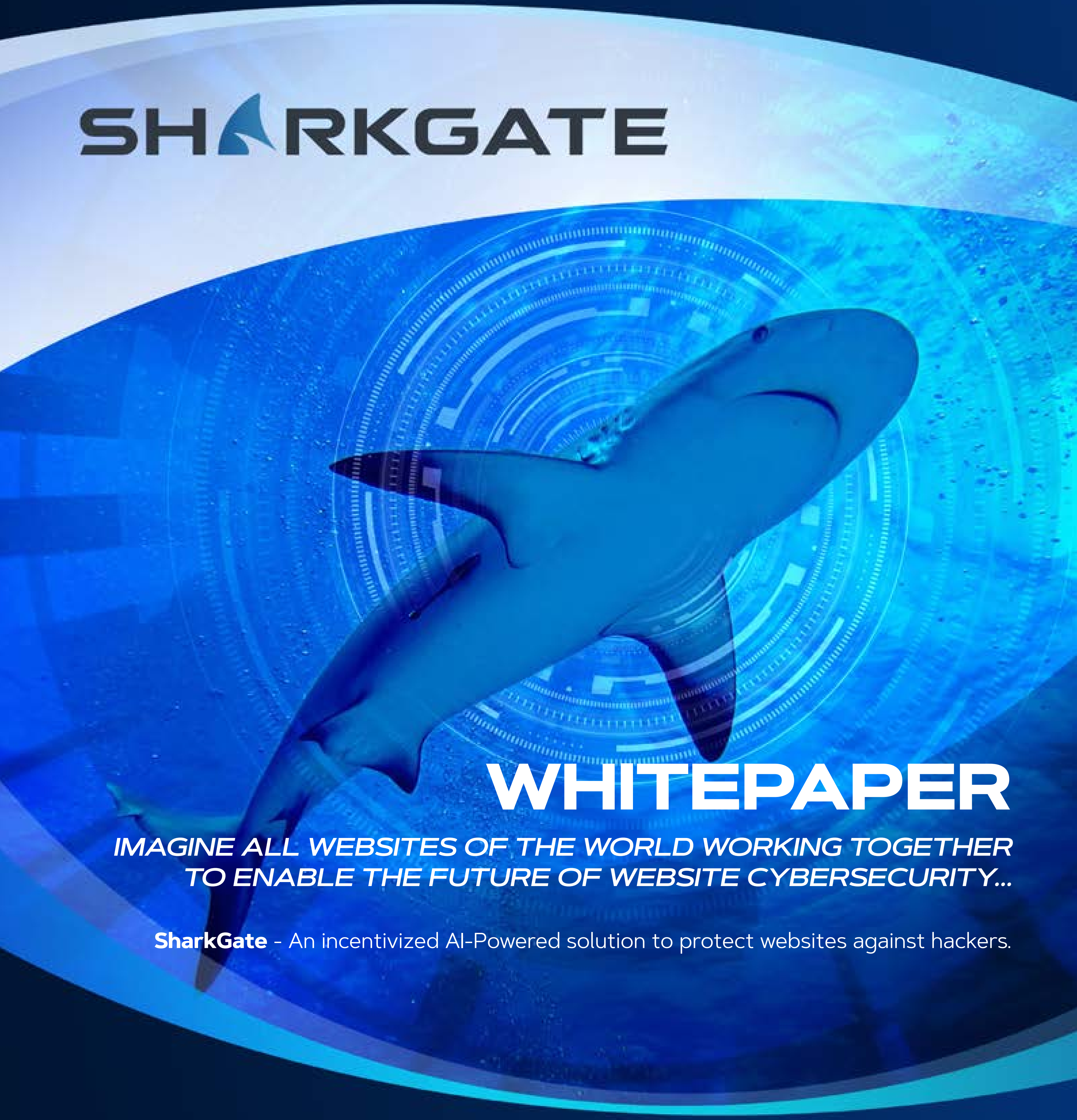
SHARKGATE



WHITEPAPER

IMAGINE ALL WEBSITES OF THE WORLD WORKING TOGETHER TO ENABLE THE FUTURE OF WEBSITE CYBERSECURITY...

SharkGate - An incentivized AI-Powered solution to protect websites against hackers.

www.sharkgate.io

Cyber attacks are the "number one problem with mankind.."

Warren Buffet 2017

There are more than 1.86 billion websites on the internet and around 18, 500, 000 (1%) of these are infected with malware at a given time each week; It is predicted that by 2021 cybercrime will cost the world $6 trillion annually. That's double the $3 trillion tab cybercrime racked up in 2015.

SHARKGATE

TABLE OF CONTENTS

OUR VISION:

“Working Together In Mutual Self-Interest To Protect All The World’s Websites"

SharkGate a UK company that specializes in protecting websites has geared up to build the next-generation of website cyber protection: **SharkGate is creating the World’s first blockchain powered Cyber Security solution designed exclusively to protect websites against hackers.** SharkGate is taking a new approach that will change website security as the industry knows it and make the next-generation of cyber protection available to all websites worldwide.

As former FBI chief Robert Mueller once said: **“There are only two types of companies: those that have been hacked and those that will be”**[1] Unfortunately, this quote is becoming more and more apparent, with thousands of websites being hacked every day and data stolen. The key issue is that threat intelligence data is being gathered but not openly shared for the greater good. The unbelievable irony is that hackers **are** openly sharing their threat intelligence data (e.g. known vulnerabilities, search & exploit scripts, etc) amongst themselves on the dark web.

This current ‘disconnected’, selfishly controlled cybersecurity model simply doesn’t work. Thousands of small businesses are losing their livelihood to hackers that are utilizing the lack of information sharing to their advantage, and getting richer in the process.

SharkGate’s combination of shared cyber attack data integrated with artificial intelligence and the blockchain will provide a community shared threat intelligence database allowing website owners and businesses an infinitely more advanced security solution than currently on offer on the open market. In addition to website owners benefiting from having an infection and hack free website, they will also be incentivized by a tokenomics model to contribute value in terms for witnessed attack data to the distributed network.

Our ‘one-click’ plug-and-play install of a distributed application that protects websites will help us meet our key mission to eliminate existing adoption barriers and create the most advanced community driven threat intelligence system in the industry, easily accessible for all websites.

The SharkGate Ecosystem and the SHKG token will become a new standard used throughout the entire cybersecurity industry to provide website security, privacy and trust. **So, join us in taking back the power from the hackers and instead, giving it to the billions of people whose websites will be contributing to the next generation of website security!**

THE CURRENT CRISIS:
The Hackers are winning!

