SHARKGATE

WHITEPAPER

WE REVOLUTIONIZE THE WEBSITE CYBERSECURITY INDUSTRY, MAKING THE INTERNET A SAFER PLACE FOR EVERYONE

SharkGate - An incentivized and AI-powered global threat intelligence platform

www.sharkgate.ai

“Cyber attacks are the number one problem with mankind”

Warren Buffett

2 billion websites on the internet

7% (120 million) of all websites are infected by malware.

Cybercrime costs will grow annually by 15%, to $10.5 trillion by 2025.

SHARKGATE

TABLE OF CONTENTS

OUR VISION

“WE ASPIRE TO CREATE A BETTER PROTECTED INTERNET, WHERE ALL WEBSITES WORK COLLECTIVELY TO BUILD A ROBUST CYBERSECURITY INTELLIGENCE NETWORK WHICH IS MUTUALLY BENEFICIAL TO EVERYONE”

SharkGate, a company that has specialized in removing malware and protecting websites for years, has geared up to build the next generation of website cyber protection: **SharkGate is creating one of the World’s largest threat intelligence feeds. An AI-powered Cyber Security solution designed with websites working together in mutual self-interest to fight back against the 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. The key issue is that threat intelligence data is being gathered by government agencies and greedy profit-making security companies but not openly shared for the greater good. The unbelievable irony is that hackers **are** openly sharing their threat intelligence data (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 will provide a 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 of witnessed attack data to SharkGate.

Our plug-and-play installable security 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 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 large corporations and instead, giving it to the millions of people whose websites will be contributing to the next generation of website security!**

THE CURRENT CRISIS

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

There is a worldwide crisis for small businesses

Cyberattacks were the biggest concern for companies globally in 2022, according to the Allianz Risk Barometer. The threat of ransomware attacks, data breaches or major IT outages worries companies even more than business and supply chain disruption, natural disasters or the COVID-19 pandemic, all of which have heavily affected firms in the past year. [1]

Cyberattacks and ransomware have indeed seen a significant increase in frequency and severity in the last few years. Small businesses are attractive targets for cybercriminals because they usually lack the cybersecurity precautions of larger organizations. In fact, 43% of all data breaches involve small and medium-sized businesses and 61% of all SMBs have reported at least one cyber attack during the previous year.[2] The consequences of these breaches can be extremely costly, from lost productivity to company reputation. According to Forbes, 60% of all small businesses victims of a data breach permanently close their doors within six months of the attack.[1]

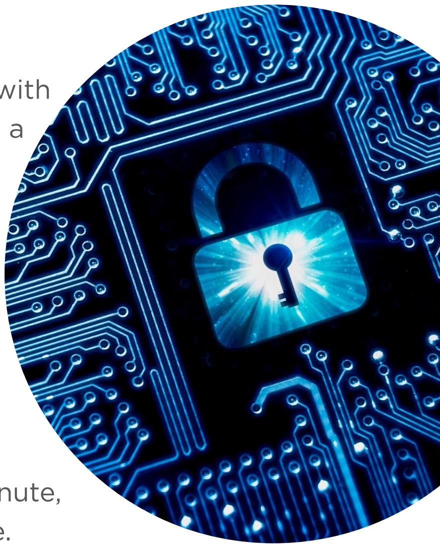
Existing solutions are being overrun

SMB's have reported that about 80% of exploits and malware have evaded their firewalls and antivirus solutions. This is because these solutions fail to protect against zero day attacks (attacks exploiting a new vulnerability introduced in a new version of e.g. a website CMS or plugin). In Q4 2021, zero-day exploits were involved in 66% of malware.[3] It should be noted also that all figures about attacks are expected to be on the lower side than reality as it takes businesses about 279 days in average to detect a breach on their network[4]. Also, cybercrimes are vastly undercounted also because they aren't reported — due to embarrassment, fear of reputational harm, and the notion that law enforcement can't help. Some estimates suggest as few as 10 percent of the total number of cybercrimes committed each year are actually reported.[2] 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 was around 3.5 million in 2021 and the same number is predicted until 2025[5].

The large money to be gained by hacking sites (crypto mining, 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, 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, contributing to a global self-learning firewall to stop the hackers in their tracks.** SharkGate will enable this. All based on an incentive 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: 48% of businesses reported a cyber attack in the year 2022, up from 43% last year.[6]

Cybercrime costs organizations an incredible $1.79M every minute, according to RiskIQ's 2021 Evil Internet Minute Report.[7]

The study, which analyzed the volume of malicious activity on the internet, laid bare the scale and damage of cyber-attacks in the past year, finding that 648 cyber-threats occurred every minute.

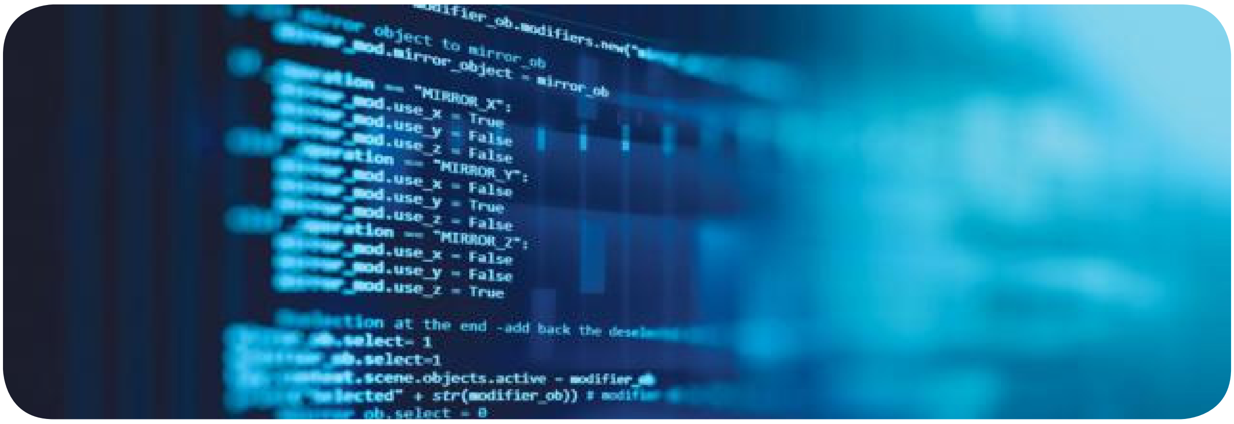
The researchers calculated that the average cost of a breach is $7.2 per minute, while the overall predicted cybersecurity spend is $280,060 every minute.

If it were measured as a country, then cybercrime — which is predicted to inflict damages totaling $6 trillion USD globally in 2022[8] — would be the world's third-largest economy after the U.S. and China.

Research by Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.[2] This represents the greatest transfer of economic wealth in history[9], risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters[5] in a year, and will be more profitable than the global trade of all major illegal drugs combined.[11]

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 winners in this current status quo are 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 a unique position to be the catalyst for a major change. To use its experience and leading expertise in the field to create a new era in website protection and cyber security intelligence services. Moving to the situation where an attack on one site enables a global immunity to be immediately developed to protect all sites in the network from similar attacks. Where a solution does not depend on one solitary party or some paid subscription, but instead a network of websites who all contribute to the evolving of the firewall, everybody profits, and actually uses the power of the hackers' own attacks against themselves.

