CaspiPoT

SECURITY GUARD

Defend Your Business Against the Latest Cyber Threads

”

Technical Documentation v2.0

Product overview

- Quick Start Guide
- Getting Started Guide

Planning

- Architecture and Deployment Guide

Installing

- Installation Guide

Configuring & Monitoring

- Honeypot Node Configuration Guide
- Attack Surface Monitor Configuration Guide
- Breach Data Control Configuration Guide
- Check WAF Configuration Guide
- Stress Tester
- IOC's Data Usage Guide

Administration

- User & Report Guide
- 3rd Party Integration Settings

Tickets

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

Quick Start Guide
Version 2.0

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.

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.caspipot.com/support/1905).

Contacting customer support for information about contacting customer support, see the Support and Download Technical Note (http://caspipot.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

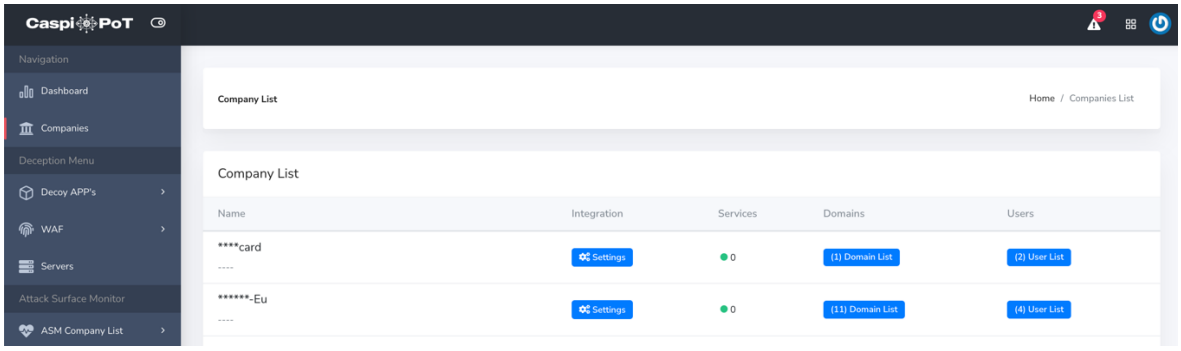
When you plan or create your CaspiPoT Security Guard deployment, it's helpful to have a good awareness of CaspiPoT architecture to assess how CaspiPoT Security Guard components might function in your network, and then to plan and create your CaspiPoT deployment. CaspiPoT processes, aggregates, and stores 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.

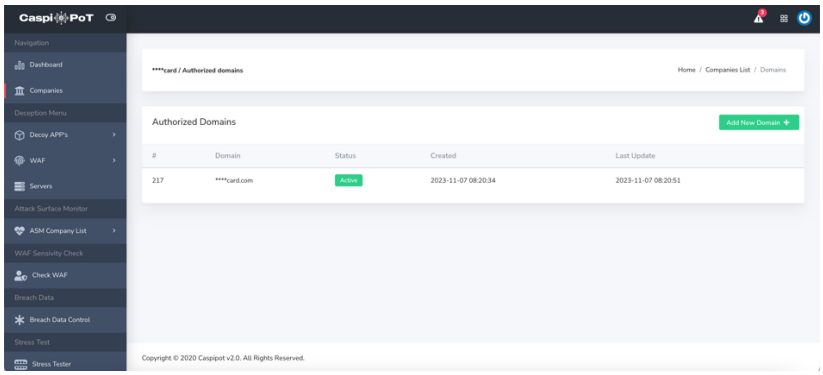
CASPIPOT COMPONENTS

CLOUD HONEYPOT Services Rules Waf	**BREACH DATA CONTROL**	**ATTACK SURFACE MONITOR** Vulnerability Scanner Asset Status Control Blacklist Control
Check WAF	**IOC's** Bad IP Pool Proxy Pool Payload Pool	**Stress Tester**

