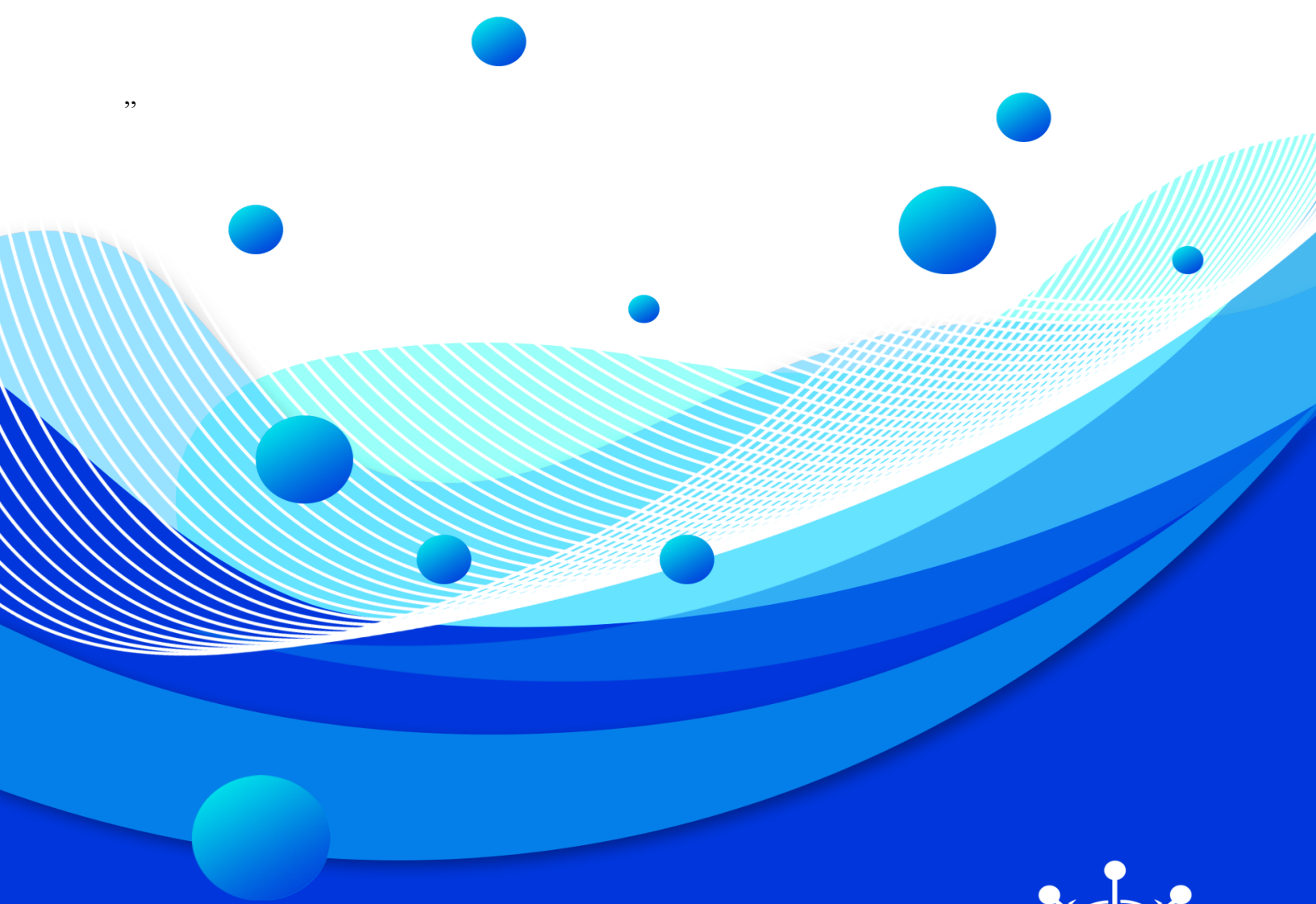


# SECURITY GUARD

Defend Your **Business** Against  
the Latest Cyber Threats



Technical Documentation





## Product overview

- [Quick Start Guide](#)
- [What's New](#)
- [Getting Started Guide](#)