"It's bows and arrows against the lightning"
- H.G. Wells' War of the Worlds

There is a worldwide crisis for small businesses

In 2016, hackers breached half of all small business websites in the United States, according to the 2016 State of SMB Cybersecurity Report[2]. In 2017 cybercrime leapt to be the second most reported economic crime[3]. The number of cyberattacks doubled in 2017, with ransomware leading the way. That's according to the Online Trust Alliance (OTA)[4], which has named 2017 "the worst year ever in data breaches and cyber-incidents around the world."

Existing Solutions Are Being Overrun

In the 2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)[5] report SMB's mentioned that at least 80% of exploits and malware have evaded their antivirus solutions. Note also this figure is expected to be on the lower side then the real reality as It takes most business about 197 days to detect a breach on their network[6]. Security threats and attacks against websites are increasing at exponential rates year over year and Cybersecurity products cannot keep up with the distributed global nature of hacker bots attacking websites. Also Cybersecurity positions remain underqualified and understaffed. The number of positions not filled is expected to triple to 3.5 million by the year 2021 [7].

The large money to be gained by hacking sites (Cryptomining, stealing credentials, data mining, ransomware, etc) encourages innovative solutions via hackers using distributed bot networks to attack sites and share vulnerability data and attack scripts. Site owners try to gather info and protect their sites in isolation whilst hackers use large cloud infrastructure (AWS, etc), compromised servers, IOT devices and shared distributed scripts to attack. Hackers even stand on the shoulders of giants such as the Google search engine (via Dorks) to find sites with vulnerabilities they can easily target.

Regardless of size, from the largest corporation site, to a humble blogger website there is currently no incentive or framework to work together to share trusted threat and attack knowledge. There is no possibility they can be rewarded to share data of attacks on their sites and gain extra protection in return and financial rewards for the new protection that can be generated from machine learning on the Big data. **To fight the global threat, websites should be sharing this vital threat intelligence, so contributing to a global self learning firewall to stop the hackers in their tracks.** SharkGate will enable this. All based on a tokenomics model that paves a purely utility-driven path forward towards better protection against the hackers.

The CyberCrime Costs Are Staggering

The universal level of website insecurity and the real costs associated with data breaches and cyber-crime are shocking: "72% of larger businesses reported a cyber incident in the past year and nearly half (47%) of all US firms experiencing two or more". [8]

In a Forbes article, Steve Morgan from CSO Online stated, "From 2013 to 2015 cybercrime costs quadrupled, and it looks like there will be another quadrupling from 2015 to 2019. Juniper Research recently predicted that the rapid digitisation of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015". [9]

The continued increase in cyber crime costs shows no sign that it will slow down any time soon. All organisations are increasing their annual IT security spending at a steady rate. The cost of global ransomware alone (ransomware is just one type of the many website threats) was estimated at $325 million in 2015. But by the end of 2017, this number had already multiplied to $5 billion. Again this growth is only predicted to get worse. By 2020, this should easily quadruple to $12 billion. Actually, it is predicted that by 2021 cybercrime will cost the world $6 trillion annually[10]. That's double the $3 trillion tab cybercrime racked up in 2015.

Lack of compensation or incentive to providers and vendors

Another issue present in the information security market is the lack of transparency over threat data, plus inadequate sharing of attack knowledge among security vendors. By protecting websites, cybersecurity vendors are able to collect vast amounts of emerging cyber threat information, such as attack patterns, script behaviors, malicious hacker fingerprints, malware files, etc. The greater the collected attack information, the higher the probability of firewalls using this information for preventing further attacks. However, threat intelligence data compiled through security servicing is not made accessible for public use or even between security providers, since there's no incentive for vendors to collaborate and create one comprehensive attack database and AI solution.

The existing model in the website security industry means websites are left trying to stand alone like single isolated towers against the hacker storm, whilst security vendors generate large profits from the collected data using it to update in-house solutions and selling industry reports and analytics. It means that the websites that help generate this data are left with little to no compensation and are forced to continue paying for largely inadequate centralized vendor protection solutions.

This uneven centralization of threat data and lack of compensation must come to an end.

A Game Changer Is Needed

- **The only winner in this current status quo is the hackers and large security vendors.**

It is clear that incremental improvements by existing security vendors are not sufficient to secure websites and protect the businesses behind them. It is time for a disruptive solution to radically change the website cybersecurity field forever. We believe that SharkGate is in the unique position to be the catalyst for major change. To use its experience and leading expertise in the field to create a new website protection that decentralizes all site generated attack information to the blockchain. Moving to the situation where an attack on one site in the network enables a global immunity to be immediately developed to protect all sites in the network from the similar attacks. Where a solution does not depend on one solitary party or some paid subscription, but instead about a network of websites who all share in the evolving of the firewall, everybody profits, everybody contributes and actually uses the power of the hackers own attacks against themselves.

MARKET:

The Cyber Security $130B market is ready for disruption

What is the potential?

The website Cyber Security market is ready for disruption

There is no denying there is a desperate need for a new way to protect sites from hackers.

Think about how Google transformed the search economy. Think how Uber and Airbnb transformed their sectors and brought untold easy to customers lives.

SharkGate will do the same thing to Website Cyber Security.

With the currently ongoing pivot to blockchain technology and innovations, we believe that we are witnessing a clear shift that will make the

$130 BILLION

Cyber Security market disrupted

Even a **1%** share of the total market would make SharkGate a leading global company.

At SharkGate with the recent innovative technological innovations and experienced team, we are aiming for much more.