GLOBAL WEB SECURITY MARKET

The global web application firewall market was valued at USD 5.08 billion in 2021 and is expected to grow at a CAGR of 18.7% and reach at an estimated value of USD 23.21 billion by 2030.[12]

The main driver propelling the global market expansion is the rising significance of online applications. The popularity of WAF solutions is being fueled by the escalating use of IoT and technological advancements. In addition, the market expansion is anticipated to be fueled by increased instances of cybercrime and fraud, as well as strict government regulations governing data security and cyber theft.

Web-based apps and services have also changed the way information is exchanged and delivered in the governmental, corporate, and educational sectors of today. The global market is being depended upon more frequently for more internal information system integration due to the inexpensive availability of information and the range of web services and web-based services, hence driving the growth of the market.

Under exceptional circumstances, the COVID-19 outbreak has increased demand for web application firewall solutions. Many businesses are refocusing their security efforts on endpoint security for work-from-home systems. Additionally, the lack of resources available to enterprise security teams to solve various online application security challenges has increased the need for efficient WAF solutions. [12]

What is the market potential?

There are about 2 billion registered website domains on the internet, and about 25% (500 million) of those are running a live website. Approximately 250,000 new websites are created every day.

The current global market leader in website security is protecting about 20 million websites, which is only about 4% of all live websites.

So even a few percent share of the total potential market would make SharkGate a leading global company. With recent innovative technological innovations and an experienced team, we are aiming for much more.

The $23 billion website cybersecurity market is ready for disruption. There is no denying there is a desperate need for a new way to protect sites from hackers.

Just as Google revolutionized the search economy and Uber and Airbnb transformed their respective sectors, SharkGate is now poised to revolutionize website cybersecurity. With the ongoing shift toward web 3 technology and innovations, SharkGate is bringing unprecedented ease and robust protection to customers' online businesses..

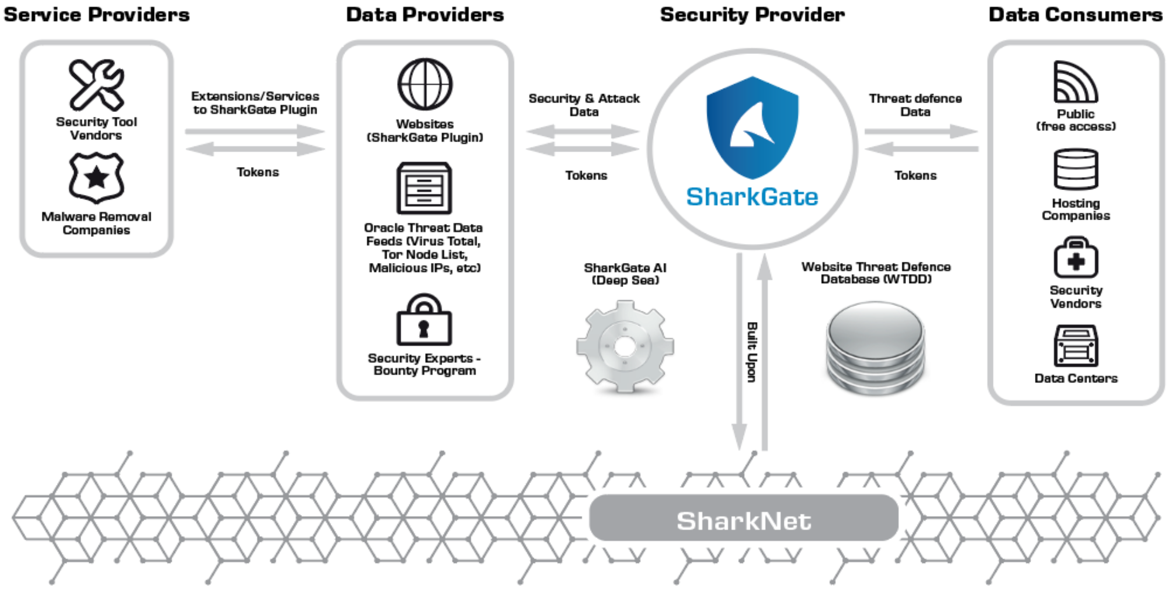
THE SOLUTION - TECHNOLOGY OVERVIEW

> *"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 AI powered threat intelligence using analyzed attack data generated from sites it protects. Furthermore, sites protected by SharkGate's Ecosystem contribute to its growth and are compensated for it.

SharkGate Ecosystem



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

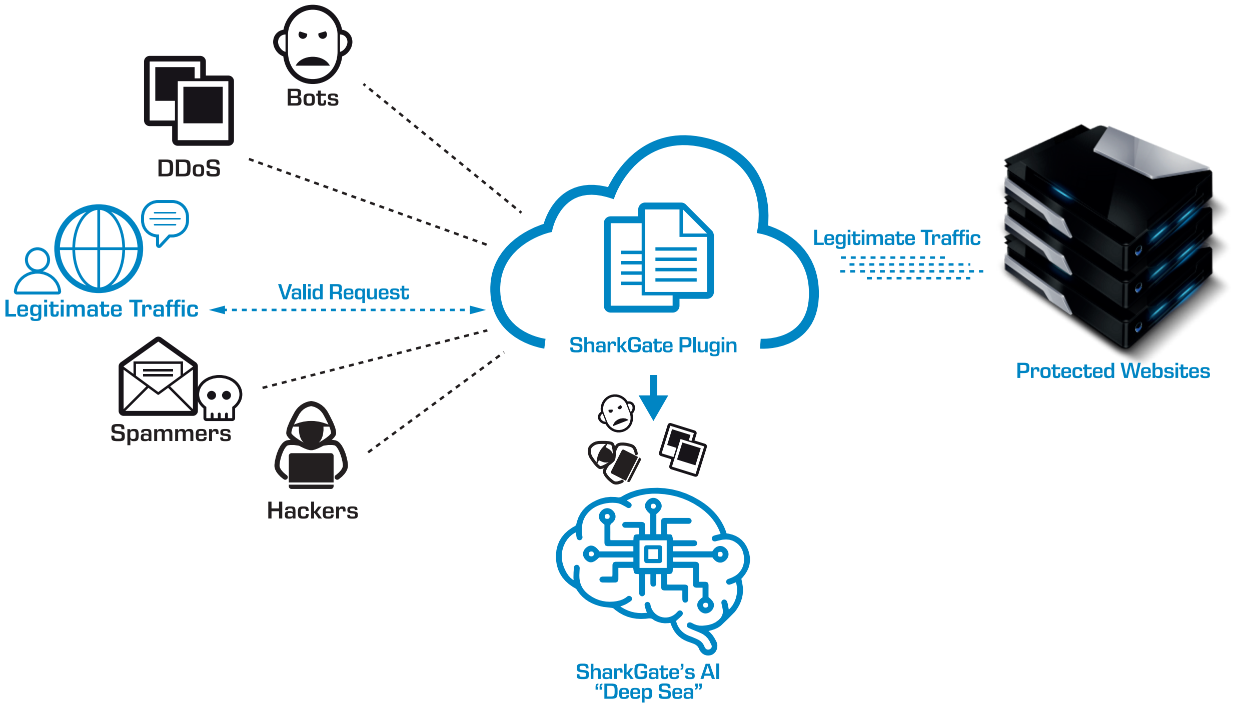
The core components of the Ecosystem are:

1. SharkGate security application for websites ("SharkGate Plugin")
2. SharkGate Website Threat Defense Database ("WTDD")
3. SharkGate 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 application for websites

Hacker Protection, Malware Scanning & Contributing Value To All



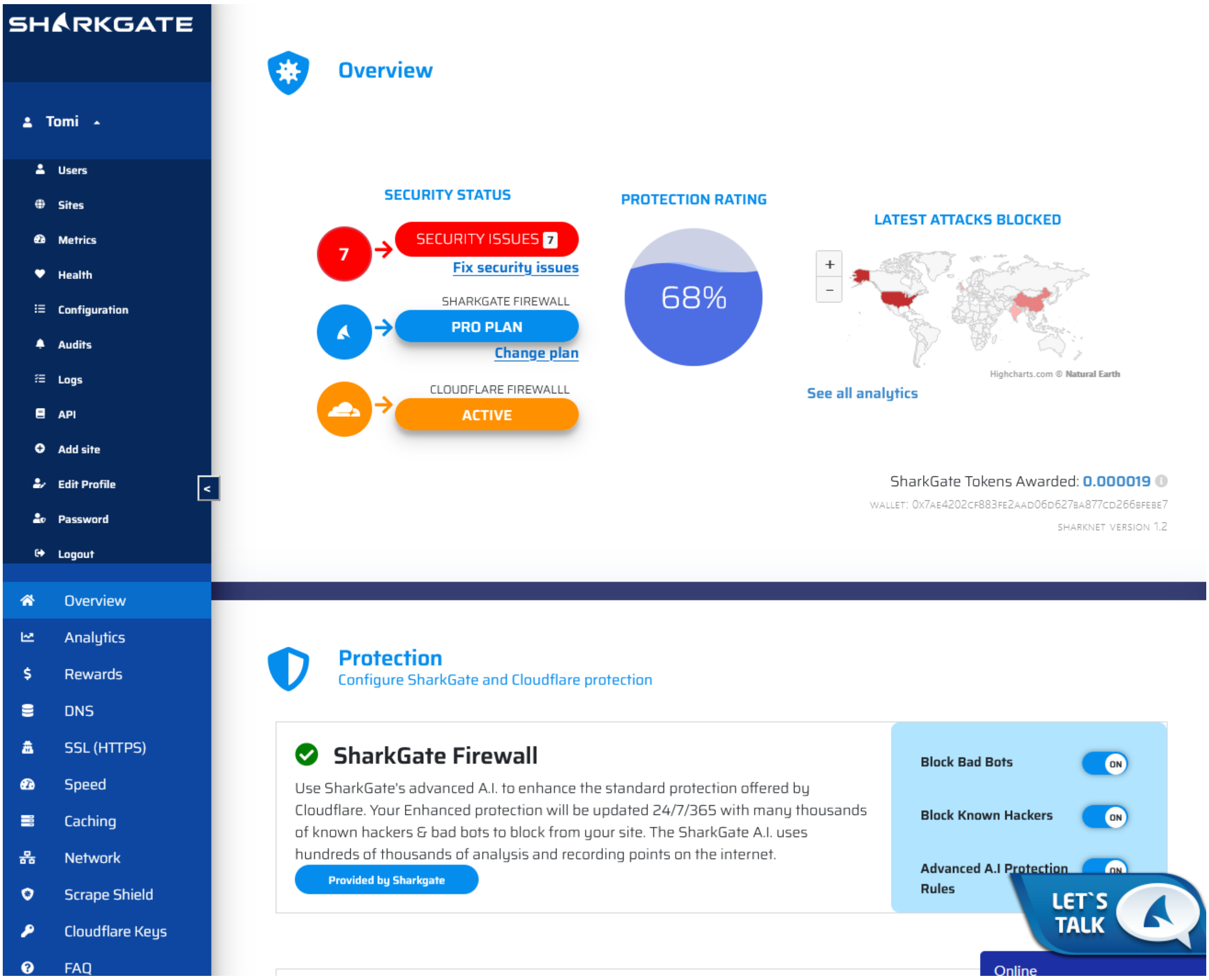
The SharkGate Plugin is an agent that helps identify and block attacks as well as acts as a provider of consolidated attack data and processing power to the Ecosystem.

The SharkGate Plugin is powered by SharkNet using the collective intelligence of the SharkGate AI ("Deep Sea") and the SharkGate Website Threat Defense Database ("WTDD"). 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 identifier, continually monitoring in case any malicious infection is placed on the site. Our experience with the previous SharkGate cloud-based firewall (that has already protected tens of thousands of websites) is that it is key to still be monitoring 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.

Easy to install

The SharkGate 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 all types of websites. Our first version of the plugin is a Cloudflare integrated application giving us an immediate direct sales channel to over 10 million websites.



SharkGate Tokens Awarded: 0.000019

WALLET: 0X7AE4202CF883FE2AAD06D627BA877CD266BFEBE7

SHARKNET VERSION 1.2

SharkGate Firewall

Use SharkGate's advanced A.I. to enhance the standard protection offered by Cloudflare. Your Enhanced protection will be updated 24/7/365 with many thousands of known hackers & bad bots to block from your site. The SharkGate A.I. uses hundreds of thousands of analysis and recording points on the internet.