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**





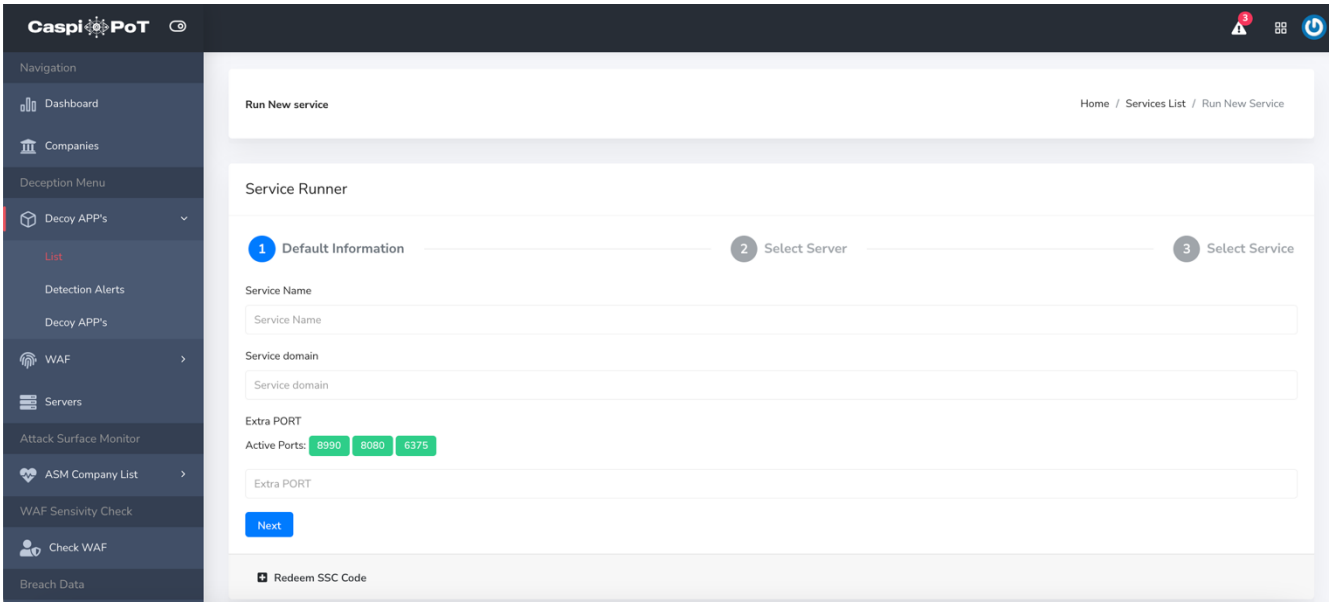
After the approved registration of your **domain name** is completed, the domain name is automatically added to **Authorized Domains** list.

CONFIGURING

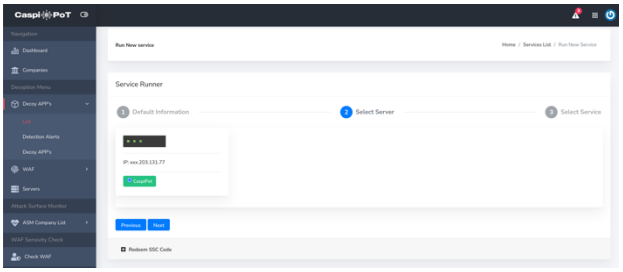
Honeypot Node Configuration Guide

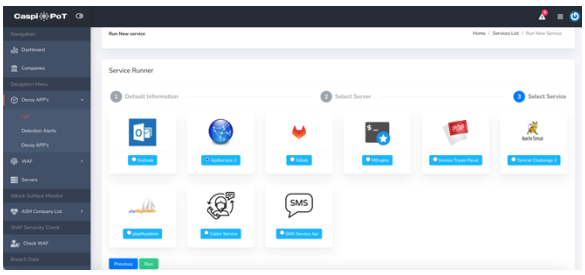
To activate honeypot services via the **Caspipot Manager Panel || Deception >> List >>> Create** field should be reached.

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



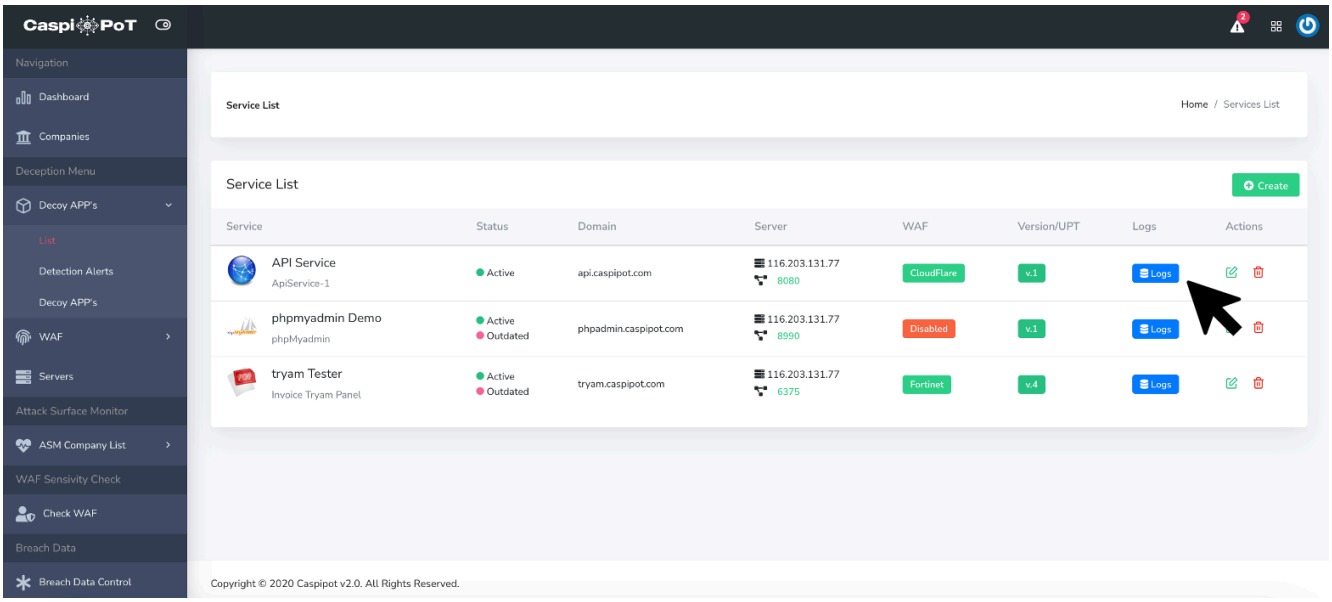
With the defined information, the area where you can choose from among the servers defined in different datacenters around the world will be displayed to within the scope of the license type.



