# Table of Contents

**Status and Challenges of the Industry** ................................................................. 4  
Web Application Facing Heavy Attacks................................................................. 4  
Websites are Defaced............................................................................................... 4  
Leak of Sensitive Information on Websites............................................................ 4  
Trojan Horse Attack ............................................................................................... 4  
Emerging Vulnerabilities lead to High Fix Costs.................................................... 4  
Cybersecurity Law and Regulations Come into Effect............................................ 5  
Bottleneck of Traditional Protection Methods...................................................... 5  
Workload of deployment and maintenance............................................................ 5  
Update of outdated policies.................................................................................... 5

**Product Introduction** ......................................................................................... 5  
Product Overview ................................................................................................... 5  
Prevention Diagram of the Product........................................................................ 6  
Diagram of the Product .......................................................................................... 6  
Protection structure of the product ......................................................................... 6  
WAF Applicable Industries and Scenarios .............................................................. 7  
Public Sectors and Enterprises ............................................................................. 7  
Finance Industry..................................................................................................... 7  
E-commerce ........................................................................................................... 7  
Aviation industry..................................................................................................... 7

**Functions and Features** ....................................................................................... 7  
Monitor and Alert..................................................................................................... 7  
Attack Alarming System ......................................................................................... 8  
Website Availability Monitoring ........................................................................... 8  
Prevention Against Web Application Attacks ....................................................... 9  
HTTP Protocol Validation ...................................................................................... 9  
Prevention Against Injection Attacks .................................................................... 9  
Prevention Against XSS Attacks .......................................................................... 10  
Prevention Against Malicious Scanners and Crawlers ......................................... 10  
Prevention Against Web Trojans .......................................................................... 10  
Authentication and Authorization Protection .......................................................... 11  
Prevention Against Web Framework Attacks ....................................................... 12  
Prevention Against Sensitive Information Leak .................................................. 12  
Self-Learning Protection Engine .......................................................................... 13  
Effective Patch Countermeasures ......................................................................... 13  
Granular Access Control for Websites .................................................................. 14  
Static IP Blacklist ................................................................................................... 14  
Dynamic IP Blacklist ............................................................................................. 14  
IP Whitelist............................................................................................................ 14
URL Blacklist .........................................................................................................................................................14
URL Whitelist .........................................................................................................................................................14
Visualization of Protection ....................................................................................................................................15

Product Value ..........................................................................................................................................................16
Zero Deployment and Zero Maintenance .............................................................................................................16
Comprehensive Structure and All-Round Security Protection .............................................................................17
Big Data-Enabled Intelligence against Emerging Attacks and Zero-Day Threats .............................................17
Efficient Emergency Response to Business Continuity ........................................................................................17

About CDNetworks ....................................................................................................................................................17
CDNetworks Science & Technology Enjoys Many FIRSTS in This Industry .......................................................18
Quality Global Resources .....................................................................................................................................18
Rich Experience of Professional Experience .......................................................................................................18
One-Stop Sales Network .......................................................................................................................................18
Status and Challenges of the Industry

With the rapid development of the Internet, service of web-based applications is widely used in many fields, including public sectors, e-commerce, and financial industry. Web applications bring quite much vitality to the Internet, but the complex and versatile nature of web applications has brought in endless system loopholes and increasingly serious security problems.

Web Application Facing Heavy Attacks

Security threats that web applications are facing:

Websites are Defaced
More websites have been affected by defacement. According to the China Internet Security Report 2016 by CNCERT, in 2016, there were 16,758 websites defaced and among these websites, 467 belong to government; Website defacement not only leads to financial loss for the owners, but more seriously, public image of related governments, institutions and enterprises could be damaged.

Leak of Sensitive Information on Websites
Information leak never stops. In December 2016, user data in the size of 12GB of jd.com (an online shopping mall) has been leaked and important information like ID numbers and passwords were also exposed; in the same month, similar tragedy reoccurred to Yahoo.com and this time, around 1 billion of accounts were involved; infringement of rights, frauds and other illegal acts from leak of sensitive information will not only damage users' individual interests, economic loss from enterprises is also commonplace.

