Who is Cyber Security Cloud, Inc.

Cyber Security Cloud, Inc. provides cutting-edge cybersecurity solutions, including comprehensive managed security services and web application security services that leverage Cyber Threat Intelligence and AI technology. As a global leader in cybersecurity, we are dedicated to creating a safe and secure cyberspace for people around the world through our comprehensive security offerings.

Cyber Security Cloud, Inc. are the creators of the following world class products:

- ## Managed Rules for AWS WAF
  - Cyber Security Cloud, Inc. is one of 7 AWS managed rules providers globally.

    WEBSITE : https://www.wafcharm.com/en/managed-rules/

    AWS MARKETPLACE :
    https://aws.amazon.com/marketplace/pp/prodview-kyur2d2omnrlg

- ## WafCharm
  - WafCharm is a service for automating the operation of cloud WAF. WafCharm automatically creates and updates rules (signatures) to respond to newly discovered attacks and new vulnerabilities based on access logs, so by using it in conjunction with the Cloud WAF. You can operate the WAF smoothly without the need for a dedicated security engineer. AWS WAF, Azure WAF, Google Cloud Armor - leave it all to us!

    WEBSITE : https://www.wafcharm.com/

    AWS MARKETPLACE:
    https://aws.amazon.com/marketplace/pp/prodview-crrflizdnl6pw

- **CloudFastener**
  - Fully Managed AWS & Google Cloud security 24 hours a day / 365 days a year. We comprehensively manage and operate cybersecurity in accordance with your AWS & Google Cloud environment. We are releasing our Azure version this fall.

    https://cloud-fastener.com/en/

    AWS MARKETPLACE:
    https://aws.amazon.com/marketplace/pp/prodview-7wxhkj52w4yu4

PRESS RELEASE & PEER REVIEWS

- **CloudFastener Press Release**
- **WafCharm Reviews G2**
- **WafCharm Reviews AWS MARKET PLACE**

CloudFastener

Security Operations Software That Uses Gen AI & Effective Risk Management Engine Combined with Human Insight.

CloudFastener performs AWS & GCP asset discovery, security risk visualization, vulnerability analysis, configuration error assessment in operating systems and software, and threat intelligence gathering within a cloud environment. It also provides continuous **24/7** protection and monitoring for your cloud platform environments, prioritizes and addresses potential risks, and offers support for managing and responding to security alerts.

https://vimeo.com/985346057?share=copy

How It Works

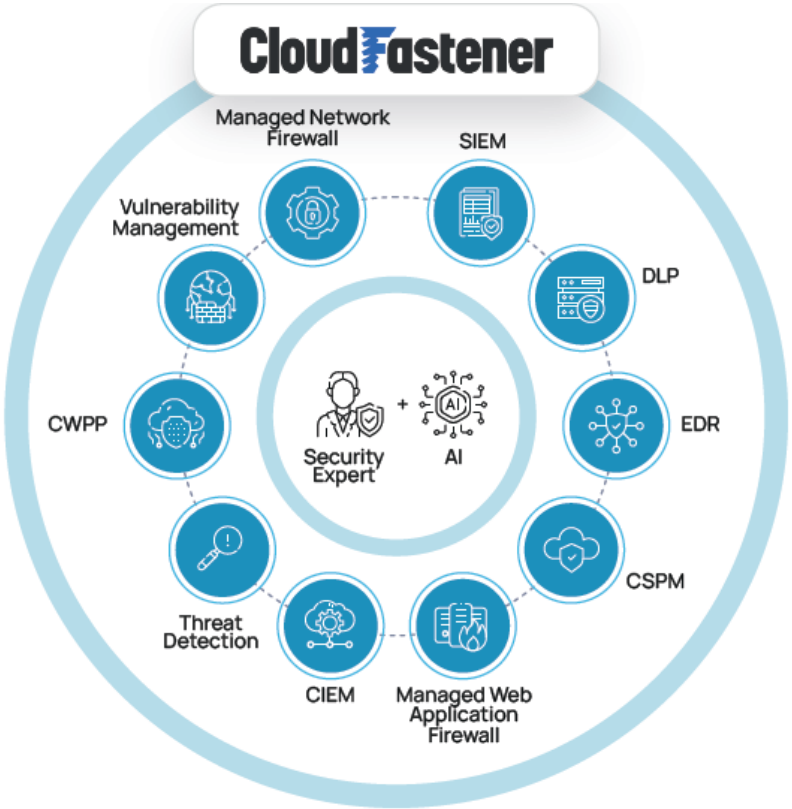
1. CloudFastener seamlessly integrates with your AWS environment