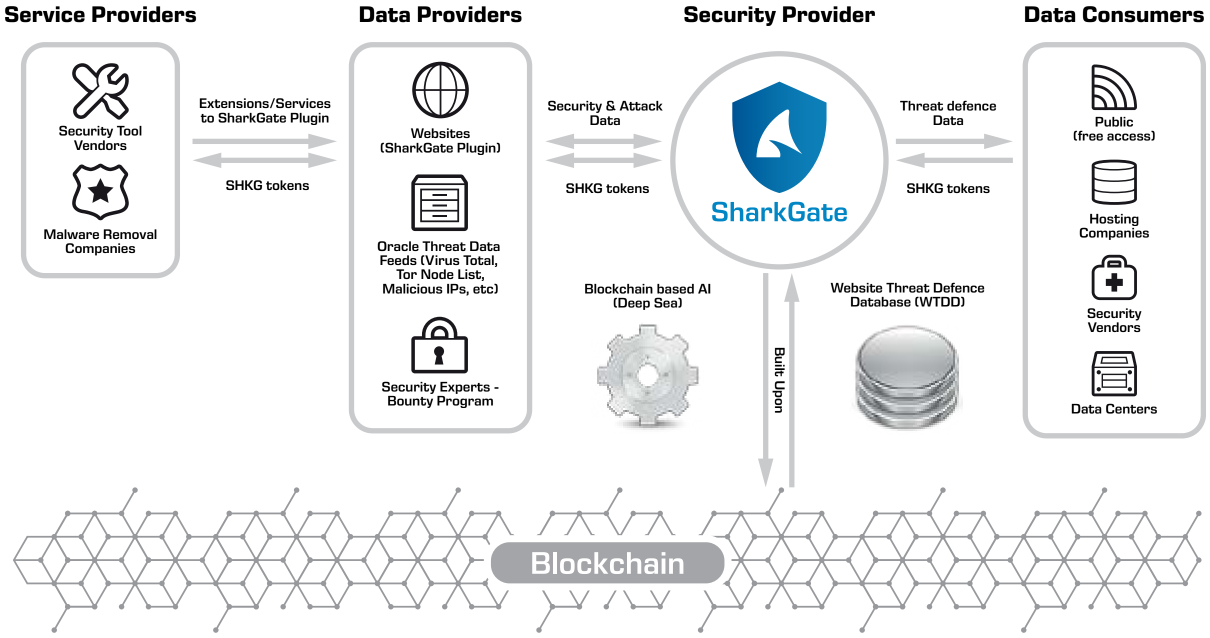
THE SOLUTION:
Technology Overview

"It is truly maddening to see examples of bad guys sharing data, tricks, methods and good guys having no effective way of doing it."
- Anton Chuvakin, research VP at Gartner

Website Cyber Protection powered by collective intelligence

SharkGate's primary mission is to revolutionize the cybersecurity arena by providing an open, intelligent and incentivized website protection system as well as the decentralization of all site attack generated threat information to the blockchain. Furthermore, sites protected by the SharkGate's decentralized ecosystem contribute to its growth and are compensated with cryptocurrency tokens known as SHKG.

SharkGate Ecosystem


Service Providers
Data Providers
Security Provider
Data Consumers
Security Tool Vendors
Malware Removal Companies
Extensions/Services to SharkGate Plugin
SHKG tokens
Websites (SharkGate Plugin)
Oracle Threat Data Feeds (Virus Total, Tor Node List, Malicious IPs, etc)
Security Experts - Bounty Program
Security & Attack Data
SHKG tokens
SharkGate
Threat defence Data
SHKG tokens
Public (free access)
Hosting Companies
Security Vendors
Data Centers
Blockchain based AI (Deep Sea)
Built Upon
Website Threat Defence Database (WTDD)
Blockchain

The SharkGate Ecosystem will protect sites against current and next-generation cyber threats.

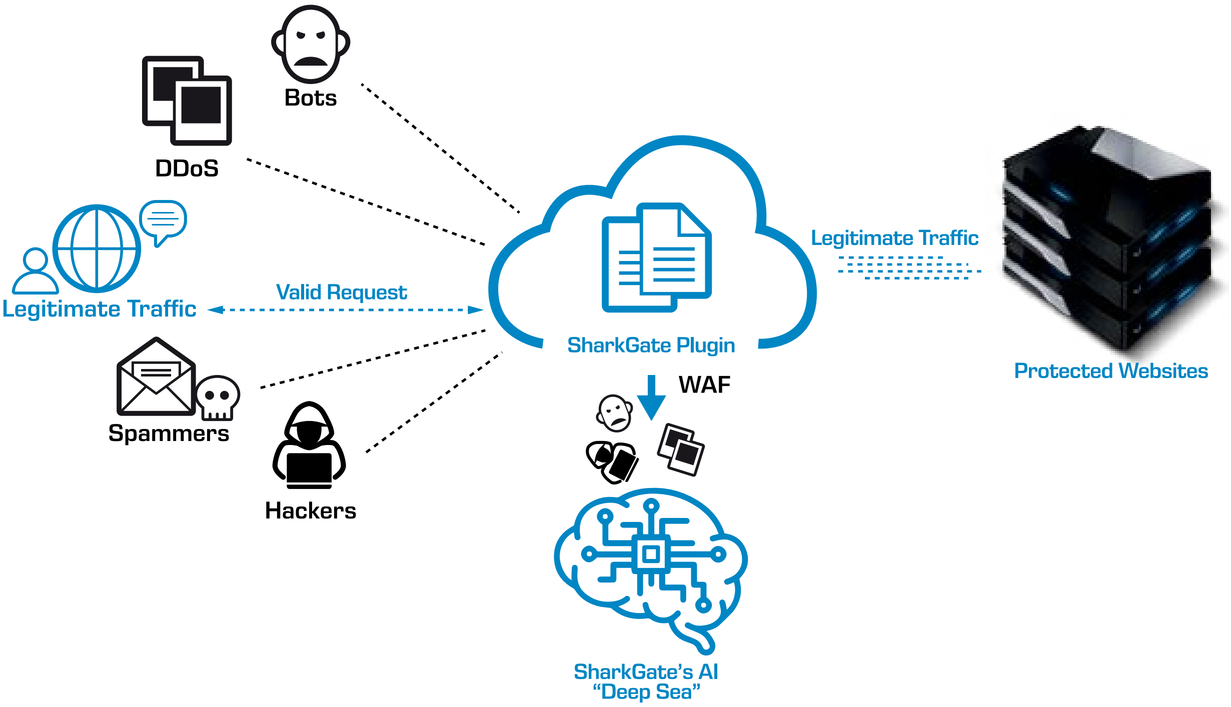
The core components of the Ecosystem are:

1. SharkGate Security Plugin For Websites ("SharkGate Plugin")
2. SharkGate Website Threat Defence Database ("WTDD")
3. SharkGate blockchain-based AI ("Deep Sea");

These 3 components form the basis of our unique approach exclusively dedicated to protecting websites and constantly evolving the ecosystem for website cyber threat protection. This Ecosystem will finally provide the solution to protect websites against current and next-generation threats.

SharkGate Security Plugin For Websites ("SharkGate Plugin")

Hacker Protection, Malware Scanning & Contributing Value To All



The SharkGate plugin is an agent that acts as a websites primary endpoint protection. It identifies and blocks attacks as well as acting as a provider of consolidated attack data and processing power to the Ecosystem.

The SharkGate Plugin is powered by the blockchain using the collective intelligence of the SharkGate AI ("Deep Sea") and the SharkGate Website Threat Defence Database ("WTDD"). It also compliments these by having its own personal AI dedicated to learning and protecting your website. From the moment it is first installed it provides a website with a very high level of hacker protection and then continually grows smarter and better at protecting against attacks as more traffic is analyzed.