Trojan Horse Attack
Monitor statistics from CNCERT shows that in 2016, there were about 40,000 IP addresses injected backdoor Trojans onto 82,072 websites in China. Among these, 2,361 were government websites. Around 33,000 IP addresses located abroad controlled 68,000 domestic websites by injecting backdoor Trojans.

Emerging Vulnerabilities lead to High Fix Costs

With the development of vulnerability disclosure, vulnerabilities in widely- used components emerge more frequently than ever, such as the Bash ShellShock, OpenSSL HeartBleed, Struts2, etc. The vulnerabilities have destructive effect and the cost of fix is pretty high. In the meanwhile, attack tools are also becoming more specialized and user-friendly, and the foreseen risks draw our attention.
Cybersecurity Law and Regulations Come into Effect

China’s Cybersecurity Law came into effect on June 1, 2017. It requires network operators to store select data within China and allows Chinese authorities to conduct spot-checks on a company’s network operations. The law, indicating China increasingly focuses on cybersecurity, was adopted by the National People’s Congress in November 2016 after a year of legislative proceedings, and it is intended to bring China in line with global best practices for cybersecurity. The government works effortlessly to protect information security and has attached unprecedented importance to this issue.

In November of 2015, State Administration for Industry and Commerce of China published *Opinions on Strengthening the Supervision of the Online Market* to regulate online market “by the laws, with cyber means, using credit and focusing on coordination”.

In 2014, President Xi Jinping said “No national security without cyber security” on the first meeting of Central Leading Group for Internet Security and Informatization.

Bottleneck of Traditional Protection Methods

The traditional method to defend against web application attacks relies on hardware WAF hardware on premise, and it faces more challenges as below:

Workload of deployment and maintenance

Network topology is usually required to be changed while deploying hardware equipment. Besides the heavy workload, there are system and business risks in the deployment process. When problems occur to equipment, due to physical location limited, trouble-shooting is hardly effective in a timely manner. Furthermore, it requires professional security team to monitor the equipment, adjust policies, or upgrade versions, when under attacks.

Update of outdated policies

Limited by timely data collecting ability, prevention policies and rules become a challenge to be updated in time. Moreover, collaboration in defense has not yet come into shape, compromising the response speed to counter zero-day attacks.

Product Introduction

Product Overview

Relying on CDNetworks globally distributed security PoPs, CDNetworks Cloud Web Application Firewall (WAF), which forms a network of cloud security integrating with the big data analysis platform on the cloud, provides protection against web application attacks covering OWASP Top10, malicious scanning, injection of web Trojan. At the same time, based on the self-learning protection engine and mechanism, WAF can detect and counter zero-day attacks timely to protect websites and sensitive data from data tampering and info exposure to ensure the security of websites.
Prevention Diagram of the Product

Diagram of the Product
Relying on CDNetworks globally distributed security PoPs, CDNetworks Cloud WAF inspects and analyzes request packets in real time, based on the big data analysis platform, the real time monitoring center, and the intelligent decision center. Illegitimate requests are intercepted once attack vectors are detected, and legitimate requests from normal users are able to access origins. In this way, websites can be prevented from defacement and sensitive info leakage to enhance website security.

The diagram below shows how Cloud WAF prevents against web application attacks in real time.

Protection structure of the product
Traditional WAF protection mainly relies on mechanisms like protocol validation, rule matching of attack signatures to counter attacks and ensure the information security of web business and assets. However, there are certain downsides of the passive protection mechanisms, for example, how to respond timely to zero-day attacks and web logic bypass attacks.

Against this backdrop, the protection mechanism of Threat Intelligence Database (Blacklist) + Self-Learning Protection Engine (Whitelist) is adopted by CDNetworks Cloud WAF.

• Threat Intelligence Database
  The database is composed not only of signatures and rules extracted from CDNetworks Cloud WAF prevention logs processed by the big data analysis engine, but also of intelligence sharing and collaboration in defense from vulnerability databases. The blacklist mechanism takes effect once the requests match certain rules in the database, and the predefined actions like interception takes place accordingly.