Block Bad Bots ON

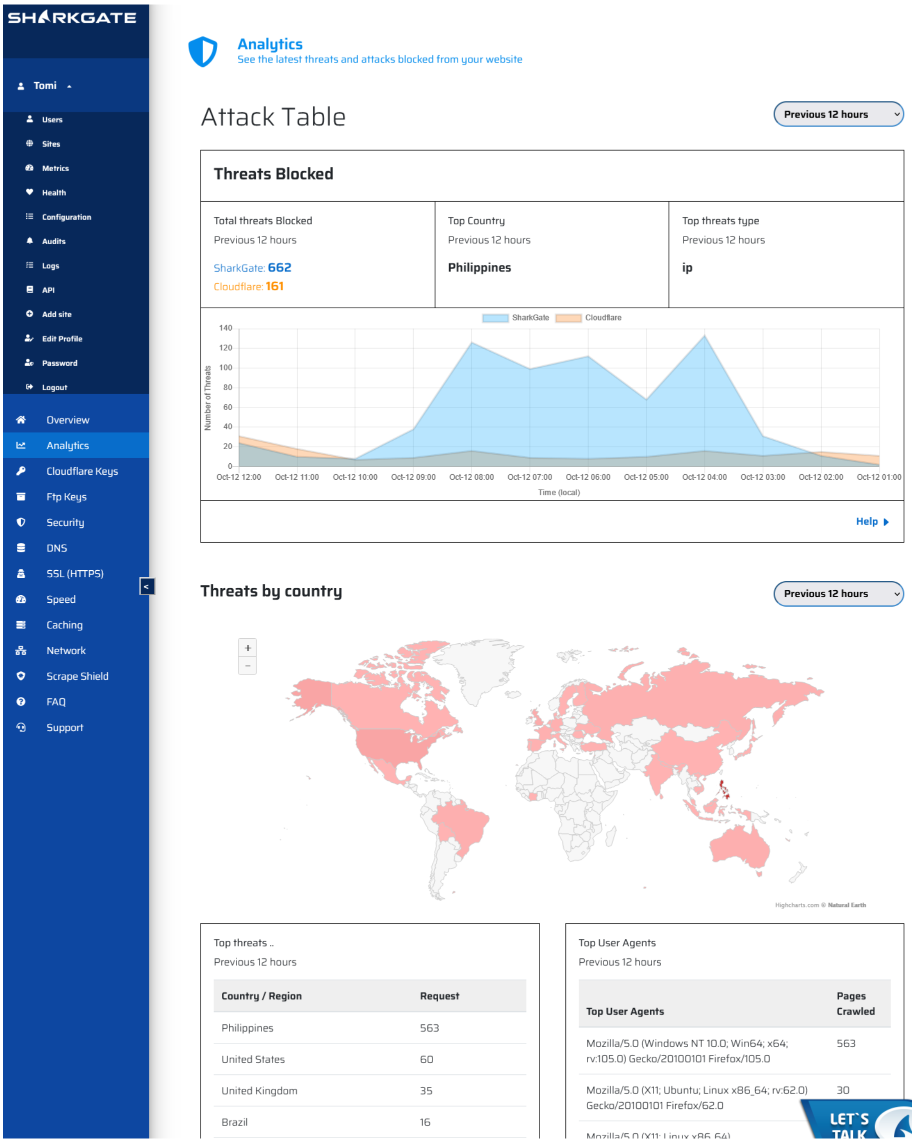
Block Known Hackers ON

Advanced A.I Protection Rules ON

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
- A vulnerability scanner
- 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 for adding value to the network. Extensions can utilize the power of the SharkGate ecosystem by accessing the WTDD. Providers must pay and pass strict consensus tests to be allowed on the marketplace. Providers are rewarded for the usage of their extensions.



Analytics

See the latest threats and attacks blocked from your website

Attack Table

Threats Blocked

Total threats Blocked Previous 12 hours	Top Country Previous 12 hours	Top threats type Previous 12 hours
SharkGate: **662** Cloudflare: **161**	**Philippines**	**ip**

Threats by country

Top threats ..

Previous 12 hours

Country / Region	Request
Philippines	563
United States	60
United Kingdom	35
Brazil	16

Top User Agents

Previous 12 hours

Top User Agents	Pages Crawled
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0	563
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0	30
Mozilla/5.0 (X11; Linux x86_64)	

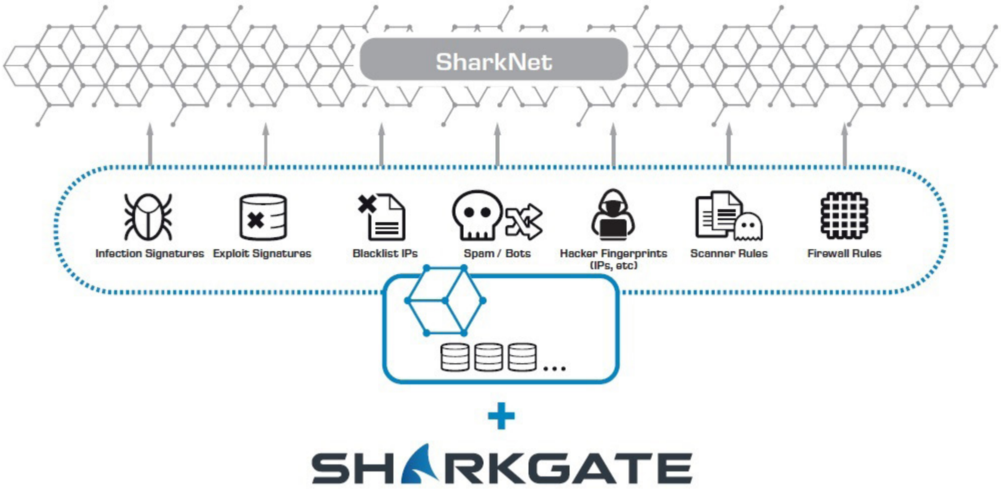
Commercial model

The SharkGate Plugin can be installed on a website and used to protect a site as a FREE product or using a paid monthly subscription for a PREMIUM package (multiple options).

Some differences between the free and premium products:

Feature	Free Version	Premium Version
Website firewall	Yes	Yes
Website firewall protection level	Basic firewall protection rules	Advanced AI protection rules - The latest and greatest full protection.
Number of websites	1	Multiple websites or whole webservers
DDoS protection level	Basic	Advanced
Website security dashboard	Yes	Yes
Automatic security analysis & recommendations	Yes	Yes
File monitor & malware scan	No	Yes
Vulnerability scanner	No	Yes
Support	Community & documentation	24/7 chat + ticket support
Dedicated account manager	No	Yes
Token rewards for contributed value	No	Yes

SHARKGATE WEBSITE THREAT DEFENSE DATABASE ("WTDD")



The Website Threat Defense Database (WTDD) is a cybersecurity threat intelligence store. It becomes more intelligent and robust with each website that joins the network and as more threat 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 to SharkGate's network (SharkNet) which is then processed by "Deep Sea" building the long-term hacker immunity of the whole SharkGate ecosystem and 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, etc. produced by "Deep Sea".
- A repository for universal benefit - A store of threat intelligence solely dedicated to website cyber-attacks. Offers API 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 are some examples of the data stored:

- Firewall rules
- Malicious IP addresses
- Hacker fingerprints (agents, referrers, networks, etc.)
- Hacker payloads
- Spam visitors
- Malicious file updates (attack shells, file upload scripts, crypto miners, etc.)
- Scanner rules
- Infected plugins
- Infected themes

Storage for the WTDD is using a mixture of cloud-based storage and the InterPlanetary File System (IPFS). Data consumers (websites, AI nodes, etc.) pull the data from the closest sources to their locations.