As well as providing unrivaled hacker protection the plugin also works as an 'always on' malware scanner, continually monitoring in case any malicious infection is placed on the site. Our experience with the current SharkGate firewall (that is already protecting many thousands of sites Worldwide) is that it is key to still be scanning a site regularly for infection even when it is behind a firewall due to issues such as cross-site contamination. This is when a site is negatively affected by neighboring sites within the same server due to poor isolation on the server or account configuration. Cross-site contamination is one of the greatest contributors to the shared hosting secure or insecure debate.

Simple to Use

The plugin provides a full security dashboard that offers features such as, but not limited to...

- A real-time view giving visibility of all traffic and hack attempts on the site
- Scan results and alerts of any potentially malicious files found
- A Site Uptime monitor
- A Site backup facility (database and files to IPFS)
- A marketplace showing "Extensions" created by 3rd party security vendors that can be enabled to add extra security solutions to the site. Examples would be a security audit tool, reCaptcha, 2FA login, etc. Users are incentivized to rate and review extensions by SHKG tokens provided as rewards to the users for adding value to the network. Extensions can utilize the power of SharkGate ecosystem by accessing the WTDD. Providers must pay SHKG tokens and pass strict consensus tests to be allowed on the marketplace. Providers are rewarded SHKG on the usage of their extensions.

Easy to Install

The endpoint protection for sites is packaged as an easy to install plugin, thus lowering the barrier to entry to protect a site. The plugins will be distributed via all the official plugin directories for each type of website. For example for a Wordpress website, the plugin will be found from the official Wordpress plugin directory and can be easily installed in just a handful of clicks.

Token Model

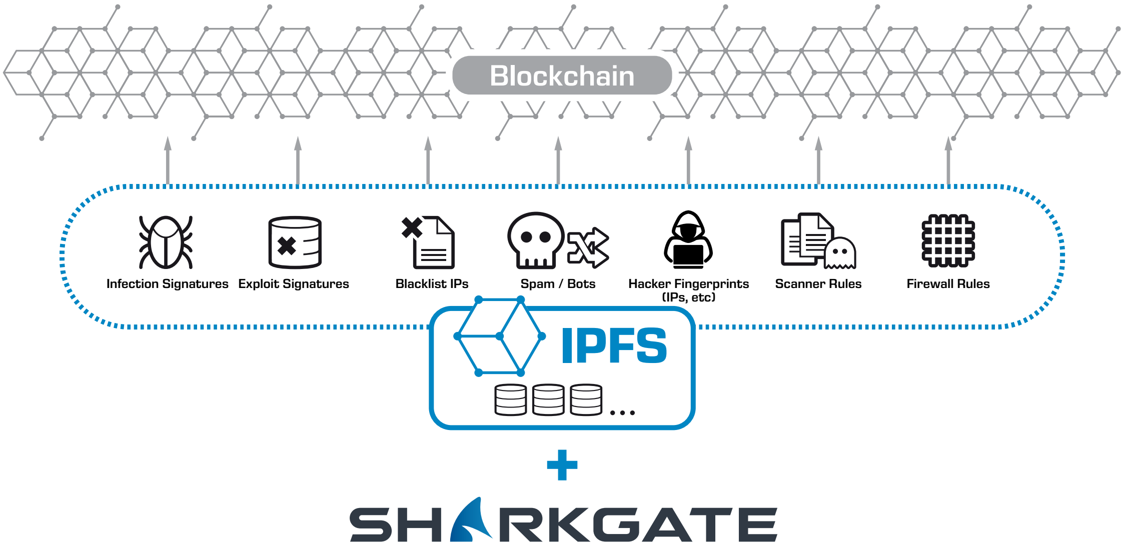
The SharkGate Plugin can be installed as a freemium product. In freemium mode, it has the 24x7 scanning service active, analyses all traffic to the site, performs AI analysis and contributes value to the distributed network by the form of consolidated attack data. So even in freemium mode websites can contribute to the ecosystem and be rewarded in SHKG for the value they create. No personally identifiable information (PII) is sent to the network as all data goes through an anonymization process.

The firewall protection part of the SharkGate Plugin is a monthly subscription based service paid for in SHKG tokens. The use of 3rd party "Extensions" is also paid for using SHKG tokens. Site owners who do not wish to have their anonymized site's attack data distributed into the deep learning SharkGate AI can still enjoy SharkGate website protection, but will forfeit the right to earn SHKG tokens.

A beta release of the plugin will be announced at

https://www.sharkgate.io

SharkGate Website Threat Defence Database (“WTDD”)



The Threat Defence Database (“WTDD”) is an open, decentralized cybersecurity threat intelligence store powered by the blockchain. It becomes more intelligent and robust with each website that joins the network and as more existing threat data feeds and data providers join the ecosystem. We expect the WTDD to eventually become the World’s largest repository of threat intelligence for the security of websites.

Data Usage

WTDD provides data to the rest of the SharkGate ecosystem. With key usages such as..

- A Big Data feed to the SharkGate AI - Vast amounts of data is collected on the distributed network which is then processed by “Deep Sea” building the long-term hacker immunity of the whole SharkGate ecosystem and thus every site protected by it.
- Feed and arm the SharkGate Plugins - The plugins continually receive updates from the WTDD. Updating with the latest firewall rules, malware signatures, hacker fingerprints produced by “Deep Sea”.
- An open repository for universal benefit - A publicly accessible store of threat intelligence solely dedicated to website cyber attacks. Offers programmatic access to the data allowing a fast-moving marketplace for organizations and other security vendors.

Data Privacy

Collected data passes through an anonymization and extraction process to pull relevant attributes that are then normalized and processed before placement in the WTDD.

Data Stores

The WTDD stores a vast amount of relevant threat defense data. The following is some examples of the data stored...