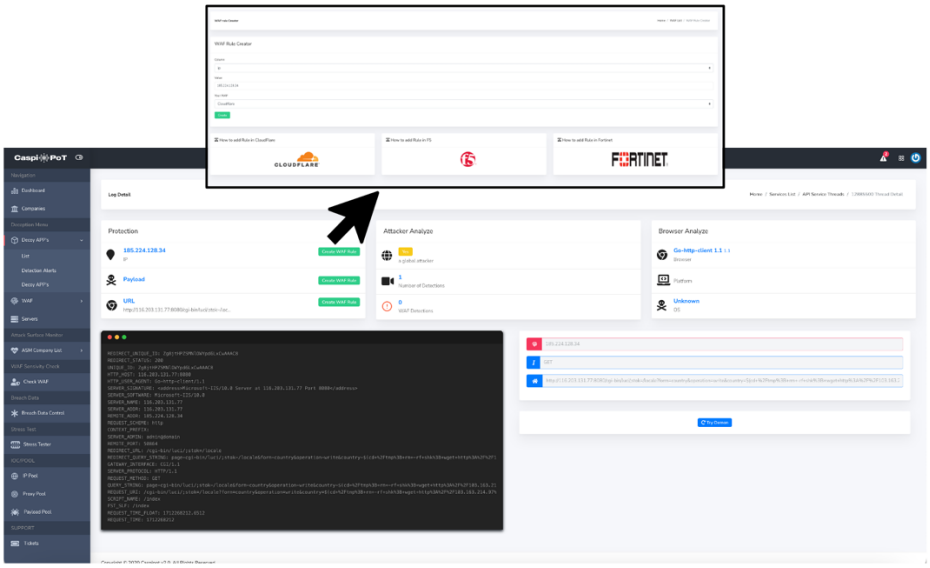


These are the things that need to be done in order to take a **service live**.

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 **Caspipot Manager Panel || Deception >> Decoy APP's >>> List**

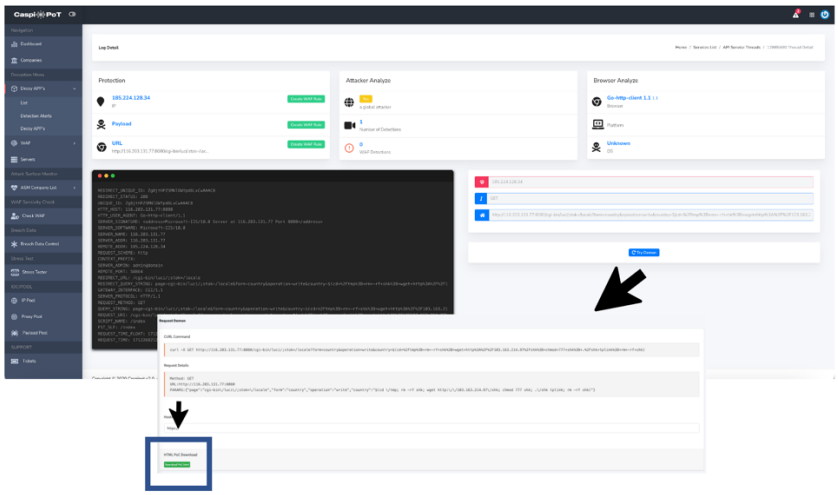


Logs field should be accessed to list the attacks on your services and write new rules



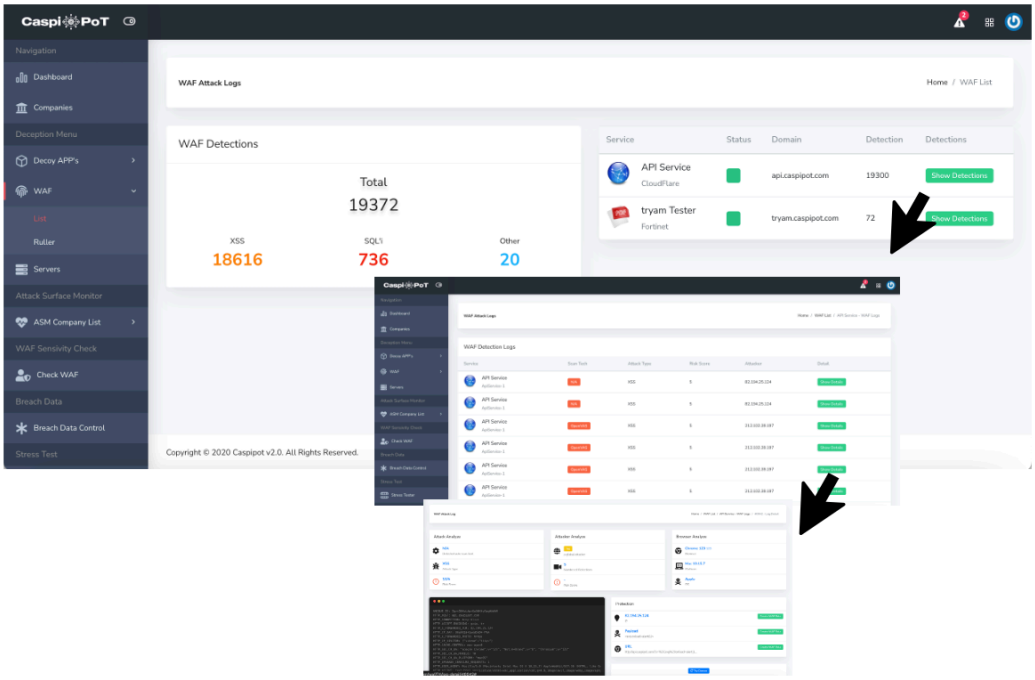
You can define your detailed **rules** for **IP, PAYLOAD AND URL.**