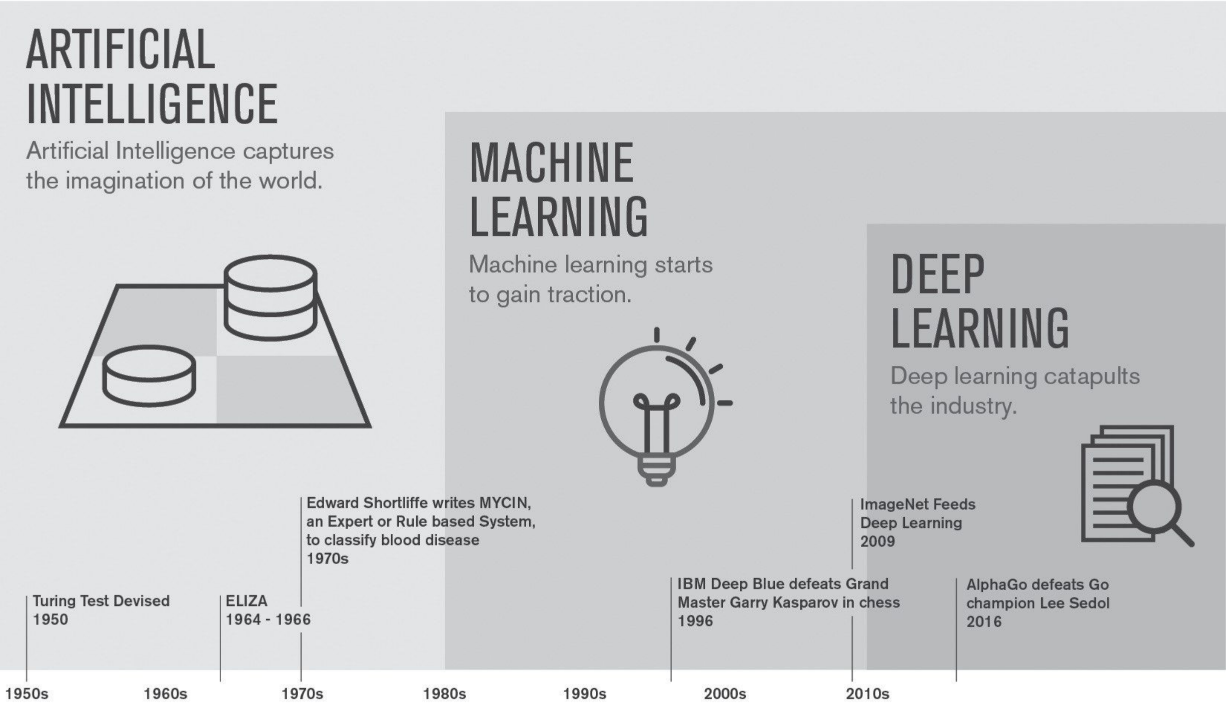
Data distribution

The data stored in the WTDD will be available for security organizations to be utilized in their products and services as a paid monthly subscription. The data is served programmatically via APIs conforming to industry standard formats (JSON, etc.) and a set of SDK’s. SharkGate is also generating a monthly report from the data, which anyone can subscribe to, also as a monthly paid subscription.

Some examples of data provided from the WTDD:

- Attack sources (countries, IP addresses, user agents, bots, etc.)
- Attacked website software (WordPress, Joomla, Drupal, etc.) and their plugins and themes)
- Attack types, ports, protocols, etc.
- Detected vulnerabilities (CMS versions, plugins, themes, etc.)
- Detected malware (files, signatures, patterns, data, referrers, etc.)

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
ImageNet Feeds Deep Learning 2009
IBM Deep Blue defeats Grand Master Garry Kasparov in chess 1996
AlphaGo defeats Go champion Lee Sedol 2016
Turing Test Devised 1950
ELIZA 1964 - 1966
1950s
1960s
1970s
1980s
1990s
2000s
2010s

Big Data is not Smart Data, 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 SharkNet.

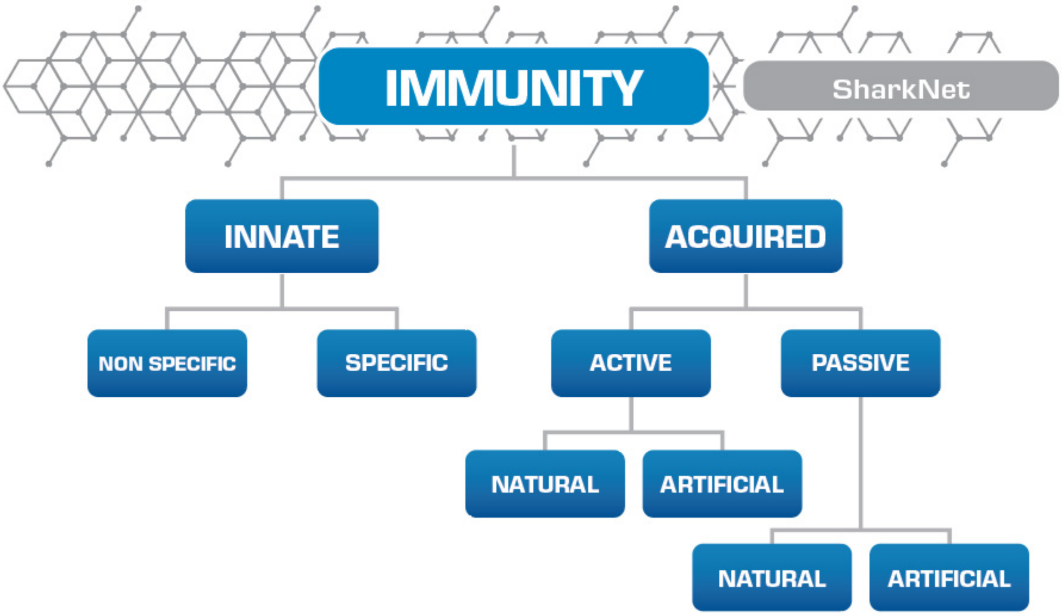
Deep Sea uses distributed consensus when learning from the Big Data and improving protection assets (e.g. threat data classifications, firewall/scanner rules, hacker identifications and markings, score adjustments, known exploits, malicious files, adaptive rules, false positive identifications, malware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

Deep Sea coordinates the memory of each attack encountered on any site worldwide and thus enables any site on SharkNet to mount a strong response if the attack is attempted again. It also creates 'adaptive' rules that evolve during the lifetime of the network 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: A hacker attacking one website in the world that is part of the ecosystem actually strengthens the hacker protection of every other website on the 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 immunity



The self-learning protection process of Deep Sea has some analogies to the marvelous 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".

Rule types

- Innate Immunity Rules - Rules that require no additional "training" to do their jobs. The firewall 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 many years from the data collected by the SharkGate firewall and OneHourSiteFix malware scanner.

SharkGate and OneHourSiteFix are already keeping vast amounts of websites clean from infection, so even in the first release, these innate rules will provide a very strong protection.

- Adaptive (Acquired) Immunity Rules - Produced by the SharkNet AI ‘Deep Sea’ from contributed data on the network. These rules are learned and improved upon exposure to attacks. The advantage 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 network, it is expected the most rapid gain will be in the first years of the chain.