## Planning

- [Architecture and Deployment Guide](#)

## Installing

- [Installation Guide](#)

## Configuring

- [Honeypot Node Configuration Guide](#)
- [Attack Surface Monitor Configuration Guide](#)
- [Breach Data Control Configuration Guide](#)
- [Phish Data Configuration Guide](#)
- [IOC's Data Usage Guide](#)
- [O365 Integration Guide Line \(Quick Start Guide Version 2.0\)](#)

## Administering

- [Administration Guide](#)

## Monitoring

- [Attack Surface Monitoring \(Quick Start Guide Version 2.0\)](#)
- [Breach Data \(Quick Start Guide Version 2.0\)](#)
- [Honeypot \(Quick Start Guide Version 2.0\)](#)

## Tuning and Troubleshooting

- [Troubleshooting and System Notifications Guide](#)
- [Tuning Guide\(Quick Start Guide Version 2.0\)](#)



# Effective Approach for Your Cyber Security with **CaspiPoT** Security Guard

## Quick Start Guide Version 1.2.2

**CaspiPot Security Guard** is an all in one SaaS security solution where you can create your honeypot services within minutes, track the attackers and gather information with attack surface monitoring & breach data control.

This guide gets you started with a typical installation and configuration. To obtain the Quick Start Guide in other languages, print the language-specific PDF from the installation media.

© Copyright CaspiPoT 2023.

## WHAT'S NEW

Office 365 security compliance can help to protect all parties involved, maintain public reputation, avoid fines, and ensure important data is not lost or stolen. Large companies, small and medium-sized enterprises and even smaller companies have already deployed these solutions to increase the productivity and collaboration of their teams.

Microsoft 365 solutions offer unprecedented flexibility in information sharing and collaboration, allowing employees to connect to their work environment on a variety of devices and from any location.

However, this flexibility to access documents, data and other company information via SharePoint, OneDrive, Exchange, creates many problems and opportunities for highly targeted cyber-attacks on the information system.

With the **CaspiPoT-OSeC365** module, all your risks can be monitored on an integrated screen. With machine learning-based analysis, it helps you detect and catch potential threats faster.





# Getting Started Guide

CaspiPoT Security Guard Getting Started Guide introduces you to key concepts, an overview of the installation process, and basic tasks that you perform in the user interface.

## Intended audience

This information is intended for use by security administrators who are responsible for investigating and managing network security. To use this guide you must have a knowledge of your corporate network infrastructure and networking technologies.

Technical documentation for information about how to access more technical documentation, technical notes, and release notes, see CaspiPoT Security Guard Security Documentation Technical Note (<https://www.caspiopot.com/support/1905>).

Contacting customer support for information about contacting customer support, see the Support and Download Technical Note (<http://caspiopot.com/support/>).

Statement of good security practices IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. CaspiPoT Security Guard systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. CaspiPoT DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note: Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. CaspiPoT Security Guard may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of CaspiPoT.



# Architecture and Deployment Guide

When you plan or create your CaspiPoT Security Guard deployment, it's helpful to have a good awareness of CaspiPoT architecture to assess how CaspiPoT Security Guard components might function in your network, and then to plan and create your CaspiPoT deployment. CaspiPoT processes, aggregates, and stores attack-data in real time. CaspiPoT Security Guard providing real-time information and monitoring, alerts and offenses, and responses to threats. CaspiPoT Security Guard is a modular architecture that provides real-time visibility, which you can use for threat detection and prioritization. You can scale CaspiPoT to meet your collection and WAF response. Attack Surface Monitoring systems helps to find critical issues in assets.