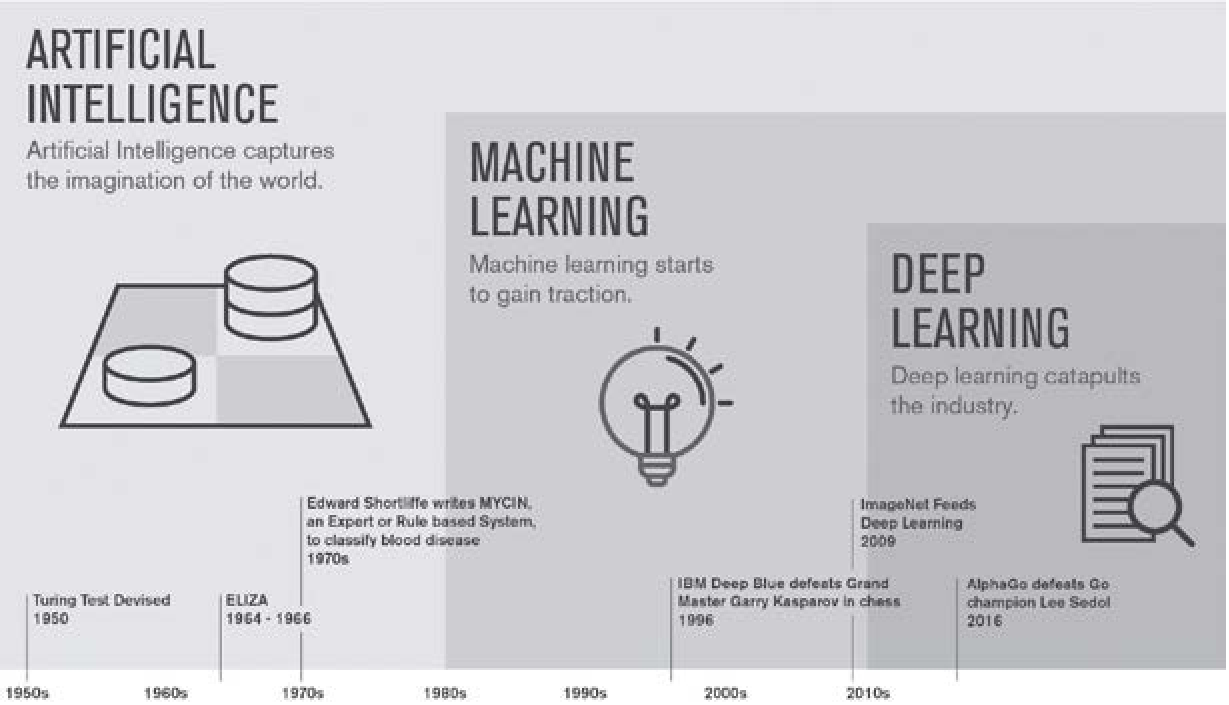
- Firewall Rules
- Malicious IPs
- Hacker Fingerprints (e.g. Agents, referers, networks, etc.)
- Hacker Payloads
- Spam Visitors
- Malicious File Updates (e.g attack shells, file upload scripts, cyrptominers, etc.)
- Scanner Rules
- Infected Plugins
- Infected Themes

Storing vasts amount of data on the blockchain directly is not wise with the current blockchain implementations. So the storage for the WTDD will be the InterPlanetary File System (IPFS) with the hash values stored on the blockchain. Data consumers (websites, AI nodes, etc) will pull the data from the closest sources to their locations.

Data Access

The data stored in the WTDD will be free for personal and public use. However, organizations that wish to utilize this information for their security products and solutions will need to pay a SHKG fee. The marketplace for the paid data provided by WTDD is exclusively powered by SHKG via smart contracts. Access to the collected samples and their attributes will be available programmatically via APIs conforming to industry standard formats (e.g. JSON, etc.) and a set of SDK’s will be created.

SharkGate's Artificial Intelligence ("Deep Sea")


ARTIFICIAL INTELLIGENCE
Artificial Intelligence captures the imagination of the world.
MACHINE LEARNING
Machine learning starts to gain traction.
DEEP LEARNING
Deep learning catapults the industry.
Edward Shortliffe writes MYCIN, an Expert or Rule based System, to classify blood disease 1970s
Turing Test Devised 1950
ELIZA 1964 - 1966
ImageNet Feeds Deep Learning 2009
IBM Deep Blue defeats Grand Master Garry Kasparov in chess 1996
AlphaGo defeats Go champion Lee Sedol 2016
1950s
1960s
1970s
1980s
1990s
2000s
2010s

Big Data… is not Smart Data and so for it to be useful for the ecosystem the SharkGate artificial intelligence named 'Deep Sea' is required.

The HTTP attack requests, hacker fingerprints and malicious files from one website are of incredible value to other websites that want to be protected from such future attacks. The SharkGate Plugins on each site provide this data to the SharkGate ecosystem. This consolidated data combined with existing data from the WTDD is processed by Deep Sea to learn from and improve the 'Distributed Acquired Attack Immunity' of the SharkGate ecosystem and subsequently the protection of every website on the distributed network.

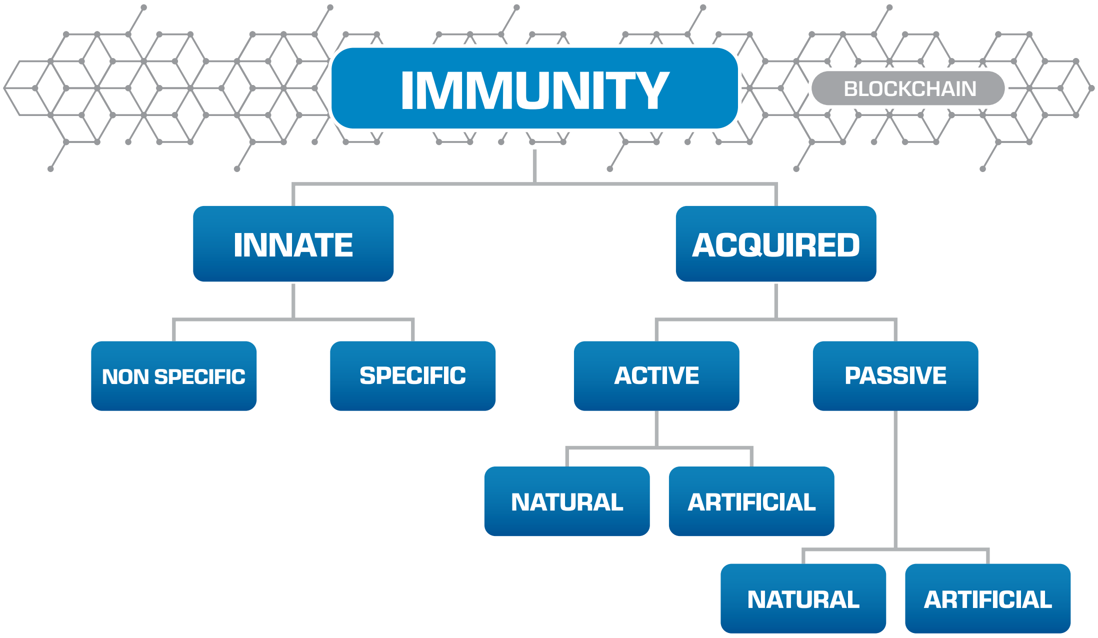
Deep Sea uses distributed consensus when learning from the Big Data and improving protection assets (e.g. threat data classifications, firewall/scanner rules, hacker identifications and markings, score adjustments, known exploits, malicious files, adaptive rules, false positive identifications, malware signatures, etc.)

Deep Sea coordinates the memory of each attack encountered on any site worldwide and thus enables any site on the distributed network to mount a strong response if the attack is attempted again. It also creates 'adaptive' rules that evolve during the lifetime of the blockchain as an adaptation to a threat and prepares protection for future similar, but yet unseen, attacks.