• Self-Learning Protection Engine
  CDNetworks Cloud WAF also builds a whitelist profiling the website structure, normal traffic from user access, data models of business logic, via learning the normal traffic to the protected websites. Requests are inspected and analyzed according to the whitelisting rules, and predefined actions takes place, for instance, either WAF blocks the requests or passes the abnormal request to further inspection.
The protection mechanism of Threat Intelligence Database (Blacklist) + Self-Learning Protection Engine (Whitelist) combines the passive prevention and the active prevention, not only thwarts the known threats, but is also able to respond quickly to emerging threats (variation of disclosed vulnerabilities and zero-day attacks).

WAF Applicable Industries and Scenarios

The targeted industries and scenarios of WAF includes but not limited to:

Public Sectors and Enterprises
As an important channel for Internet users to obtain information or online self-services, web portals face various types of security challenges like web defacement, web Trojan implant, SQL injection, user data leakage, and so on. Once a security incident occurs, the public image and reputation would be affected or even damaged. In the meanwhile, compliance is another force and stress to public sectors and enterprises facing security assessment and test.

Finance Industry
Security threats like injection and cross-site scripting could lead to exposure of user accounts and passwords, and risks of user economic losses. In case of such threats, reputation and economic losses would become inevitable to the financial industry.

E-commerce
E-commerce websites, as a main target, bear the brunt of web application attacks and more than often, attacks including transaction data tampering, user info leakage, online frauds, etc. Attacks like these not only harm personal interests, but also seriously damage the public image of victim companies.

Aviation industry
Airline websites and online ticket-selling portals are also web attacks targeted, as a large amount of personal information and itinerary details are stored on the sites, which interests the black market. Private info leakage could be utilized for fraud, which leads to personal loss for travellers and economic loss for the victim websites.

Functions and Features

The main functions of CDNetworks Cloud WAF include monitor & alert, prevention against common web attacks, self-learning protection engine, effective patch countermeasures, granular access control, visualization of protection, and etc. Data security of various industries can be ensured with these functions.

Monitor and Alert
It provides users with multi-dimensional monitoring and alerting services, including attack alarming system, website availability monitoring, security prewarning, and QoS monitoring on security PoPs, and aims to enable users to have a clear understanding of their websites.
Attack Alarming System
CDNetworks Cloud WAF provides the function of all-around attack monitoring and alerting, and a baseline of normal access is to set up after the analysis on historical access logs from the security PoPs (such as access frequency of each resource, behavior signatures of each request, etc.). With dynamic learning and log analysis, WAF is able to recognize attack signatures; once abnormal access is detected, alerts are sent out according to notification policies.

Website Availability Monitoring

• HTTP/HTTPS Monitoring
The monitoring mechanism relies on regularly stimulating visitors' access to monitored websites and analyzing on responses from globally distributed monitor nodes in real time, once anomaly is detected, alerts via email or SMS will be sent out, so the website staff can be aware of the anomaly in a timely manner.

• PING Monitoring
The monitoring mechanism relies on regularly probing the monitored servers or website connectivity and obtaining websites/servers connectivity status, packet loss ratio, and RTT response time, in order to detect connection anomaly. Alerts via email or SMS will be sent out, so the website staff can be aware of the anomaly in a timely manner.

• Security Pre-Warning
CDNetworks Cloud WAF analyzes the cloud-based attack data via the big data analysis platform and extracts attack signatures like IP addresses, UA, Refer, etc. Then it conducts security event correlation analysis on the similar attack techniques from different websites or industries. Prevention policies will be deployed to the entire network, in advance of similar attacks happen to the potentially susceptible websites in certain industry.

• QoS monitoring on security PoPs
CDNetworks Cloud WAF provides QoS monitoring on all the security PoPs 24/7. Refer to the PoP status, intelligent deployment and switch-over is enabled based on service quality of each node (such as load and traffic of each node) to ensure service availability and stability.
Prevention Against Web Application Attacks

CDNetworks Cloud WAF provides attack prevention against common web attacks mainly in the categories as below.

### HTTP Protocol Validation
- **Attack principle**
  Hackers usually send requests not compliant with HTTP protocol specification to fingerprint web server information or intend to bypass websites protection.