2. Our SIEM ingests security events and logs from your AWS services

3. AI-driven Effective Risk Management Engine automatically triages and prioritizes threats

4. Dedicated security experts provide human insight and remediation guidance

5. Continuous updates ensure alignment with latest AWS security standards



Key Benefits

- Round-the-clock monitoring and protection of your entire AWS environment
- Automated threat detection and risk prioritization powered by cutting-edge AI
- Comprehensive security coverage across all critical areas
- Reduced operational burden and costs compared to traditional managed services
- Continuous compliance with industry security standards and best practices
- Customizable to your specific security needs and priorities

[Click here to learn more]

WafCharm

https://youtu.be/uKSQu3fWRl0

WafCharm is the only "auto configuration" system for AWS WAF!

Click here to download our WafCharm Overview Document

Take advantage of our **30 day FREE TRIAL**! If you need more time, then please contact us and we can send you a private offer!

WafCharm's Main Features:

OWASP TOP 10 ENTERPRISE SIGNATURES

- BOT CONTROL PROTECTION
- DDos Prevention and Early Detection System
- AUTOMATED IP BLOCKING

Checkout WafCharm's **Lightning Talk at AWS re:Invent 2023**.

https://youtu.be/GqAh2EfMqPU

-

Compliance and Cyber Security Insurance

Application Whitelisting
CloudFastener

A security solution that allows organizations to specify what software is allowed to run on their systems, in order to prevent any nonwhitelisted processes or applications from running.

Asset Inventory
CloudFastener

A list of all IT hardware and devices an entity owns, operates or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

Custom Threat Intelligence
Waf'Charm CloudFastener

The collection and analysis of data from open source intelligence (OSINT) and dark web sources to provide organizations with intelligence on cyber threats and cyber threat actors pertinent to them.

Database Encryption
CloudFastener

Where sensitive data is encrypted while it is stored in databases. If implemented correctly, this can stop malicious actors from being able to read sensitive data if they gain access to a database.

Data Loss Prevention
CloudFastener

Software that can identify if sensitive data is being exfiltrated from a network or computer system.

Vulnerability Scans
CloudFastener

Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

DDoS Mitigation
Waf'Charm CloudFastener

Hardware or cloud based solutions used to filter out malicious traffic associated with a DDoS attack, while allowing legitimate users to continue to access an entity's website or web-based services.

DMARC

An internet protocol used to combat email spoofing – a technique used by hackers in phishing campaigns.

DNS Filtering
Waf'Charm CloudFastener

A specific technique to block access to known bad IP addresses by users on your network.

Email Filtering

Software used to scan an organization's inbound and outbound email messages and place them into different categories, with the aim of filtering out spam and other malicious content.

Employee Awareness

Training programs designed to increase employees' security awareness. For example, programs can focus on how to identify potential phishing emails.

Web Application Firewall
Waf'Charm CloudFastener

Protects web facing servers and the applications they run from intrusion or malicious use by inspecting and blocking harmful requests and malicious internet traffic.

Endpoint Protection
Waf'Charm CloudFastener

Software installed on individual computers (endpoints) that uses behavioral and signature based analysis to identify and stop malware infections.

Incident Response Plan
CloudFastener

Action plans for dealing with cyber incidents to help guide an organization's decision-making process and return it to a normal operating state as quickly as possible.

Intrusion Detection System
Waf'Charm CloudFastener

A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

Managed Service Provider
CloudFastener

A third party organization that provides a range of IT services, including networking, infrastructure and IT security, as well as technical support and IT administration.