Deep Sea ensures one of the key goals of SharkGate is met. This is that a hacker attacking one website in the world that is part of the decentralised cybersecurity system actually strengthens the hacker protection of every other website on the distributed network.

Note: The term artificial intelligence ("AI") used by SharkGate within the Ecosystem encompasses many fields including machine learning, pattern recognition, deep learning, neural networks, anomaly detection and more.

Deep Sea - Innate & Adaptive (Acquired) Immunity



The self learning protection process of Deep Sea has some analogies to the marvellous human immune system. It uses a system of innate and adaptive (acquired) rules. Acquired rules are produced by 2 types of "Distributed Attack Immunity" called "Artificial" and "Natural".

Rules Types

- Innate Immunity Rules - Rules that require no additional "training" to do their jobs. The plugin continually updates with these rules as they become available. On the first release, these will contain industry standard rules for each type of Website plus thousands of rules developed in-house over the last 4 years by the SharkGate firewall and OneHourSiteFix malware scanner. SharkGate & OneHourSiteFix are already keeping vast amounts of websites clean from infection, so even on release 1.0, these innate rules will provide a very strong protection indeed.

- Adaptive (Acquired) Immunity Rules - Produced by SharkGate Plugin's AI and by the Blockchain AI 'Deep Sea' from contributed data on the network. These rules learn and improve upon exposure to attacks. The advantages of the adaptive rules is that they are able to adapt and protect from new types of attack as they emerge. These rules will be running on all sites from day one, but will not come into full force until they have gained the experience necessary for optimal attack and malware protection. The feedback of these rules to Deep Sea also enables further Innate rules to be created at a later date. Although the formation of global threat memory and experience from these rules occurs 24/7 throughout the life of the blockchain, it is expected the most rapid gain will be in the first years of the chain.

Immunity Creation Types

- Natural (Acquired) Distributed Attack Immunity - This is a long-term active memory that is acquired by 'Deep Sea' based on attacks against any of the websites on the distributed network. With the ecosystem building the collective intelligence from each attack. it means all other sites worldwide are then equipped to mount a strong response if such attacks are detected again. This type of immunity is 'adaptive' because it occurs during the lifetime of the blockchain as an adaptation to attacks and prepares the cybersecurity system for such future challenges.
- Artificially Acquired Distributed Attack Immunity - This is when threat payloads from selected nodes, oracle sources (e.g. external threat database, consensus agreed on attack scripts, etc.) are run against the system for it to learn from and improve the overall immunity. This works in the same way the active immunity of a human body would be generated artificially through vaccination.

The Blockchain and Proof-Of-Shark

We are currently testing the SharkGate ecosystem with the EOS.io™ Blockchain as our primary choice. At its core, EOS is intended to be a highly scalable platform that has been designed to support millions of transactions per second. It allows us to sidestep some very large hurdles that other blockchain solutions are facing in terms of transaction fees and speed. It has also been designed to have closer analogies to a global operating system, thus allowing the quick and easy deployment of distributed applications (Dapps). We are finding that it is greatly simplifying our prototype implementations. We have also been encouraged by the delegated proof-of-stake which helps prevent the formation of mining pools, which in theory, can threaten the security of a blockchain by centralizing resources.

Whilst EOS is a strong contender for the SharkGate system we are not ruling out other options and are also testing alternatives such as Ethereum and Cardano. We live in interesting times and the blockchain situations are very fluid so we will be holding back our public announcement until the beta is release. In the meantime, we will continue our testing with a number of blockchain solutions to help us find the perfect fit for SharkGate. More details will be announced shortly on our website at **https://www.sharkgate.io**

30% of all sites now run on the WordPress CMS

The first version of the SharkGate Plugin is for the Wordpress CMS. Wordpress was chosen as Wordpress sites make up more than 30% of all sites on the internet[11]. It is also the most common type of website targeted by hackers. Shortly after the Wordpress plugin, we will release plugins for other content management systems (CMS) and a general one that works for any website that is not a standard CMS.

SharkGate Bounty Pool For Manual Attack Submissions

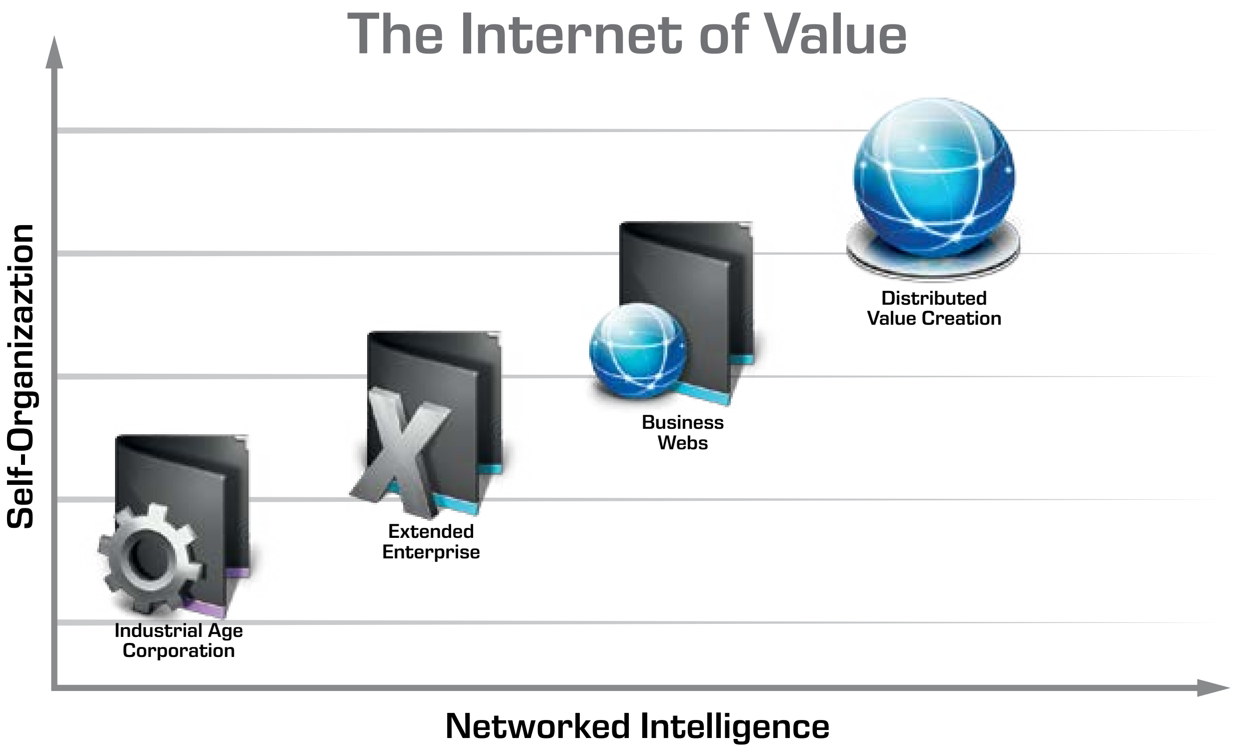
SharkGate will offer a bug bounty program by which individuals can receive recognition and compensation for reporting bugs, exploits and vulnerabilities. The bounty programs main goal is to challenge experts to try to find ways to bypass the SharkGate firewall or evade the SharkGate malware scanner.