With the **TRY DEMON** button you can *simulate* an attack on your applications and with the **Download PoC** option you can test the same attack vector on your own computer..

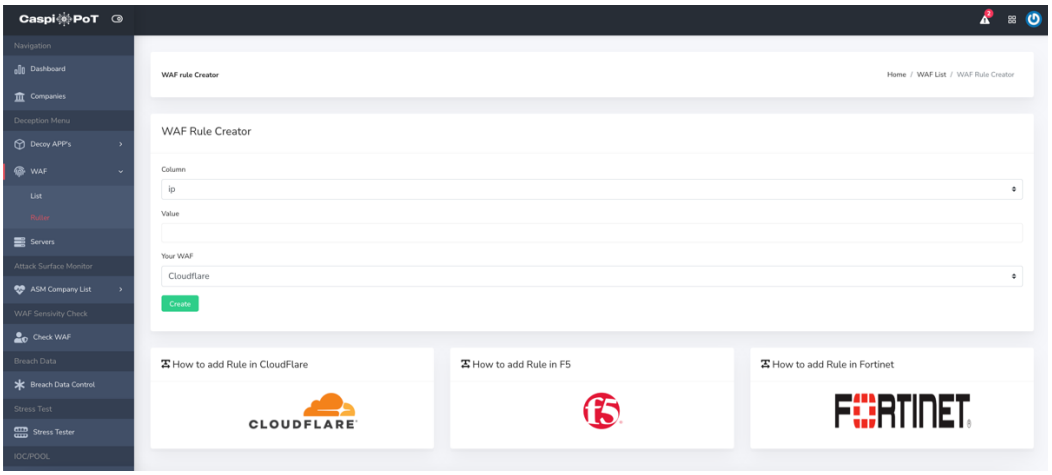


Honeypot WAF services via the **Caspipot Manager Panel || Deception >> WAF >>> List** field should be reached.

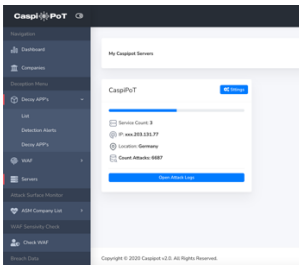
To see the statistics of the attacks and to write new rules for incoming attacks, just click on the P field.



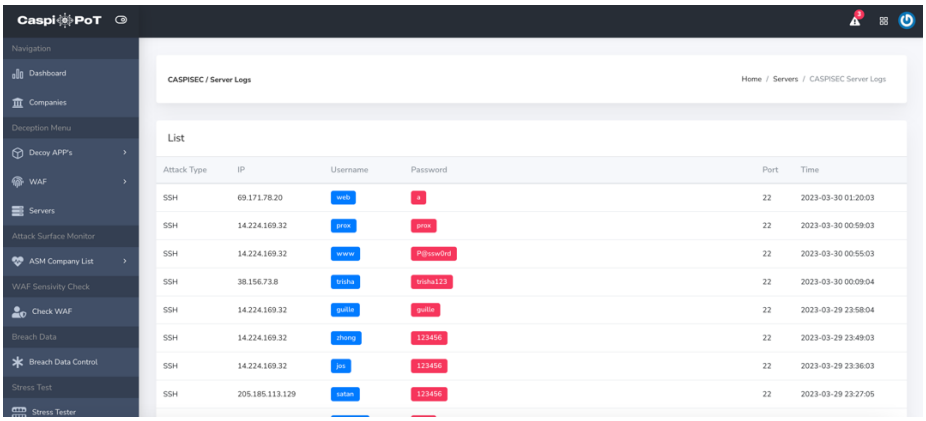
To write **new rules** for incoming attacks toHoneypot WAF Ruller services via the **Caspipot Manager Panel || Deception >> WAF >>> Ruller** field should be reached.