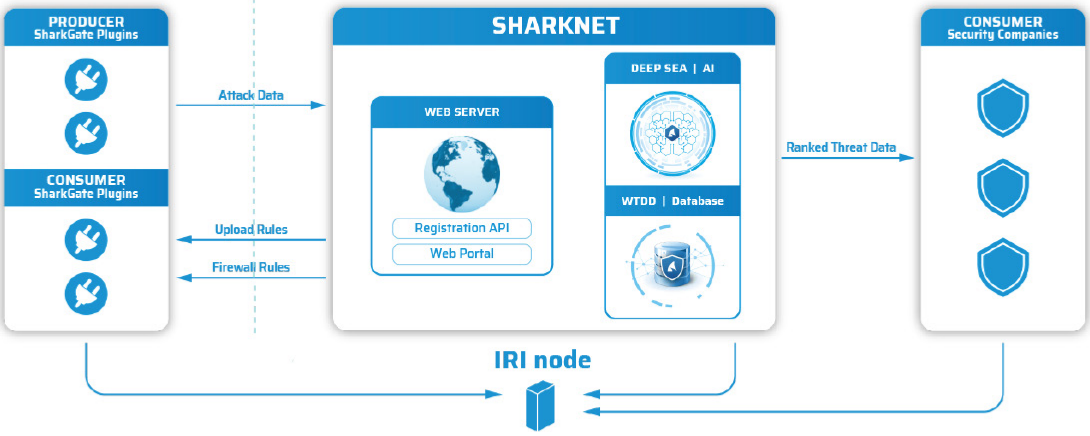
Immunity creation types

- 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 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 system 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.

Key components of SharkGate solution

- SharkNet - The environment where all SharkGate's business logic and data is stored, implemented on cloud-based storage.
- Deep Sea – SharkGate's artificial intelligence system that runs on SharkNet, receives attack data, processes it and distributes updated protection information to consumers.
- Website threat defense database (WTDD) that runs on SharkNet and stores all threat intelligence data.
- SharkGate Plugin – A software installed in front of websites that communicates with SharkNet and protects websites from attacks.

SHARKNET - ARCHITECTURE DIAGRAM

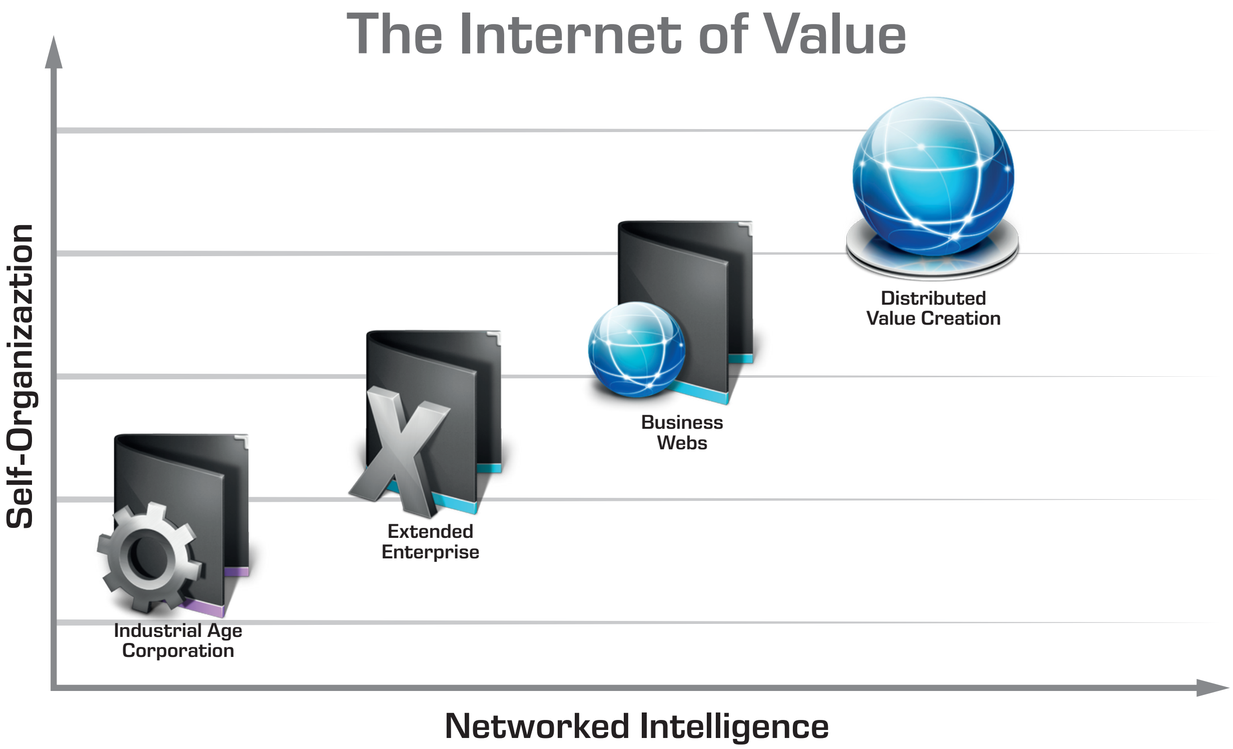


SharkGate bounty pool for manual attack submissions

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

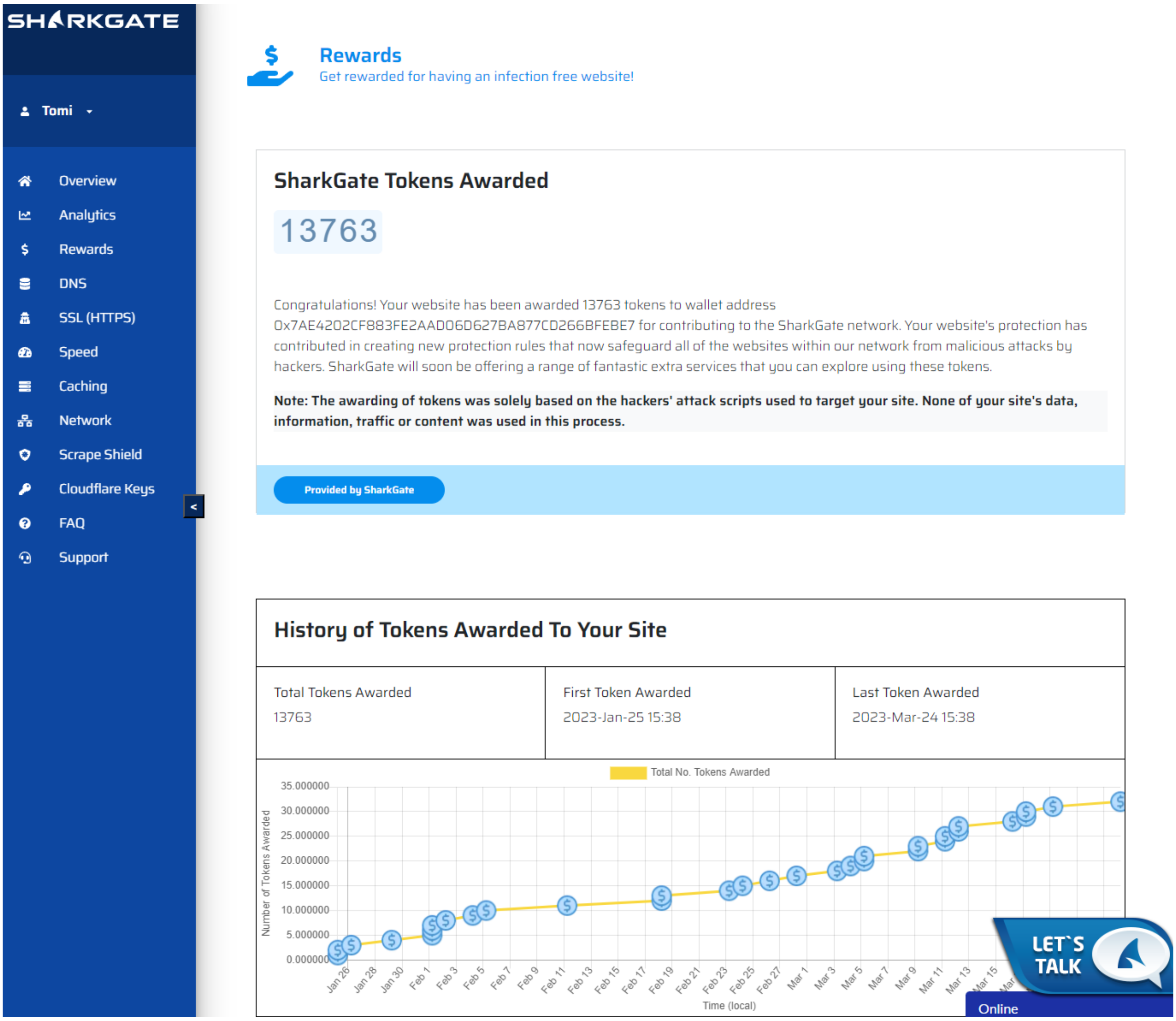
The SharkGate ecosystem will provide test 'sandbox' containers for each type of website (WordPress, Joomla, Drupal, custom Java, custom PHP, custom .NET, etc.) for experts to download and run against.