Mobile Device Encryption

Encryption involves scrambling data using cryptographic techniques so that it can only be read by someone with a special key. When encryption is enabled, a device's hard drive will be encrypted while the device is locked, with the user's passcode or password acting as

Multi-Factor Authentication

Where a user authenticates themselves through two different means when remotely logging into a computer system or web based service. Typically a password and a passcode generated by a physical token device or software are used as the two factors.

Network Monitoring
Waf'Charm CloudFastener

A system, utilizing software, hardware or a combination of the two, that constantly monitors an organisation's network for performance and security issues.

Penetration Tests
Waf'Charm CloudFastener

Authorized simulated attacks against an organisation to test its cyber security defences. May also be referred to as ethical hacking or red team exercises.

Perimeter Firewalls
Waf'Charm CloudFastener

Hardware solutions used to control and monitor network traffic between two points according to predefined parameters.

Security Info & Event Management
CloudFastener

System used to aggregate, correlate and analyse network security information – including messages, logs and alerts – generated by different security solutions across a network.

Web Content Filtering
Waf'Charm CloudFastener

The filtering of certain web pages or web services that are deemed to pose a potential security threat to an organisation. For example, known malicious websites are typically blocked through some form of web content filtering.

If it's in the cloud, we got you covered!

We focus on the important things that matter. From Compliance, Cyber Security Insurance , Info Sec Documentations & Questionnaire.

Benefits & Advantages

Partnering with us not only secures your customers, but easily qualify to the best Cyber Security Insurance premiums that your company offers.

	Satisfying the mandatory list for customers in order for them to get Cyber Insurance with CSC products	Lowering Insurance premium by selling CSC products to insurance customers
Cyber Insurance Company	**Co-sell/ marketing with CSC to target wider customer base**	**Increase customer base**
Cyber Insurance Customers	**Customers will satisfy qualification to purchase cyber insurance**	**Lower cyber insurance cost**

COMPLIANCE UPDATES

We no longer need access on various web request logs. On special cases that we do, we utilize our compliance frameworks to analyze each web request to fortify your security and enhance our signatures.

No logs are needed for the following:

- Amazon API Gateway
- REST APIs
- GraphQL APIs
- Amazon Cognito

Log accesses are required for the following endpoints below for WafCharm to learn and improve our signatures.

- Application Load Balancers
- Elastic Load Balancers
- CloudFront distributions

Get in Touch

Anri Nakayama

VP of Partner Relations

anri.nakayama@wafcharm.com

M: 214-714-3919

LinkedIn

I was born and raised in the United States, and after going to college and working at an accounting firm in Los Angeles, I moved to Japan to help launch the Tokyo branch of an Irish fintech company. After working in Tokyo for about a year and a half, I realized I wanted to return to Los Angeles, where I was used to living, and decided to return to Japan. Just as I was starting to look for a new job, I learned that Cyber ⊠⊠Security Cloud (CSC) was looking for members to start an organization in Los Angeles, so I joined the company in September 2020

If you want to schedule a meeting with Anri, please click here.

Privacy Policy for Overseas Customers: Cyber Security Cloud, Inc. and Cyber Security Cloud Inc. (USA) (hereinafter collectively referred to as "**CSC**," "**we**," "**us**," "**our**," or "**ours**") have established the following Privacy Policy for Overseas Customers ("**Global Privacy Policy**") in order to establish a secured system to protect your personal data and ensure that all executives and employees of CSC recognize the importance of protecting your personal data and are fully committed to doing so when providing our various services (the "**Services**").

This Agreement for design services is between Cyber Security Cloud, Inc ("Designer"), and "Your Company" (Client), for the performance of the services described in the proposal sent to Client on Proposal delivery date ("Proposal"). The parties, therefore, agree as follows:

Information Security Policy

- https://www.cscloud.co.jp/security/?lang=en

Privacy Policy

- https://www.cscloud.co.jp/en/privacy/

Questions?

Contact | anri.nakayama@wafcharm.com | Phone: 214-714-3919