- **Protection principle**
  CDNetworks Cloud WAF validates HTTP requests following RFC specification. It can also set restrictions to request methods and protocol versions in request information as well as request header length, number of parameters, length of parameter name s, etc. Illegitimate requests will trigger alarm system and be blocked and recorded in logs. Based on ensuring normal service of web applications, WAF filters non-compliant requests to the maximum extent to reduce risks of web applications compromised.

### Injection
- **Attack principle**
  Injection attacks utilize web applications lack of input validation, for instance, SQL injection is used to attack data-driven applications, in which crafted SQL statements are inserted into an entry field for execution like exporting the database contents to the attacker, or even controlling database server.

### Prevention Against Injection Attacks

Injection attacks mainly include SQL injection, XPATH injection, LDAP injection, SSI injection, command injection, etc.

- **Attack principle**
  Injection attacks utilize web applications lack of input validation, for instance, SQL injection is used to attack data-driven applications, in which crafted SQL statements are inserted into an entry field for execution like exporting the database contents to the attacker, or even controlling database server.
• **Protection principle**
With the self-developed signature recognition engine, CDNetworks Cloud WAF can split a HTTP request to its finest granularity and test efficiently all split parts susceptible to possible attacks (such as URL, parameters, request body, request headers, etc.) to inspect whether certain parts match attack signatures for effective prevention. For example, a request is http://www.test.com?a=’1’ or 1=1, after splitting the request to several segments and testing each part, WAF determines the value of parameter a in the URL request with “’1’ or 1=1” matches a SQL injection rule with the signature. The request is blocked while the action is set to block.

**Prevention Against XSS Attacks**
• **Attack principle**
Similarity lies in lack of input validation for most scripting-based attacks. Take Cross-Site Scripting (XSS) for example, Cross-site Scripting (XSS) is a type of web application vulnerabilities, and enables attackers to insert client-side scripts into web pages viewed by other users and manage to modify content in response pages, steal user cookies and credentials, etc.

• **Protection principle**
With the self-developed signature recognition engine, CDNetworks Cloud WAF can segment a HTTP request to its finest granularity and test efficiently all segments susceptible to possible attacks (such as URL, parameters, request body, request header, etc.) to inspect whether some parts match attack signatures and protect against XSS attacks. For example, a request is http://www.test.com?a='><script>alert(document.cookie)</script>, after splitting the request several parts and testing each part, WAF determines that the value of parameter a in the URL request with “’><script>alert(document.cookie)</script> ” matches XSS attack rule with the signature. The request is blocked while the action is set to block.

**Prevention Against Malicious Scanners and Crawlers**
• **Attack principle**
There are two main types of attacks in this category, malicious scan and malicious crawling, which facilitate attackers to fingerprint target websites and gather relevant information as much as possible to determine further attacks.

• **Protection principle**
CDNetworks Cloud WAF is able to recognize requests sent from malicious crawlers and scanners and block such requests directly. For example, requests sent by Appscan scanner usually contain a character string of appscan in the User-Agent field, and WAF detects the header field and inspects attacks from the corresponding scanner. Regarding new scanners or crawlers, WAF refers to the database of malicious signatures to intercept illegitimate requests and attempts.

**Prevention Against Web Trojans**
• **Attack principle**
After attackers obtain web server permissions by exploiting web vulnerabilities, they would install their own programs to control and manage the target websites in a later phase. This is called web Trojan implant.

• **Protection principle**
Two-dimensional inspection is conducted by CDNetworks Cloud WAF.
1. Stop uploading backdoor Trojans in time.
There are multiple ways that WAF could use to stop web Trojans being uploaded to websites, for instance,
inspecting the known web Trojans and malicious contents in the files, or restricting dynamic scripts like
ASP and PHP being uploaded.