The SharkGate ecosystem will provide test ’sandbox’ containers for each type of website (e.g. Wordpress, Joomla, Drupal, custom Java, custom PHP, custom .NET, etc) for experts to download and run against.

Contributors must also provide the remediation (scanner rules in YARA format and firewall rules in ModSecurity format) needed to solve the newly discovered issue. Submissions are automatically checked against the WTDD to ensure they are indeed a new cyber threat and autorun against sandbox implementations to verify the remediation worked and also produced no false positives. The findings from the automatic tests are distributed accordingly to be verified and checked by trusted experts (consensus model). Successful contributors will receive compensation denominated in SHRK (via Smart contracts).

SECURITY REWARDS PROGRAM

All revenue streams in the SharkGate ecosystem are powered by the SHKG token via smart contracts. Goodwill only scales to a certain extent, so the contribution and use of value with SharkGate is incentivized by a tokenomics model for value provided either to or from the ecosystem.



Revenue Stream	Revenue Flow Direction	Details
Websites running the SharkGate Plugin and sending anonymized attack data to WTDD	From the SharkGate Ecosystem to Site owners	Sites running the plugin receive SHKG rewards for contributed value to the network. The SharkGate Plugin analyses all the sites file and the traffic to and from it. It performs AI processing and contributes values to the distributed network in form of consolidated anonymized attack data. This is automatically handled by the plugin and smart contracts. Site owners who do not wish to have their site's attack data distributed into the deep learning SharkGate AI can still enjoy SharkGate website protection and malware scanning, but will forfeit the right to earn SHKG tokens.
Websites running the SharkGate Plugin with the firewall module activated to protect their website from all attacks.	From Site owner to the SharkGate Ecosystem	Via the online interface of the SharkGate Plugin users can pay via SHKG to enable the firewall module that runs 24/7 to blocks any malicious attacks, spam and scraping bots from reaching the website.
API access to the WTDD	From Organisations to the SharkGate Ecosystem	The data in the WTDD will be free for personal and public use. However, organizations will need to pay SHKG tokens to use it for their security solutions. Access to the data will be available programmatically via SDK's for all the leading technologies and APIs conforming to industry standard formats (e.g. JSON)
Bounty pool for manual attack submissions	From the SharkGate Ecosystem to Security Experts	Bounty program by which individuals can receive recognition and compensation for reporting bugs, exploits and vulnerabilities. Contributors and reviewers receive SHKG compensation for value added to the network.
3rd party 'add-ons' to the SharkGate Plugin	Flows from and to the SharkGate Ecosystem, 3rd Party Vendors & Site Owners.	The SharkGate Plugin includes a marketplace page where 3rd party security experts and vendors offer extra security 'add-ons' for websites e.g. a site security audit tool, reCaptcha tools, 2FA logins, etc. As run via the plugin, these tools will be able to use the SharkGate ecosystem to aid their solutions (Deep Sea and WTDD) • 3rd party vendors pay SHKG to have their solutions listed on the marketplace page. • 3rd party vendors receive SHKG for customer usage of their 'add-ons' • Site owners are charged SHKG to use additional 'add-ons' • Site owners receive SHKG for providing feedback (e.g. voting, comments) on the 'add-ons'
Hackers attacking any website on the SharkGate distributed network	Flow from then hackers to the SharkGate Ecosystem	As crazy as it sounds the hackers are part of growing the community as we use their attacks against them. Our 'Deep Sea' AI learns from all attacks improving the 'Distributed Acquired Attack Immunity' of every site using the decentralised cyber security system. This means a hacker attacking one website actually strengthens the hacker protection of every other website on the distributed network. It is seriously awful news for the the bad guys as all the effort they put in gets used against them and makes us Stronger. There is no rewards for the hackers but SharkGate Ecosystem gets rewarded in knowledge gained.

SharkGate's tokenomics model paves a purely utility-driven path for incentivizing all the good guys to join together in mutual self-interest to protect all the world's websites against hackers.

COMPETITION

Web 2: Current Competition

In the current cybersecurity market (Web 2.0) we see only 3 main competitors. From our analysis and also feedback from our customers that have come to us after bad experience with them, we are confident that we are providing better protection, better service and better value for money.

Our keys to success against competition:

1. Best protection in the market. Our firewall and the AI it uses (‘Deep Sea’) is identifying more types of hacks and learning new types of hacks than any competing firewalls.

2. Most complete cleanups of hacked sites. Our in-house built scanners together with our experienced service team are able to find and clean more kinds of hacks than competition and tools are also updated immediately when a new type of hack is identified. We also make sure the site doesn’t break when cleanup is performed, which is not always the case with competitors.

3. Excellent customer service. We have made the customer experience the best in the market, which can be seen e.g. from our Trustpilot reviews. We take care of everything for the customer, don’t require any actions or technical knowledge from them and keep them informed of all steps during cleanup and setting up the firewall.

Web 3: Current Competition

In the decentralized blockchain arena there are less than a handful of possible competitors but upon closer inspection, none of these focus solely on the protection of websites. They all have a more general goal of protecting all internet devices such as phones, personal computers, etc. They are offering a more “jack of all trades master of none” solution which will not solve the crisis for websites especially as hackers use very different attacks against websites than they do for other devices (e.g. phones, laptops, etc).

Summary

Websites behind hacked is a global crisis that cost Worldwide businesses billions of dollars annually. The situation is getting worse every day. Current solutions are unable to stop the flood. Such a massive problem need a major solution and fast ! thus the SharkGate token sale. **For a blockchain powered cybersecurity focussed solely on protecting websites, we are the first and only. We aim to become a household name for website protection. If any business needs their website instantly protected they will think SharkGate.**

CURRENT STATUS & ROADMAP

Since its launch, SharkGate has built a fast-growing firewall and malware removal service for websites. The SharkGate firewall investigates and learns from many millions of requests per day, blocking thousands of attacks every minute 24/7/365. We use an AI platform for stopping attacks and finding malware on websites based on self-learning AI algorithms analyzing every HTTP request. Our service has a very high website owner satisfaction and is currently recommended by a subset of the worlds largest hosting companies. Over the last years, SharkGate has formed an experienced and diverse team of AI and security experts.