To Access your licensed servers, **Caspipot Manager Panel || Deception >> Decoy APP's >>> Servers**



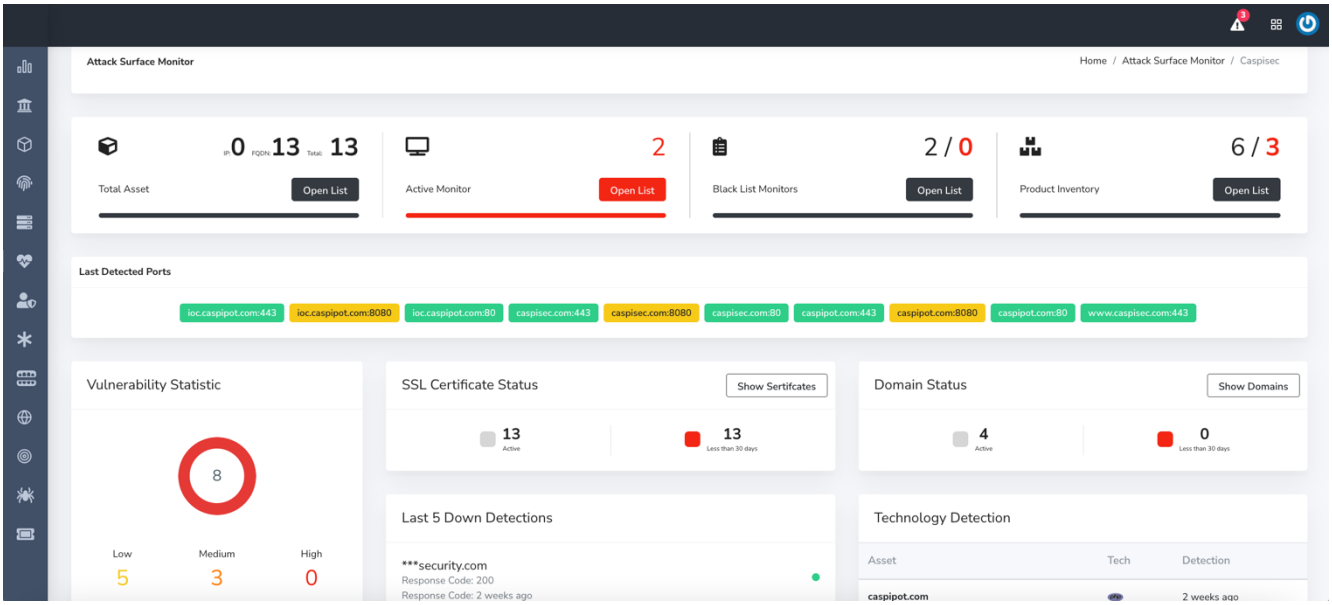
With the operations performed, attacks on services that are now defined begin to be detected. **Important rules** can be written for the listed attack types and critical situations. You can receive **hourly**, **daily**, **monthly** reports on detected attacks and automatically forward them to the relevant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



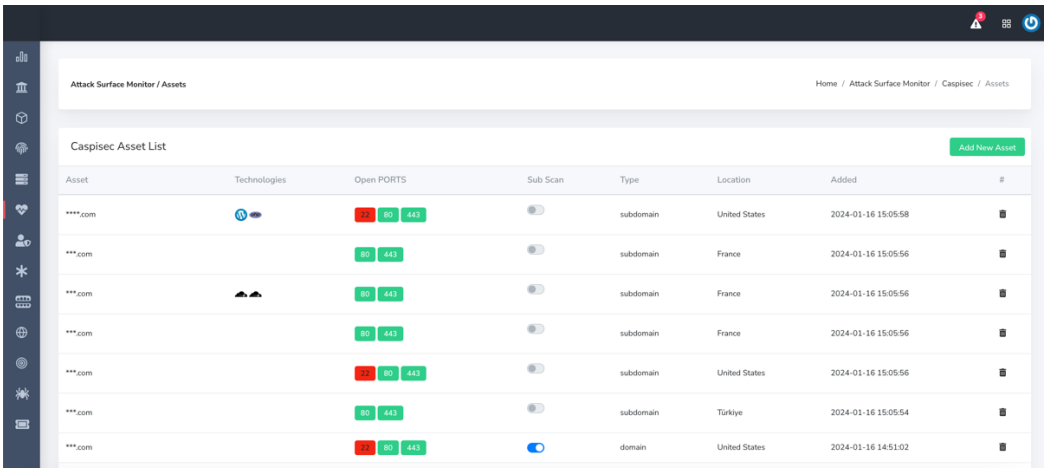
Attack Surface Monitor Configuration Guide

To activate attack surface management services via **Caspipot Manager Panel || 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.

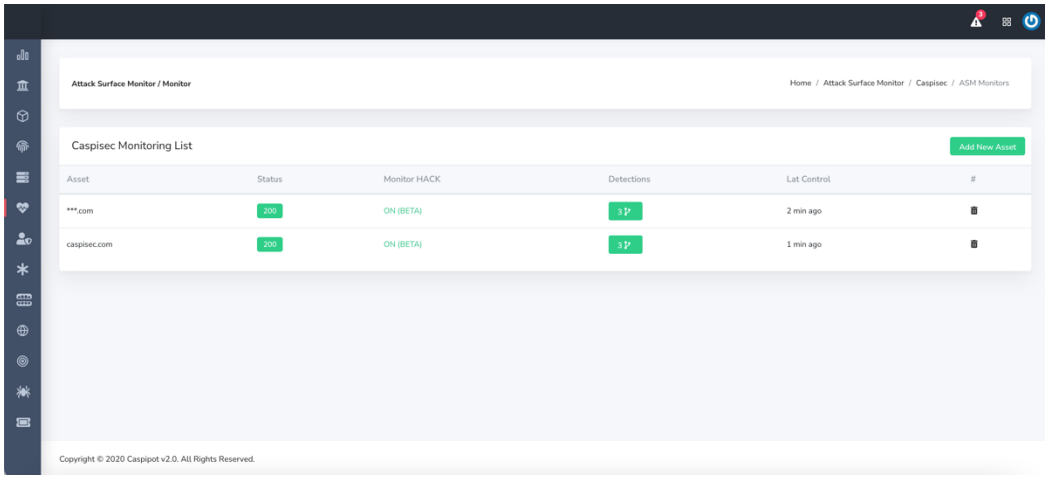


With the correct entry of the information, the system will automatically scan the **Technology**, **Port**, **Vulnerability** information of the added asset and display the results in a short time.

