CASPIPOT

SECURITY GUARD

SOLUTION BRIEF

Overview

Caspipot Security Guard is a security solution whose security features form a multiple and flexible chain to fight against cyber threats.

It may be easily integrated into cloud and hybrid architectures and boasts of top-level security products such as threat intelligence, attack surface management, data loss prevention, and security assessment.

Caspipot's deception technology helps to trick the attacker and study their actions, which allows to detect and counter attacks in real time.

Through continuous evaluation and analysis of an organization's online presence, potential vulnerabilities are identified early, ensuring the system remains secure.

Core features such as web application firewall (WAF) control and malicious traffic blocking with IOC management reduce the workload for security teams while providing high levels of automation against breaches.

This kind of structure helps organizations to be much more effective in their fight against cyber threats by providing them with the tools and components that can be easily added into their existing systems.

KEY CHALLENGES

LIMITED ASSET VISIBILITY	**Challenge:** Expanding infrastructure makes it difficult to track all of an organization's assets. **Need:** Continuous assessment to track management and identify deficiencies in each asset.
ADVANCED CYBER ATTACKS	**Challenge:** Traditional security measures struggle to adapt to new attack tactics and attack vectors. **Need:** Advanced monitoring tools that detect emerging challenges in advance and provide practical solutions.
REGULATORY COMPLIANCES	**Challenge:** Companies must comply with strict data protection laws and industry-specific regulations such as GDPR, PCI/DSS, HIPAA, SOC 2. **Need:** Facilitate compliance analysis to ensure compliance with standards and avoid unwanted financial consequences.
SYSTEM ENDURANCE TEST	**Challenge:** Many businesses lack clarity on how their systems will respond to real-time threats. **Need:** Evaluating the system's capabilities during high-volume scenarios and aggressive threats.
TOO MANY ALERTS	**Challenge:** Security teams are faced with a flood of alerts and have difficulty identifying critical threats. **Need:** Reduce unnecessary alerts and focus on important threats by establishing automatic mechanisms.

HOW IT WORKS?

Security Guard from Caspipot is the set of security measures and steps that would protect the object on different levels.

The platform makes use of modern threat data and involves self- organizing security features, which means it can be easily incorporated into your infrastructure and scales well.

Caspipot applies deception technology in an attempt to lure attackers and study their techniques, with a view of quickly identifying attacks and containing them.

Moreover, as the evaluation progresses, new areas become added to the digital context to be scrutinized and potential threats are noted early enough to enhance safety of the system.

Essentials such as web application firewall (WAF) control filter external threats, reducing the manual workload on security professionals and offering strong automated security measures against attacks.

MODÜLLER

Modül	Çözüm Alanı
DECEPTION MODULE	By imitating real services, attracts malicious parties and collect important information about attackers' tactics. These traps help quickly detect problems and create prepared defenses by recording attack details.
ATTACK SURFACE MONITOR	Monitors assets accessible over the internet and detects potential vulnerabilities and open endpoints. Organizations monitor live changes to keep their sensitive assets in order.
BREACH DATA CONTROL	Searches for stolen or compromised company credentials and data from external sources. Teams are alerted about potential breaches so they can mitigate risks before they escalate.
WAF CONTROL & IOC MANAGEMENT	While WAF Control inspects and blocks malicious web traffic, the IOC pool provides a continuously updated blacklist of risky IPs and proxies. This combination simplifies automation while reducing monitoring overhead.
STRESS TESTING	It helps companies determine the resilience of their systems to real-world conditions by simulating heavy traffic threats. The generated reports enable teams to take precautions against threats.

USE CASES

Retail Providers – Deception and WAF Control

Deception Module is used by two leading retailers in Turkey.

*Draws attackers into fake systems, gathering insights without endangering real assets.

WAF Control and IOC Management are integrated.

*Stops malicious traffic.
*Creates custom security rules suitable for with two-way data transfer.
*The integration offered with WAF systems has the capability to identify the malicious traffic and take action quicker.

USE CASES

Insurance, Finance and Banking – Attack Surface Monitor and Stress Testing

A leading insurance company uses Caspipot's Deception and Attack Surface Monitor modules.

*Regularly scans IP addresses and services accessible over the internet.
*Detects potential vulnerabilities.

Tests systems under heavy traffic with the module.

*Measures system endurance.
*Identifies and improves weak points through reports.

This feature is useful for banks and fintech companies to assess their system performance against real-time attacks.

Digital Media Platforms – Traffic Monitoring, WAF Control and Attacker Analysis

Turkey's two leading digital media platforms use Caspipot's solution.

*Monitors the traffic on their platform.
*Strengthen their WAF.

Deception attracts attackers and collect in-depth data about their attack methods and behaviors.

*Extracts attacker profiles.

Analyzes requests coming to web applications with WAF Control.

*Takes automatic actions when malicious traffic is detected.

These methods increase the security levels of the platforms.

*Helps to block potential attack vectors at an early stage.

For detailed technical use case documents: info@caspipot.com

Contact us.

For inquiries, business partnerships, or customer support, please contact our team at info@caspipot.com or through our social media accounts.

Your attention is greatly appreciated.

linkedin/caspipot

www.caspipot.com