The current SharkGate services are centralized using large cloud infrastructures. It is time to pursue a clear roadmap leveraging SharkGate's existing core assets of state-of-the-art AI technology and a great team to bring blockchain powered website hacker protection to the masses and allow each site to be rewarded for contributing value to the whole.

The following roadmap represents relevant ongoing work and to provide significant benefit to the SharkGate ecosystem and achieve the vision of making the internet a safer place to do business.

Q4 2013 to Q1 2014

Ideation & conceptualisation of Version 1 of the SharkGate ecosystem
Detailed research and analysis conducted
Core team built
Advisory board formed

Q2 2014

Security team further assembled
SharkGate Firewall V1 Release to public

Q3 2014

Malware removal service OneHourSiteFix created by SharkGate and released to public
Malware scanner AI created.
Further growth of Security team

Q4 2014 to Q1 - 2017

Massive growth of 7000% in 3 years.
Became one of the top 3 website malware cleaning and protection services.
Released SharkGate firewall version 2 (centralized) to the public. Including:

- Enhanced AI's based on big data analysis and findings
- Thousands of new innate rules
- Adaptive rules that learn and customise for each site

Q3 2017

Genesis - SharkGate version 3 (blockchain powered security).
Initial data gathering, our security experts use data provided by version 2 and learnings from protecting thousands of sites to form the next generation of website security.

Q1 2018

Partnership created for firewall/malware services for one of the largest legal organisations in Europe. Numerous website hosting partnerships for SharkGate version 2 established.

Q2 2018 to Q3 2018

Whitepaper created for SharkGate Verson 3 (blockchain powered security).
Website launch for tokenization of security to solve the worldwide cybersecurity crisis.
Product architecture development and testing..

Q4 2018

R&D integrate Oracle sources feed and start indexing into Website Threat and Attack Database ("WTAD").
R&D developing API integrations to WTAD and testing.
SharkGate version 3 (blockchain powered security) prototype beta test - 10,000 sites.

Q1 2019

FIRST LAUNCH - SharkGate version 3 (blockchain powered security) full launch to Wordpress sites as plugin delivered from the official Wordpress plugin site. Wordpress websites make up more than 30% of the web.

Q2 2019

FULL LAUNCH - SharkGate version 3 (blockchain powered security) plugins available to all CMS's and custom websites. Enabling the ability for SharkGate Version 3 to have protect any website on the internet API now available to WTAD.

Q3 2019

Further Expansion & Global Dominance.
Aggressive marketing in current markets to strengthen the market leader positions.
Attain parternship deals with large hosting solutions. Such as AWS and Rackspace (both currently have no offering for website malware removal, scanning and subsequent protection).
Attain partnership with Google (linked to Google safe browsing). Agreement with Google for sites using SharkGate to obtain score enhancements in search placements in Google search results.

2020 - 2025

Further worldwide expansion,
Become a household name for Cyber protection. If you need your website protected think SharkGate.

Throughout this journey, we'll maintain our focus on the widespread adoption and growth of the SharkGate ecosystem.

COMPANY BACKGROUND

Unlike the majority of cybersecurity vendors on the market, SharkGate is an established and trusted web security vendor based already protecting thousands of websites worldwide. Nearly all hosting companies know of SharkGate and many recommend us to their clients. SharkGate is one of the top 3 website malware removal and protection companies worldwide. Recently it was approached by Comodo Group (**https://www.comodo.com/**) for a potential takeover, which we did not pursue as we felt they did not match our plans.

Our Story – Helping Thousands Of Businesses Worldwide

SharkGate is not your typical tech start-up. It was founded in 2014 by security experts that had spent over 20 years working in IT security for multinational brands including Nokia, Microsoft, Accenture, German Stock Exchange and numerous city banks. The 'light bulb' moment that started it all was the realisation that small businesses were becoming increasingly targeted by hackers, who could make large money from their sites and yet these companies often had no in-house security expertise to deal with them.

So, the idea was simple; create an affordable, robust Cloud-based security platform called SharkGate that anyone with a website could turn on to immediately protect themselves from hackers. Utilising our combined experience and the best of our development and support resources from previous companies, we built the SharkGate product for Web 2.0 and a global service team.

Back in 2014 people did not realise sites needed protection

Unfortunately 4 years ago site owners had no idea of the Cybercrime that was rushing at them. Those days the daily Ransomware and Data Breach headlines had not started to reach the press. Back in 2014, we found that the majority of small business owners don't actually realize they need to protect themselves. In fact, the ones who were turning to our protection for help had already been hacked; thus OneHourSiteFix was born. In some cases, the damage inflicted by hackers could be enough to put a business at risk of going under. So the OneHourSiteFix team set out to make sure they were there as the new Internet's Emergency Team to save businesses from going under because of a hacked website.

Nearly 5 years on and thousands of websites helped

Approaching five years later, and with thousands of customers across four continents, SharkGate has grown rapidly, providing a super fast service for removing all Malware from a website and Cloud-based firewall that then keeps businesses safe from hackers 24/7.

SharkGate's aim has always been to stay one step of the hackers and with this in mind has always used the latest and greatest technologies. With the dawn of Web 3 and the internet of value, SharkGate quickly realised it was time to adjust the structure, technology and products to meet the new World head on. It is time for a disruption.

Transparency & Trust

SharkGate insists on maintaining high standards for operating a transparent business. SharkGate Limited has a certified Pass On Cyber Essentials Scheme (Certificate No: 0201337407389088). Cyber Essentials has been mandatory for suppliers of UK Government contracts which involve handling personal information and providing some ICT products and services. SharkGate Limited is registered under the Data Protection Act with the Information Commissions Office (**www.ico.org.uk**) with registration number ZA108845.

Existing key partners & affiliates

UKFast® YOUR FUTURE IS OUR BUSINESS	HostGator
UKFast is the largest privately owned hosting provider in the UK. A Premium host for Small, Medium and Enterprise Businesses	HostGator is an award winning web host and one of the 10 largest web hosting companies in the world! Located in Houston and Austin, Texas

BOTTOM LINE

"Nothing is more powerful than an idea whose time has come."
Victor Hugo

We have an ambitious plan to protect all the world's websites from hackers by incentivising all sites to work together in mutual self-interest.

Our existing technology is already one step ahead of the competition. With sites working together, utilising the blockchain, we can also ensure cybersecurity always keeps one step ahead of the hackers too.

**We are ready to protect every website in the World.
The cybersecurity market is ready for disruption.
Join us, as with the support of the people we can hit the speed of growth required to address the cybercrime crisis and change the status quo.**