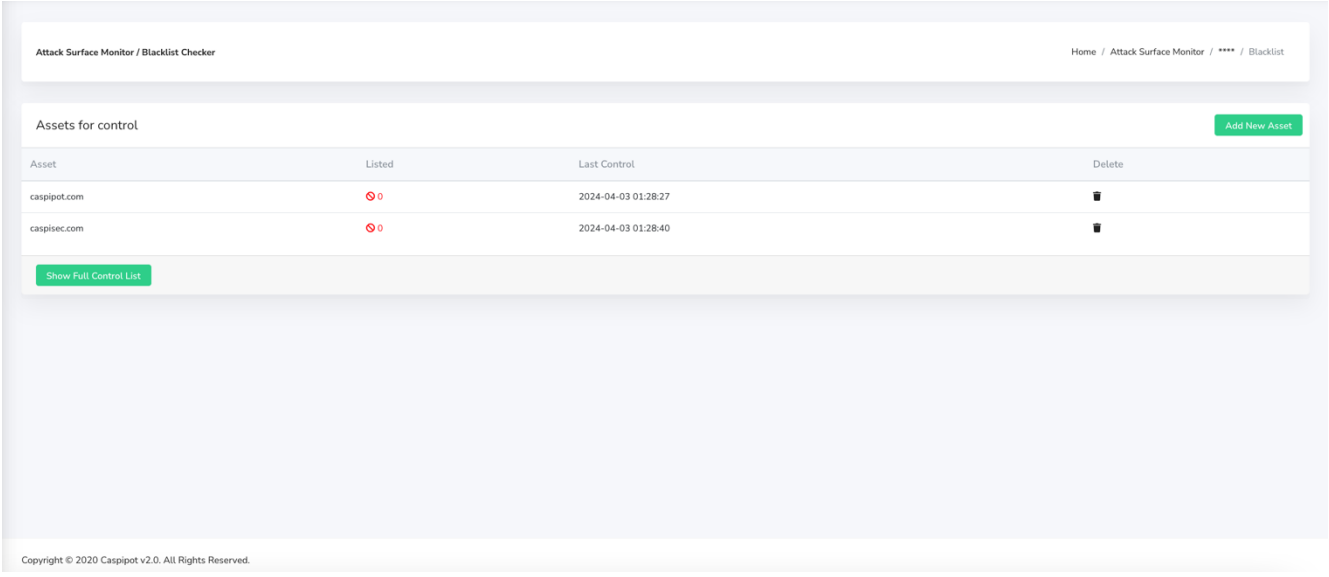


Active Monitor allows you to monitor the health status of all your inventory that provides internet service that is open to the world. **Caspipot Manager Panel || Attack Surface Monitor >> Active Monitor** field should be reached.

