefts has left a lasting impression on the entire cryptocurrency market. However, by utilizing Cloudbric's secure CLB wallet, users will be able to deposit, store, and transfer their cryptocurrency with confidence. Cloudbric's Secure Web Gateway client, alongside its deep learning module, will be able to better detect and prevent the transfer of user owned digital assets to fraud cryptocurrency addresses. The database for compiling the list of fraud wallet addresses will also be powered by Cloudbric users from around the world by contributing malicious addresses to Cloudbric Labs as part of Cloudbric's Security Rewards Program.

Threat Database

The mere presence of spam and phishing websites will always be in existence, as long as users have the ability to interact with websites using sensitive information. One would assume that in this day in age, identifying and avoiding spam and phishing websites would be an easy task. However, the sophistication and accuracy of new age counterfeit websites, especially within targeting cryptocurrency users, is reaching a new peak.

Many users are falling prey to scam cryptocurrency exchange websites that look and feel like the original, but with very subtle and hard to spot differences. For instance, these phishing websites replicate a trustworthy website page by page, but may be sourced from an unencrypted protocol (no SSL applied) or could have very subtle character nuances in the address URL. If users are not careful, these scam websites could lead to the cryptocurrency theft or the inability to access one's exchange account.

Conventional solutions do an adequate job of preventing access to spam and phishing websites. For example, users will report the identification of a scam website or email address and browsers/email clients will institute an update to block access to these sources accordingly. However, the diversity of these spam/phishing databases and the slow updating of these databases have always been a problem, especially when hackers launch new attacks.

Cloudbric's decentralized threat intelligence database (compiled by Cloudbric's security system and real time user contributions) plans to become the go-to resource for spam and phishing address prevention. Cloudbric's Secure Web Gateway will utilize this growing database to block access to malicious email phishing attempts and/or scam websites. In addition, Cloudbric will also prevent transfer of funds to fraud cryptocurrency address listed in the decentralized threat intelligence database.

Additionally, cryptocurrency wallet addresses are extremely difficult to memorize as they are a series of arbitrary numbers and characters, which means that most people simply copy and paste respective addresses or use a QR code for fund transfers. Once users download the Cloudbric Secure Web Gateway client, the security client will automatically run a simple check against the threat intelligence database as soon as users copy and paste a recipient cryptocurrency wallet address (for third party wallets). If the outgoing wallet address was reported as malicious or fraudulent by the Cloudbric community, the Secure Web Gateway client will immediately notify the user about the possibility of fraud and prevent the transfer of funds. This will allow the Cloudbric users to have more reassurance that their funds are being protected 24/7 even in the event of human error.

Furthermore, files existing on a personal computer would follow the same logic. Cloudbric's Secure Web Gateway will be able to scan and properly read the binary codes of system files in order to crossmatch with the decentralized threat intelligence database for malware infections. If a malicious file that matches the binary on the decentralized threat intelligence database was downloaded from a particular website or email address, then this information would also in turn be added to Cloudbric's database. All information from Cloudbric's threat intelligence database will be made accessible through Cloudbric Labs as interactive tools and security resources for all users.

Data Protection & User Authentication

Personal information has always been a concern on end-point devices. People typically store valuable information on their computers and mobile phones since they assume that all information on personal devices are safe. This is far from the truth. Information, such as personal contacts, stored passwords, credit card numbers, and even personal vacation or meeting schedules, can easily be exposed once a device connects to the open internet.

As mentioned in earlier, Cloudbric will place a priority on establishing an extensive network of Cloudbric service nodes (data centers) around the world. These service nodes will act as a proxy between end users and the rest of the world. Since the basic concept of the Cloudbric Secure Web Gateway tunneling traffic through a virtual private network, all traffic going in and out of the end user's device will flow through one of these global service nodes.

Each node will monitor all internet connected traffic from a device and allow users to control the type of traffic that flows in and out of their end-point device. This will function the same as the current Cloudbric WAF service, but with more finely tuned standard to meet the security needs of a mobile device.

Resources

1. Gilchrist, Michelle. (2018, January 29). Retrieved from http://www.sandiegouniontribune.com/news/data-watch/sd-me-data-breaches-20180129-story.html
2. Kaspersky. (2017, October 31). Retrieved from https://www.kaspersky.com/blog/cryptoshuffler-bitcoin-stealer/19976/
3. McLean, Asha. (2016, November 23). Retrieved from http://www.zdnet.com/article/security-landscape-plagued-by-too-many-vendors-cisco/
4. Shane, Daniel. (2018, January 29). Retrieved from http://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html
5. Smith, Sarah. (2018, January 23). Retrieved from https://www.prnewswire.com/news-releases/global-cyber-security-market-is-projected-to-reach-a-size-of-1652-billion-by-2023-300587117.html
6. Markets and Markets. (2018, February). Retrieved from https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-market-74851580.html?gclid=EAIaIQobChMI98fK3cXD2wIVxjUrCh1v2wVlEAAYASAAEgK2S_D_BwE
7. X. Zhang and Y. LeCun. (2015). Retrieved from "Text understanding from scratch," arXiv preprint arXiv:1502.01710.