2. Stop uploaded backdoor Trojans executed
For the backdoor Trojans that have been uploaded to the websites before security polices deployed in
place or Trojans implemented from Intranet, CDNetworks Cloud WAF analyzes the access behaviors of
the web Trojans based on the big data database, in addition to the analysis on historical access logs.
WAF determines whether it shares the similarity of Trojan behaviors, such as web Trojans could be an
independent file and only very few IP addresses access, etc. Furthermore, suspicious requests are sent
to conduct to double check whether attackers attempt to access existing backdoor Trojans.

Authentication and Authorization Protection
• Attack principle
There are weaknesses and vulnerabilities of privilege allocation in web applications, which could be utilized
by attackers. Attackers could use deliberately crafted requests to bypass authentication and obtain either
user or even admin privilege or obtain unauthorized permissions. Typical attacks in this category include:
cookie tampering, session fixation, session hijacking, directory traversal, forced browsing, etc.

Cookie theft and tampering, by modifying cookies, attackers can obtain users’ unauthorized information to
steal users’ identities.

Session Fixation is an attack that permits an attacker to hijack a valid user session. The attack explores
a limitation in the way the web application manages the session ID, more specifically the vulnerable web
application.

Session hijacking is the exploitation of a valid computer session, sometimes also called a session key, to gain
unauthorized access to information or services in a computer system.

Directory traversal is usually crafted with “../” in URL or parameters, and it could allow attackers to access
restricted files in certain directories and execute commands outside of the web server’s root directory.

• Protection principle
CDNetworks Cloud WAF is able to detect and block the unauthorized malicious requests as below.

Session hijacking: CDNetworks Cloud WAF can protect session IDs related to user permissions against session
ID hijacked by attackers.

Cookie theft and tampering: CDNetworks Cloud WAF is able to set dedicated protection for cookies issued
and prevent against attackers tampering cookies.

Session fixation: CDNetworks Cloud WAF protects against session fixation targeting on user permissions via
session ID management. For example, WAF adds info like successful login into session ID to avoid attackers
obtaining user credentials via tricking users to submit fixed session IDs.
**Directory traversal and forced browsing protection:** CDNetworks Cloud WAF is able to detect and block unauthorized access to directories and files, to ensure important information is only accessible by authorized users.

**Prevention Against Web Framework Attacks**

**Attack principle**
The main types of attacks include attacks on CMS and open-source web applications components, as they are widely used in website development, and it might result in terrible consequence when vulnerabilities in the framework disclosed and exposed in the wild.

**Protection principle**
CDNetworks Cloud WAF protects against many known web vulnerabilities, for example, in aspcms, phpems, dedecms, ecshop, phpweb, FCKEditor, eWebEditor, struts2, phpmyadmin, etc. Additionally, with analysis on big data from real-time monitoring, WAF can immediately detect and counter attacks utilizing emerging vulnerabilities to protect website framework.

**Prevention Against Sensitive Information Leak**

**Attack principle**
Attackers deliberately intend to gather sensitive information from the target websites, for example, obtain sensitive information such as passwords, configurations, backup files, database, etc and utilize it directly for attacks. Another means is to gather exception or error messages from the website responses, for example, attackers craft incorrect database statements to make websites return error messages, which could be used to probe database software, versions, and more details, so as to launch attacks using vulnerabilities in the databases.

**Protection principle**
Different measures can be taken by CDNetworks Cloud WAF to protect sensitive information against leakage. Firstly, it can detect and block requests for sensitive information, and secondly, it can detect and block HTTP responses with sensitive information.

1. **Protection of sensitive information on server:** CDNetworks Cloud WAF can prevent sensitive information relating to programs and systems from being exposed via exceptions or error messages (such as server exception information, database exception information, application exception information, etc.).

2. **Protection of status codes:** CDNetworks Cloud WAF supports alarming or intercepting of commonly returned sensitive status codes started with 4 and 5, to avoid sensitive information on server side exposed.

3. **Protection of sensitive files download:** CDNetworks Cloud WAF can thwart attackers downloading website sensitive information (like passwords, configurations, backup files, database, etc.).

4. CDNetworks Cloud WAF also supports custom sensitive keywords, for example, sensitive keywords in responses. WAF is able to automatically block illegitimate content from being browsed by users.
Self-Learning Protection Engine

By learning normal traffic features of websites (such as data type, data boundary, data values, etc.) and access logics of business, self-learning protection engine of CDNetworks Cloud WAF can profile website structure of protected websites, build traffic data model based on normal traffic, to detect and filter abnormal access and mitigate potential attacks.