## CASPIPOT COMPONENTS

<b>CLOUD HONEYPOT</b>  Services  Rules  Waf	<b>BREACH DATA CONTROL</b>	<b>ATTACK SURFACE MONITOR</b>  Last Scanner Activities  Asset Status Control  Blacklist Control
<b>PHISH DATA</b>	<b>IOC's</b>  Bad IP Pool  Proxy Pool  Fqdn Pool	<b>O365 GUARD</b>



# ALL-in-ONE DEPLOYMENT

Although the product consists of multiple modular structures, it is very easy and simple to install. First of all, in order to activate your services, you must register your domain name. You can access panel with <https://manager.caspipot.com>

Name	3d Party	Credits	Active Services	Domains	Users	Cred(s)
IS-Eu	<a href="#">Integrations</a>	105	0	1	3	<a href="#">Tryed creds</a>

#	Domain	Status	Created	Last Update
188	example.com	Active	2023-08-01 18:21:31	2023-08-01 18:22:02

After the approved registration of your domain name is completed, the domain name is automatically added to the asset list.

Company	Domain	Assets	Last Control
Eu	<a href="#">example.com</a>	1	2023-08-01 18:22:02



# CONFIGURING

## Honeypot Node Configuration Guide

To activate honeypot services via **the manager panel || CLOUD HONEYPOT >> Services >>> Create** field should be reached.

In order to define services, it is necessary to complete the **service name, domain name** and **port information** of your service completely.

Cloud HoneyPot

Services

+ Create

List

Rules

WAF

Servers

Modules

Attack Surface Monitor

Phish Data

Breach Data Control

IOC

Bad IP Pool

Run New service

Home / Services List / Run New Service

Service Runner

1 Default Information

2 Select Server

3 Select Service

Service Name

FTP

Service domain

ftp.example.com

Extra PORT

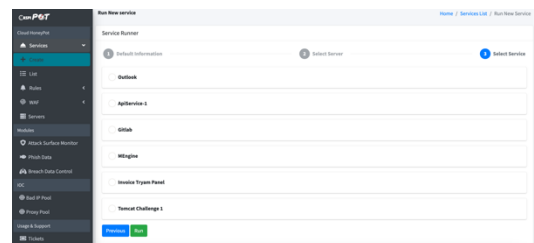
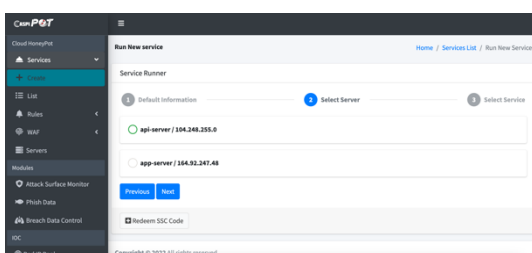
Active Ports: 8443 443 7999 7354 6375 8080 4555 8080 8008 7575

21

Next

With the defined information, the area where you can choose from among the servers defined in different datacenters around the world will be displayed to within the scope of the license type.

These are the things that need to be done in order to take a service live.





After the configurations related to the services, the manager panel shows all active and passive services. You can be viewed by following the steps of **manager panel || CLOUD HONEYPOT >> Services >>> List**

The screenshot shows the 'Service List' page in the CaspIoT Manager Panel. The page is titled 'Service List' and has a breadcrumb trail 'Home / Services List'. A 'Run New Service' button is located in the top right corner. The main content area displays a grid of service cards. Each card represents a service configuration and includes the following information:

- Service Name:** Gitlab / Test Gartner, Tomcat Challenge 1 / \*\*\*\*baktomcat, Tomcat Challenge 1 / Tomcat Test, Gitlab / Test, Pusula for \*\*\*\*\*/ pusula, ApiService-1 / Test
- Waf Status:** Not Active, fs, Not Active, Not Active, Not Active, Not Active
- Domain:** exaple-1-gartner.com, \*\*\*\*bak.com, tomcat.caspipot.com, Test, pus\*\*\*\*him.com.tr, api\*\*\*\*him.com.tr
- Server:** 116.203.131.77, 164.92.247.48, 116.203.131.77, 116.203.131.77, 104.248.255.0, 104.248.255.0
- Port:** 7575, 8080, 8080, 8080, 443, 8443

Each card also features a status banner (ACTIVE or DISABLED), a service icon, and a set of control buttons (Logs, Rules, and a settings icon).