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 is valid and produces no false positives. The findings from the automatic tests are distributed accordingly to be verified and checked by trusted experts (consensus model). The compensation system of tokens is built on blockchain technology and managed via smart contracts.



REWARDS PROGRAM

All revenue streams in the SharkGate ecosystem are implemented on blockchain technology in the form of 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 to the ecosystem.



Rewards

Get rewarded for having an infection free website!

SharkGate Tokens Awarded

13763

Congratulations! Your website has been awarded 13763 tokens to wallet address 0x7AE4202CF883FE2AAD06D627BA877CD266BFEBE7 for contributing to the SharkGate network. Your website's protection has contributed in creating new protection rules that now safeguard all of the websites within our network from malicious attacks by hackers. SharkGate will soon be offering a range of fantastic extra services that you can explore using these tokens.

Note: The awarding of tokens was solely based on the hackers' attack scripts used to target your site. None of your site's data, information, traffic or content was used in this process.

History of Tokens Awarded To Your Site

Total Tokens Awarded	First Token Awarded	Last Token Awarded
13763	2023-Jan-25 15:38	2023-Mar-24 15:38

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 token rewards for contributing value to the network. The SharkGate Plugin analyses all the sites files and the traffic to and from it. It performs AI processing and contributes value to the 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 token rewards.
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 (also by tokens) to enable the firewall module that runs 24/7 to block any malicious attacks, spam and scraping bots from reaching the website.
API access to the WTDD	From organizations to the SharkGate ecosystem	The data in the WTDD will be available for organizations for their security solutions as a paid service. 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 compensation for value added to the network.
Site/server owners running honeypots to collect and share threat data	From the SharkGate ecosystem to site owners	Anyone running a web server can install and run a threat data honeypot to collect and share threat data to WTDD and earn token rewards.
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 to have their solutions listed on the marketplace page. • 3rd party vendors receive payments for customer usage of their 'add-ons' • Site owners are charged to use additional 'add-ons' • Site owners receive rewards for providing feedback (e.g. voting, comments) on the 'add-ons'
Hackers attacking any website on the SharkGate 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 SharkGate cyber security system. This means a hacker attacking one website actually strengthens the hacker protection of every other website on the network. It is seriously awful news for the bad guys as all the effort they put in gets used against them and makes us stronger. There are 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.

COMPETITIVE ADVANTAGES

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. Fastest, almost instant identification and achieved immunity against new threats that normally get past existing solutions on the market.

3. Unique technology utilizing Web 3 (blockchain), allowing instant machine learning, immunity creation and distribution and a tokenomics model for rewarding site owners.

4. Scalable and easily deployable to many websites or webservers.

5. Easy and almost instant onboarding with no chnages needed on the webserver.

6. Most complete cleanups of hacked sites by OneHourSiteFix.com service which is part of the SharkGate offering. The in-house built scanners together with an 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. OneHourSiteFix also makes sure the site doesn’t break when cleanup is performed, which is not always the case with competitors.

7. Excellent 24/7 customer service and technical support team. OneHourSiteFix has made the customer experience the best in the market, which can be seen e.g. from Trustpilot reviews. The team takes care of everything for the customer, doesn’t require any actions or technical knowledge from them and keep them informed of all steps during cleanup and setting up the SharkGate protection.

Excellent ★★★★★

Rated 4.8 / 5 based on 371 reviews on ★ Trustpilot

FUNDING HISTORY

Background

In 2020, we made a decision to separate OneHourSiteFix and SharkGate into two different companies. Main reason was that a Cyber Security Threat feed using AI powered based processing on data collected from protected websites is a completely new solution, although gaining a lot from our past experience and utilizing the already established brand. SharkGate Plugin and SharkNet Ecosystem are now being developed by SharkGate Oy, a limited company registered in Finland.

Our directors have worked extensively at Nokia in Finland and spent time immersed in the Finnish culture. We find the open honest and straightforwardness of Finnish people a 'breath of fresh air'. Finland has been home to many innovative start-ups and tech companies and has great supporting networks with a great 'startup' mindset. There are great facilities ranging from very fast networks to collaboration spaces and a technically enthusiastic population.

Following the decline of Nokia, the Finnish people have really gritted their teeth and shown 'sisu' by re-inventing themselves and re-invigorating business. The energy and enthusiasm is amazing with many Finnish businesses wanting to help other Finnish businesses succeed. Finland has a huge amount of tech knowledge and the government and banks understand this. There is a large number of business supporting events such as Slush, where people connect and share advice and contacts. We feel businesses are well supported not only at the government, financial and infrastructure level but also within the population and customers.

Finland government funding

Business Finland is a Finnish government organization that provides funding for startups. During 2020 SharkGate Oy has established a good relationship with Business Finland and been granted a first funding step "Tempo funding" in May 2020 and consequently R&D grant in December 2020. After R&D projects the next step with Business Finland would be "Young Innovative Companies" funding that is aimed at technology companies with huge international growth potential.

Private funding

In July 2022 we signed an investment agreement with Revenue Capital. The agreement involves some funding from Revenue Capital to speed up our growth, and also a plan to work together to implement the SharkGate tokenomics and public token sale. This agreement is not exclusive though so we are open for discussions with any other potential investors. Our management team can be contacted for further discussions and more detailed information.

BUSINESS FINLAND

revenue CAPITAL

HISTORY & 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 world's 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 the SharkNet 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 provides significant benefit to the SharkGate ecosystem and achieve the vision of making the internet a safer place to do business.

Q1 2015

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

Q2 2015

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

Q3 2015

Security team further assembled. SharkGate Firewall V1 Release to public.