Example of self-learning protection engine:

a. A page from an online shopping site: http://www.xx.com/xx.php?num=x and the request parameter num means the quantity of the item to be purchased;

b. CDNetworks Cloud WAF with its self-learning protection engine, can learn the access features of this shopping site in normal business and among the results from self-learning of this site http://www.xx.com/xx.php?num=x, there is a whitelist rule: the value of parameter num is a positive integer;

c. If a request from client is http://www.xx.com/xx.php?num=1'or 1=1, WAF detects the value of num is a character string, which does not follow normal business model. So, this request will be blocked.

The self-learning engine of CDNetworks Cloud WAF adopts a dynamic active defense mechanism, and it can adjust and update the website structure models and behavioral baseline of normal traffic accordingly, without manual intervention required. Once the whitelist is built, requests that do not match whitelist rules will be alerted and blocked, or proceed with further inspection on abnormal requests, in case of potential attacks reaching the origins.

Effective Patch Countermeasures

Security vulnerabilities are increasing but difficult to fix in a timely manner, due to the following circumstances. It is difficult to install patches or upgrade versions for the production websites in real time, and secondly, with zero-day vulnerabilities disclosed, security vendors cannot provide the corresponding patches timely. Therefore, the unpatched vulnerabilities could be used by attackers for exploits.

CDNetworks Cloud WAF adds a defense line and provides a countermeasure for unpatched websites, which means protection policies can be configured against exploits and attacks utilizing the vulnerabilities before official patches applied to the websites. If zero-day vulnerabilities are found, WAF updates the corresponding policies to CDNetworks security network for collaboration prevention and mitigation.
Granular Access Control for Websites

To the requirement of restricting access from certain IP addresses or URLs to access their websites, CDNetworks Cloud WAF supports dual access control policies per IP address and URL, for example, IP blacklist/whitelist and URL blacklist/whitelist.

Static IP Blacklist
WAF blocks requests from IP addresses on the blacklist. It applies to certain IP addresses determined as attack IPs.

Dynamic IP Blacklist
According to client-side triggered logs, WAF can dynamically add certain IP addresses on blacklist and block the IP for a certain period. It applies to attackers conduct malicious scanning or attack attempt continuously.

IP Whitelist
Access from whitelisted IP addresses is allowed without further inspection. It applies to the scenario of company users and certain occasions.

URL Blacklist
Access to blacklisted URL will be blocked directly. It applies to the scenario that certain URLs of a website are defined not accessible to users.

URL Whitelist
Access to URLs on the whitelist is allowed without further inspection. It applies to certain URLs excluded from WAF protection.
Visualization of Protection

CDNetworks Cloud WAF displays details of attacks, such as attack trend, attack details, attack type, attack source, etc., and interception details. Users can view the protection status and results in real time, and understand the security status of their business based on the attack trend.

1. Displays attack and interception trend in real time. Users can get aware of security protection details in different time periods and attack types are displayed in pie chart.
2. Provides detailed information of intercepted IP addresses, including IP location, attack types, attack times, etc. to facilitate users to process and deal with the attacks in a later phase.

Product Value

Zero Deployment and Zero Maintenance

It does not require changing the existing network topology, and the professional web protection service is enabled only via adding a CNAME record. At the same time, entire network monitoring 24/7 is provided by WAF monitoring platform and service nodes can be dispatched smartly based on the service quality to ensure service stability and availability. Moreover, various types of attacks can be alarmed, and emergency measures can be taken to ensure service quality and stability. Zero deployment and zero maintenance are ensured.
Comprehensive Structure and All-Round Security Protection

Different from other WAF products in terms of protection structure, CDNetworks Cloud WAF is based on “Threat Intelligence Database (Blacklist) + Self-Learning Protection Engine (Whitelist)”. This self-developed protection structure combines passive and active defense, and it enables customized and granular protection to meet different requirements for website security, aiming to minimize risks of public image damage and economic losses caused by web security issues.