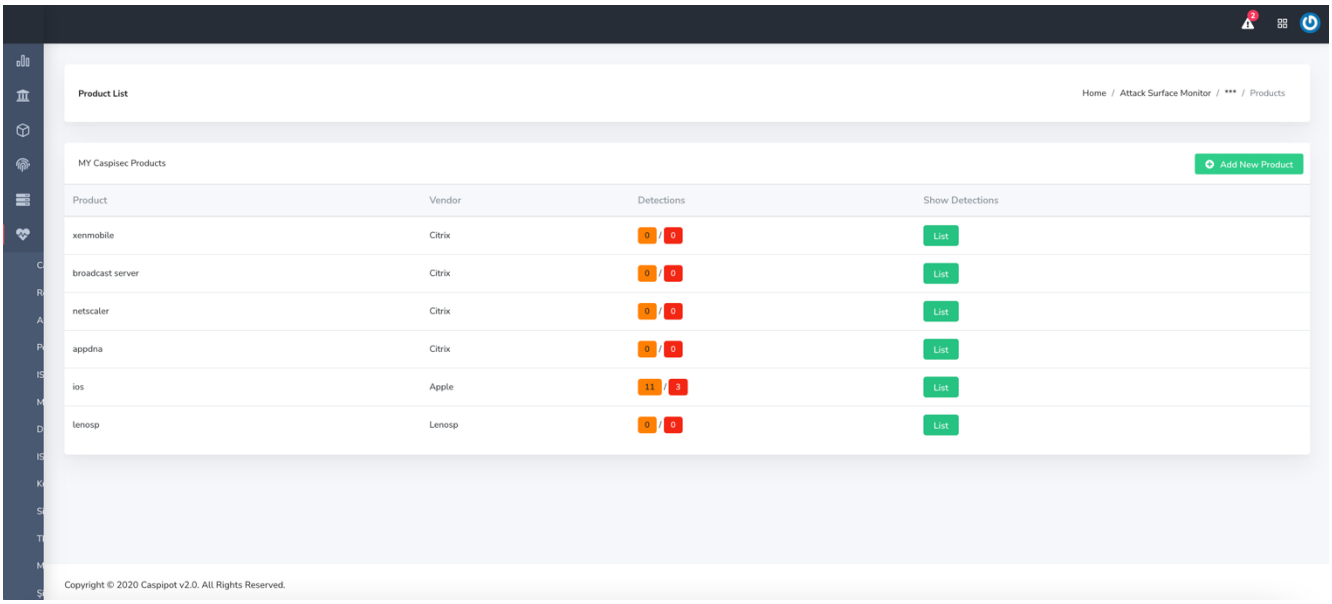
You can add **New Assets** from here



Black List Monitors allows you to monitor the black list status of all your inventory. **Caspipot Manager Panel || Attack Surface Monitor >> Black List Monitors** field should be reached. You can add **New Assets** from here.



Product Inventory allows you to monitor last vulnerability and CVE status of all your inventory. **Caspipot Manager Panel || Attack Surface Monitor >> Product Inventory** field should be reached. You can add **New Assets** from here.

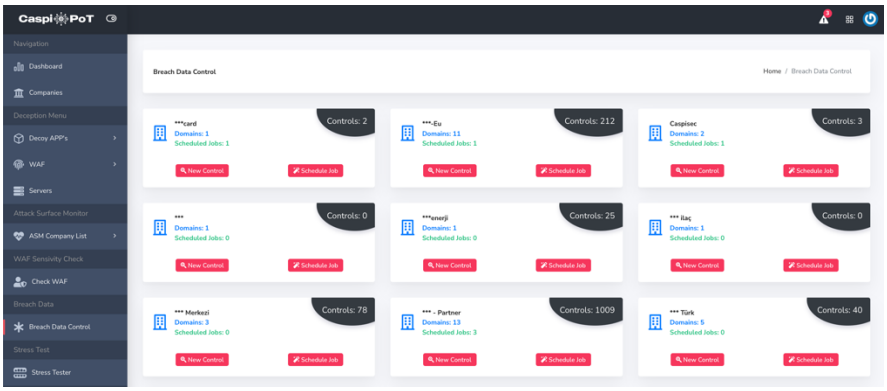


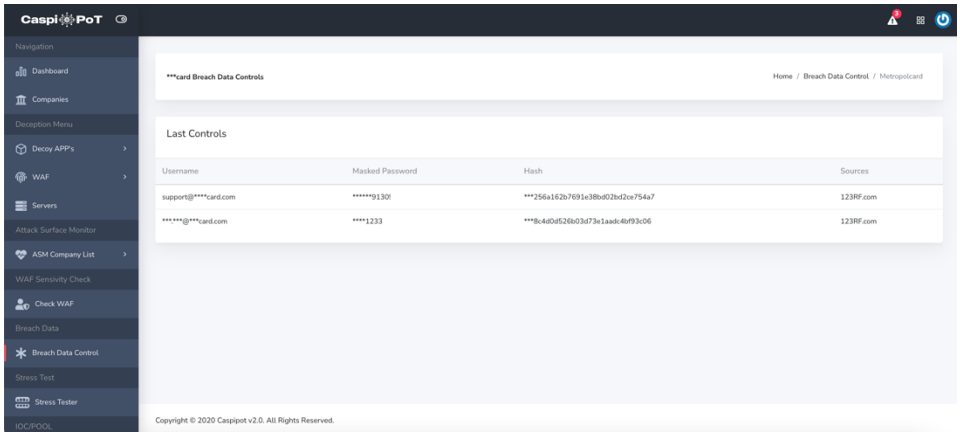
Breach Data Control Configuration Guide

To activate breach data services via the **Caspipot Manager Panel || 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 permissions for the company are displayed.

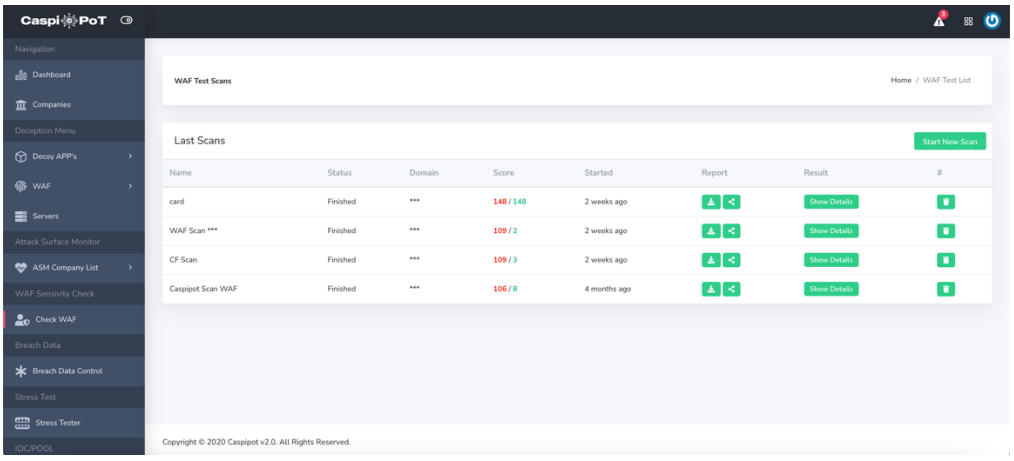
You can view *existing stolen* data by creating a new **Check Leaked Password**. By defining scheduled tasks and making these searches continuous, you are aware of a potential data leak.