To Access your licensed servers manager **manager panel || CLOUD HONEYPOT >> Services >>> Servers**

The screenshot shows the 'Active Servers' page in the CaspIoT Manager Panel. The page is titled 'Active Servers' and has a breadcrumb trail 'Home / Servers'. The main content area displays a grid of server cards. Each card represents a server configuration and includes the following information:

- Server Name:** pusula-servis, \*\*\*\*bak server, EU
- Service Count:** 2, 1, 5
- IP:** 104.248.255.0, 164.92.247.48, 116.203.131.77
- Location:** Istanbul, TR, Germany
- Created:** 2022-12-24 22:11:13, 2023-03-21 07:43:12, 2022-11-06 18:53:11

Each card also features a progress bar and a set of control buttons (Attack Logs and a settings icon).

With the operations performed, attacks on services that are now defined begin to be detected. Important rules can be written for the listed attack types and critical situations. You can receive hourly, daily, monthly reports on detected attacks and automatically forward them to the relevant teams.

IP	Action Type	Location	Password	Request Method	Browser / Platform	URL	Time
116.203.131.77	HTTP	TR	NA	GET	Opera/9801.223.146.0	http://116.203.131.77/	1 week ago
116.203.131.77	HTTP	TR	NA	CONNECT	Go-http-client/1.1	http://116.203.131.77/	1 week ago
116.203.131.77	HTTP	TR	NA	CONNECT	Opera/9801.223.146.0	http://116.203.131.77/	1 week ago
116.203.131.77	HTTP	TR	NA	GET	Opera/9801.223.146.0	http://116.203.131.77/	1 week ago
116.203.131.77	HTTP	TR	NA	GET	Opera/9801.223.146.0	http://116.203.131.77/	1 week ago
116.203.131.77	HTTP	TR	NA	CONNECT	Go-http-client/1.1	http://116.203.131.77/	1 week ago
116.203.131.77	HTTP	TR	NA	GET	Opera/9801.223.146.0	http://116.203.131.77/	1 week ago





# Attack Surface Monitor Configuration Guide

To activate attack surface management services via **the manager panel || Modules >> Attack Surface Monitor** field should be reached.

In order to define services, it is necessary to complete at the “*Total Assets*” **domain name** and **IP address** service completely. CaspiPoT security guard will automatically scan and add subdomains to the system.

The dashboard displays the following information:

- Attack Surface Monitor Risk Score:** A (98.5%). Conditions that may cause risk were observed.
- Total Assets:** 5 (1 IP, 0 FQDN)
- Asset monitor:** 3 (9 DETECTIONS, 7 SECURITY REPORT)
- Usage Status:** 5 Asset Usage. You have 100 asset usage limit. 5 assets are used 95 pieces can be added.
- FQDN Status:** 3 DOMAINS, 0 SUBDOMAIN
- SSL Certificate Status:** 4 TOTAL, 3 LESS THAN 90 DAYS TO EXPIRE
- Domain Registration Status:** 3 TOTAL DOMAIN, 0 LESS THAN 90 DAYS TO EXPIRE
- Blacklist Control:** 2 ASSET LIST, 0 BLACKLISTED ASSETS

The Assets list shows the following data:

Asset	Sub Scan	Type	Location	Added	#
ioc.example.com	<input type="checkbox"/>	subdomain	Canada	2023-03-11 01:52:52	
13.50.124.130	<input type="checkbox"/>	ip	Sweden	2023-02-05 13:13:13	
manager.example.com	<input type="checkbox"/>	N/A	Germany	2023-02-03 01:44:03	
example.com	<input type="checkbox"/>	N/A	Canada	2023-02-03 01:39:59	
api.example.com	<input type="checkbox"/>	N/A	Germany	2023-02-03 01:39:55	

Copyright © 2022 All rights reserved.