Q2 2018

Massive growth in 3 years. Became one of the top 3 website malware cleaning and protection services in the world.

Q3 2018

Established as one the World's leading malware cleaning & protection services.

Q4 2018

Obtained partnership for providing security services for one of Europe's largest legal organizations.

Q1 2020

Incorporated SharkGate Oy in Finland and obtained R&D funding from Business Finland to research, design and develop the SharkGate AI, machine learning and blockchain based solution.

Q2 2020

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

Q4 2020

R&D funding from Business Finland

Q2 2021

Product architecture development and testing

Q3 2021

SharkGate Plugin prototype development finished. Internal Beta test with 200 sites executed.

Q1 2022

FIRST LAUNCH - SharkGate Plugin full launch to sites as add-on to Cloudflare.

Q3 2022

Funding agreement with Revenue Capital

Q3 2023

B2B Sales team ramp-up

Q3 2023

SharkGate is the AIBC (Artificial Intelligence & Blockchain) Malta conference pitch winner 2023!

Q2 2024

SharkGate IEO & token rewards public launch

Q3-Q4 2024

Product releases for other platforms (AWS, Google, Azure, Endpoint, etc.)

2024 - 2025

Further Expansion. Aggressive marketing in current markets to strengthen the market leader positions. Utilize external lead generation providers. Attain partnership deals with large hosting companies and web development agencies.

2025 ->

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

COMPANY BACKGROUND

Unlike the majority of cybersecurity start-ups, SharkGate is an established and trusted website security vendor already protecting thousands of websites worldwide. Nearly all hosting companies know of SharkGate and OneHourSiteFix and many recommend us to their clients. SharkGate is one of the top 5 website malware removal and protection companies worldwide.

Our story – Helping thousands of businesses worldwide

SharkGate is not a 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 realization 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 to create an affordable, robust cloud-based security platform called SharkGate that anyone with a website could purchase to immediately protect themselves from hackers. Utilizing our combined experience and the best of our development and support resources from previous projects, we built the SharkGate product for Web 2.0 and a global service team to operate it.

Back in 2014 people did not realize sites needed protection

Unfortunately, 8 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 service 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 10 years on and tens of thousands of websites helped

Ten years later, and with tens of thousands of customers across 95 countries and five continents, SharkGate has grown rapidly, providing an extremely fast service for removing all Malware from a website and a 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 realized 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

We insist on maintaining high standards for operating a transparent business. OneHourSiteFix 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. OneHourSiteFix Limited is registered under the Data Protection Act with the Information Commissions Office (**www.ico.org.uk**) with registration number ZA108845. For our Finland company SharkGate Oy, we are using accounting and auditing services from reputable providers to ensure legal & accounting standards are met.

Our key partners

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
revenue CAPITAL	AEXUS
The World's First Tokenized Revenue Based Ecosystem. Revenue Coin (RVC) holders fund high-tech companies to scale. Startups receiving funding allocate a % of the revenues to the systematic purchase of RVC from the market, reducing supply and increasing value.	Aexus helps innovative tech and software companies extend their reach into Europe, the Americas and Asia Pacific by providing expert sales, business development and inbound marketing services.

FOUNDER TEAM MEMBERS

Marc Roberts - Chief Executive Officer

Co-founder and lead director of SharkGate.
Blockchain and Deep Learning evangelist, serial entrepreneur with numerous successful dot-com startups with a solid 30 year IT history, working for IBM, Nokia and Oracle.
Founder of a popular Threat Analysis Website and Scam Detection System that is now used by millions of users.
https://www.linkedin.com/in/marc-roberts-uk/

Jonathan Morrissey - Chief Technology Officer

Co-founder and lead security specialist of SharkGate.
Certified Architect and Application Developer with over 25 years' experience working on mission-critical and high throughput large-scale systems.
Lead Enterprise Architect for the largest B2B portal in Europe. Formed an IT Service Company that was the sole vendor for development and 24/7 support to Nokia's Global ordering system. The system was deployed to over 150 countries and used as the Ordering and Warranty system for all of Nokia's Mobile phone sales worldwide.
Performed the role of Enterprise Architect & Lead Developer in development teams for companies such as German Stock Exchange, UBS Warburg, Hewlett Packard, Nokia, Accenture, IBM, Metro AG and a Dot Com start-up in Silicon Valley.
https://www.linkedin.com/in/jonathan-morrissey-41760/

Tomi Kervinen - Chief Financial Officer

Co-founder and lead operations & financial director of SharkGate.
A specialist in Big Data, data models, business logic, business consulting and entrepreneurship, with a 25 year long career, which has involved responsibility of mission-critical systems of a blue chip company as well as running the IT development services for smaller clients and startups. Owns a company that provided outsourcing for all of the technical services for Nokia's global B2B portal and eCommerce system. A certified technical consultant in SAP and Oracle with over 25 years of IT project experience, having also worked with other large IT corporations such as IBM, Accenture, Tieto and Fujitsu.
https://www.linkedin.com/in/tomikervinen/

FOUNDER TEAM MEMBERS

Yann Lafargue - Chief Communications Officer

Seasoned international Head of Marketing & Communications with more than 18 years in global agency, local and HQ in-house experience, from start-ups to A-brands in Silicon Valley, Europe and beyond. Entrepreneurial spirit and global brand builder with expertise in digital media, fintech, banking, entertainment, and tech communications working for Banco Santander / PagoNxt, Netflix, TomTom & HK Strategies.

https://www.linkedin.com/in/yann-lafargue/

Matthew Morel - Chief Marketing Officer

Highly experienced Chief Marketing Officer with more than 23 years' experience in professional services, capital markets, FMCG, technology, fintech and telecommunications sectors. A driven and entrepreneurial leader with expertise in building global award-winning and engaging brands that include Deloitte, Bharti Airtel, Vodafone Group plc and Sanne Group plc.

https://www.linkedin.com/in/matthew-morel-028b2314/

REFERENCES

01. https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/

02. https://cybersecurityventures.com/cybersecurity-almanac-2022/

03. https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/

04. https://securethoughts.com/how-long-does-it-take-to-detect-a-cyber-attack/

05. https://cybersecurityventures.com/jobs/

06. https://www.hiscox.co.uk/cyberreadiness

07. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-threat-intelligence

08. https://cybersecurityventures.com/annual-cybercrime-report-2020/

09. https://blogs.cisco.com/financialservices/how-to-prevent-the-bank-robbery-no-one-can-see

10. https://www.forbes.com/sites/rajindertumber/2019/01/05/cyber-attacks-igniting-the-next-recession/

11. https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/attceocyberreport_compressed.pdf

12. https://www.polarismarketresearch.com/industry-analysis/web-application-firewall-market

BOTTOM LINE

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

We have an ambitious plan to build one of the World’s largest cyber intelligence services and protect all the world’s websites from hackers. 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, we can also ensure our cyber security solution always keeps one step ahead of the hackers.

Join our quest!

We will revolutionise the website cybersecurity industry, making the internet a safer place for everyone.

Better protected, collectively smarter, and ultimately stronger together.

We are SharkGate