Big Data-Enabled Intelligence against Emerging Attacks and Zero-Day Threats

With prevention practices for tens of thousands of websites, CDNetworks Cloud WAF builds up a database of comprehensive rules, in addition to correlation analysis from attacks to different websites. When a new type of attacks is spotted, WAF applies the corresponding protection policy to the entire network and builds a protection system to guard the entire CDNetworks network.

Efficient Emergency Response to Business Continuity

CDNetworks Cloud WAF offers dedicated service team to provide one-to-one service 24/7. Once zero-day attacks are detected, emergency response and collaborative defense in place for the entire network to mitigate threats and ensure business continuity for customers.

About CDNetworks

Founded in January of 2000, CDNetworks Science & Technology provides global solutions and services that cover content distribution and acceleration, server hosting and renting and network optimization for ISP. It’s a premier comprehensive service provider of CDN and IDC. CDNetworks was publicly listed on Shenzhen Stock Exchange in October, 2009.

Headquartered in Shanghai, CDNetworks Science & Technology also has three offices in other three global cities in China: Beijing, Guangzhou and Shenzhen. CDNetworks also has set up subsidiaries in America, Hong Kong, Malaysia, Tianjin, Nanjing, Jinan and other places all 9 of them. In Xiamen and Silicon Valley of US, it has set up a R&D center in each place. There are over 2,000 employees in CDNetworks and more than 60% of them are in research and development. Our customers cover a wide of range of industries and types of portals, from Internet companies in streaming media, gaming, e-commerce, search browsers and social media to governments, enterprises and various ISPs. At present, our customers are up to 3,000 and we are proud to say that our company is second to none in this industry in terms of number of customers and business range it covered.

Holding the Business License for Cross-region Value-added Telecommunications Busines (IDC, ISP) issued by Ministry of Industry and Information Technology of China, CDNetworks Science & Technology is also a member to Asia-Pacific Network Information Centre (owning Autonomous System) and a member to China Internet Network Information Center (owning Autonomous System).
CDNetworks Science & Technology Enjoys Many Firsts in This Industry

- First publicly listed company in China that is specialized in CDN and IDC
- The most profitable CDN and IDC company in China
- The first company in China that has developed CDN platform independently
- The first company in China that has developed the technology of dynamic acceleration
- The first company in China that has developed the CDN content distribution platform with cloud architecture
- Largest CDN content distribution platform in China in terms of scale
- The first CDN company in China that has passed the compliance certification of PCI DSS V3.0

Quality Global Resources

A complete coverage of ISPs in China, and in cooperation with big three telecommunication companies (China Mobile, China Telecommunications, and China Unicom) and two specialized network (China Education and Research Network and China Science & Technology Network). CDN content distribution and acceleration nodes of CDNetworks cover the entire globe and besides its nearly 500 domestic nodes, CDNetworks has deployed almost 60 nodes overseas, in San Jose, Los Angeles, Dallas, Chicago, New York, London, Amsterdam, Paris, Mumbai, Singapore, Sydney and other cities. Its service has expanded to developed countries and regions in 6 continents, North America, Europe, Asia, South America, Asia and Oceania. Acceleration requirements from customers around the world can be supported with our quality resources.

Rich Experience of Professional Experience

With 15 years of operation experience in acceleration and improvement of Internet user experience, CDNetworks is a premier service provider of Internet acceleration and it also has been serving Four Web Portals (sina.com, souhu.com, qq.com and 163.com) for many years. CDNetworks knows clearly the basic structure and applications of the Internet in China.

CDNetworks is committed to providing its customer with one-to-one professional service and in serving many foreign and domestic big brands with quality acceleration, it has collected many years of service experience, which in turn can help us better meets customers’ needs of informationization and business development.

One-Stop Sales Network

In Beijing, Shanghai, Guangzhou, Shenzhen and other cities or regions, CDNetworks has set up subsidiaries or offices that cover regions with more than 80% of China Internet users. Business consultation and business process are available in each office of CDNetworks for 7*24, with fast response and other one-stop sales service.