Asset Monitor allows you to monitor the health status of all your inventory that provides internet service that is open to the world. **The manager panel || Modules >> Attack Surface Monitor >> Asset Monitor** field should be reached.

**Attack Surface Monitor / Monitor** Home / Attack Surface Monitor / Example / ASM Monitors

RedLabIS Monitoring List Add New Asset

Asset	Status	Monitor HACK	Detections	Lat Control	#
example	301	ON (BETA)	5	1 min ago	
example.eu	200	ON (BETA)	34	1 min ago	
example.xyz	200	ON (BETA)	9	2 min ago	
13.50.124.130	302	ON (BETA)	1	3 min ago	
example.com.tr	200	ON (BETA)	111	4 month ago	
ticket.example.com	302	ON (BETA)	41	4 month ago	
api.example.com	200	ON (BETA)	3044	2 min ago	

Copyright © 2022 All rights reserved.

With the correct entry of the information, the system will automatically scan the **Service, Port, Vulnerability** information of the added asset and display the results in a short time.

**CASPIPOT**

Modules

- Attack Surface Monitor
- Phish Data
- Breach Data Control

IOC

- Bad IP Pool
- Proxy Pool

Usage & Support

- Tickets
- Licenses

Profile

- Profile
- Logout

**FQDN Status**

10 DOMAINS | 7 SUBDOMAIN

**SSL Certificate Status**

99 TOTAL | 96 LESS THAN 90 DAYS TO EXPIRE

**Domain Registration Status**

10 TOTAL DOMAIN | 0 LESS THAN 90 DAYS TO EXPIRE

**Blacklist Control**

0 ASSET LIST | 0 BLACKLISTED ASSETS

**Last Vulnerability List**

- Missing Security Headers / cmms-prod-apac.corp.google.com
- Missing Security Headers / cmms-mobile-prod.corp.google.com
- Missing Security Headers / cmms-dev6-mobile.corp.google.com
- Missing Security Headers / cmms-dev5-mobile.corp.google.com
- Missing Security Headers / cmms-dev4-mobile.corp.google.com

N/A
Informative
Low
Medium
High/Critical
+ Open Full List



# Breach Data Control Configuration Guide

To activate breach data services via **the manager panel || Modules >> Breach Data Control** field should be reached.

When the stolen data area is accessed, the company lists defined for you will be displayed automatically. While you access the company field you want to process, the **domain names** that have been given permission for the company are displayed.

You can view *existing stolen* data by creating a new **Check Leaked Password**. By defining scheduled tasks and making these searches continuous, you are aware of a potential data leak.

**BlaBla(Breach)** Home / BlaBla Breach

Company Controls

Company Name	Schedule Cron Jobs	Controls
Eu	0	0
****sec	1	4939
****S	0	0
****enerji	0	25
****K	2	294
****ç	0	0
Me	0	78
**** - Partner	3	81
	0	40

**BlaBla(Breach) / Unicrop - Partner Controls** Home / BlaBla Breach / \*\*\*\* - Partner

Last Controls Cron Jobs New Control

Username	Masked Password	Hash	Sources
m		7e0d62e2a93f9d94b03cf	N/A
e.		i636ea5f17d44e21269fb	N/A
e.		ie3f28125e060aa9e9390	N/A
i.t		4d0030aa86437e05c1eb6	N/A
m		dad331da8a61213c8d2c1	Stealer Logs
tu		e0e46efad7ba4ef2e8706	Dubsmash.com
bi		i69d9816a06cca86b46952	iMesh.com
kl			N/A



# Phish Data Configuration Guide

To activate attack phish data services via **the manager panel || Modules >> Phish Data** field should be reached.

The screenshot shows the ASPI POT interface. On the left is a dark sidebar with a menu: Modules (Attack Surface Monitor, Phish Data, Breach Data Control), IOC (Bad IP Pool, Proxy Pool), Usage & Support (Tickets, Licenses), and Profile (Profile, Logout). The main content area is titled 'PH Data' and includes a breadcrumb 'Home / PH Data List'. Below the title is a 'My PH Datas' section with a 'Create +' button. A central card displays '. PH for \*\*\*IS' with an 'UPDATING.' banner. Below the card are two columns: 'DATA' with a '2' and a refresh icon, and 'CONNECTED SERVICE' with 'N/A' and a refresh icon. At the bottom, it says 'Copyright © 2022 All rights reserved.'

Use the *Create* tab to search for a new PH data.

The screenshot shows the 'Create PH Data' form in the ASPI POT interface. The breadcrumb is 'Home / PH Data List / PH Data Create'. The form has the following fields: 'List Name' (text input with placeholder 'Name or PH List'), 'Company' (dropdown menu with 'Select Company'), 'Usernames' (text input with placeholder 'Input Usernames'), 'Keywords' (text input with placeholder 'Input Keywords'), and 'Other' (text input with placeholder 'Input Other words for PH'). A blue 'Create' button is located at the bottom left of the form.



# IOC's Data Usage Guide

IOC's services via **the manager panel || IOC** field should be reached.

IOC data can be accessed under the **the manager panel || IOC >> Bad IP Pool&Proxy Pool** tab.

**Proxy Pool** Home / Bad IP Pool

Proxy List / 2022-08-05 18:08:01

These IP addresses are collected from open communities that are used for Layer 7 Stress tests and illegal works and are presented to you in bulk. This list is presented after being checked 3-4 times a day.

IP	Port	Proxy Type
94.73.239.124	55443	https
94.74.163.220	80	https
94.233.39.70	8080	https
94.247.208.16	8123	https
94.74.163.195	80	https
94.74.163.218	80	https

Use the *Export CSV* or *API integration* to collect for a new IOC's.

43.130.7.75	United States	106	2 week ago
180.250.124.227	United States	122	2 week ago
138.68.162.6	United States	119	2 week ago
59.103.236.74	United States	127	2 week ago
213.74.115.162	United States	112	2 week ago
137.184.184.139	United States	154	2 week ago
159.89.40.119	United States	112	2 week ago
95.181.238.104	United States	29489	2 week ago
165.22.210.239	United States	109	2 week ago
112.133.228.250	United States	115	2 week ago

[Export to CSV](#)



# ADMINISTRATION GUIDE

## Licences

To activate licences via **the manager panel || Usage&Support >> Licences** field should be reached. All license management of the application is performed on this panel.

Cloud HoneyPot License List					
Name	IP	Services	Time to end	End Date	
*****	164.92.247.48	1	225 Day	2024-03-20 07:43:12	
*****EU	116.203.131.77	7	60 Day	2023-10-07 03:25:25	
*****servis	104.248.255.0	3	139 Day	2023-12-24 22:11:13	

Attack Surface Monitor License List					
Company	Asset Limit	Active Assets	Time to end	End Date	
*****	100	5	489 Day	2024-12-08 23:20:43	
*****IS	100	100	180 Day	2024-02-03 21:47:05	
*****erji	30	0	83 Day	2023-05-16 09:03:45	
IS*****	30	8	225 Day	2024-03-20 07:55:54	
*****t	20	16	3 Day	2023-08-11 01:54:14	
*****Merkezi	5	5	95 Day	2023-05-03 14:56:32	
AZN	50	0	59 Day	2023-10-05 14:23:16	

IOC   Pool Access Keys / Licenses					
Company	API Key	Access Proxy List	Access Bad IP Pool	Time to end	End Date
*****	e48e1c0b-11-52-52	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	204 Day	2024-12-08 23:20:43

License addition, deletion, new license request and modification operations are done here.

## Tickets

To send any request and information via **the manager panel || Usage&Support >> Tickets** field should be reached.

# Caspi PoT