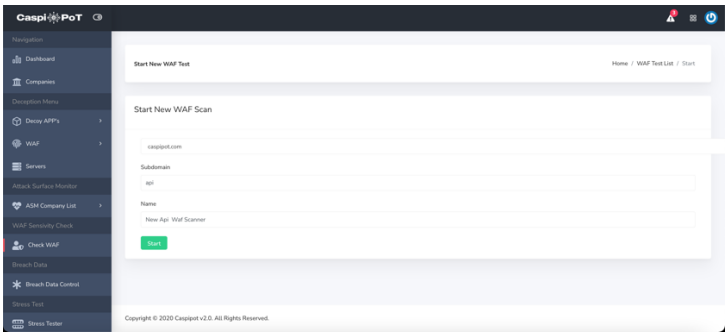


Check WAF Usage Guide

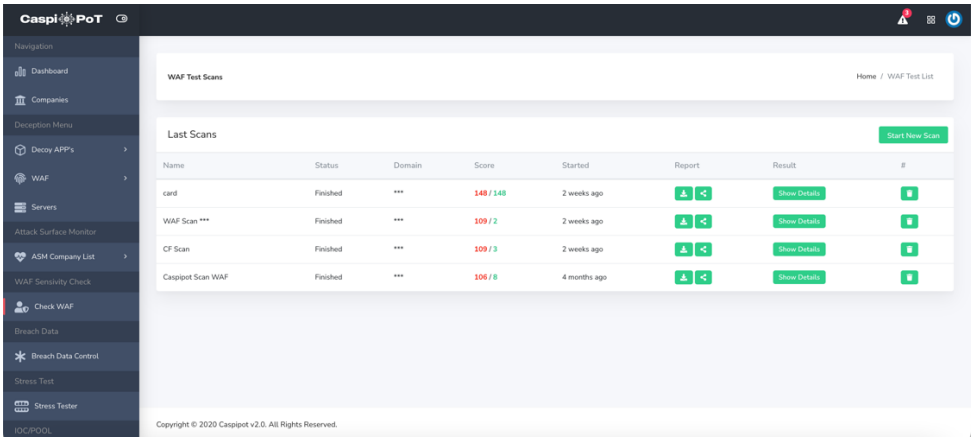
To activate Check WAF services via **Caspipot manager panel || Check WAF** field should be reached.

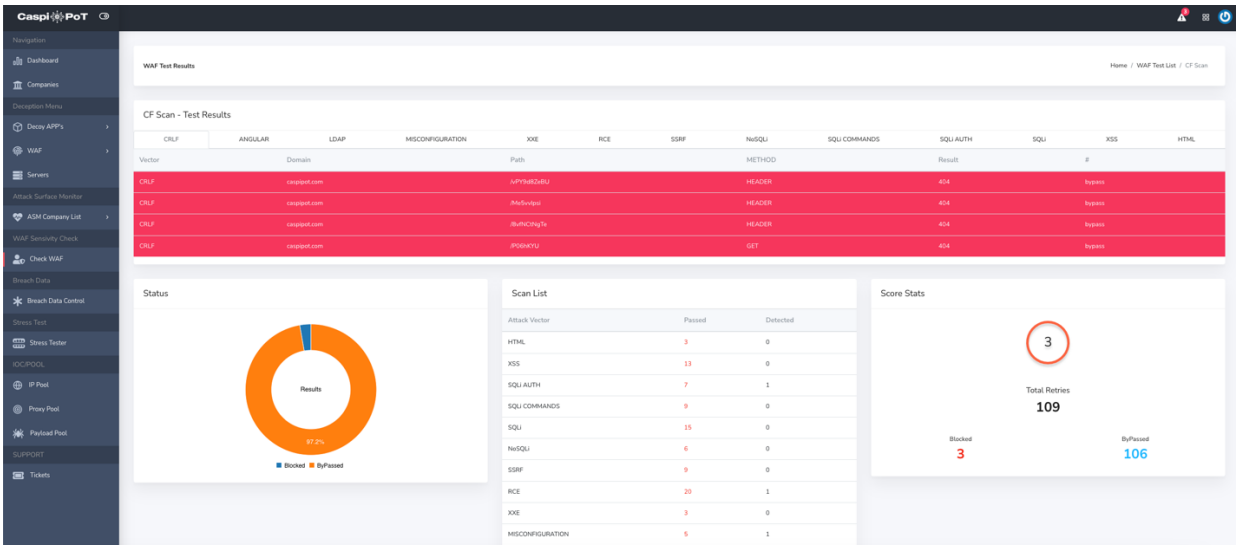


Use the ***Start New Scan*** tab to test for a new WAF.



After the new scan you can **Download, Share** (generates a 24-hour download link) and **Show** your test details.

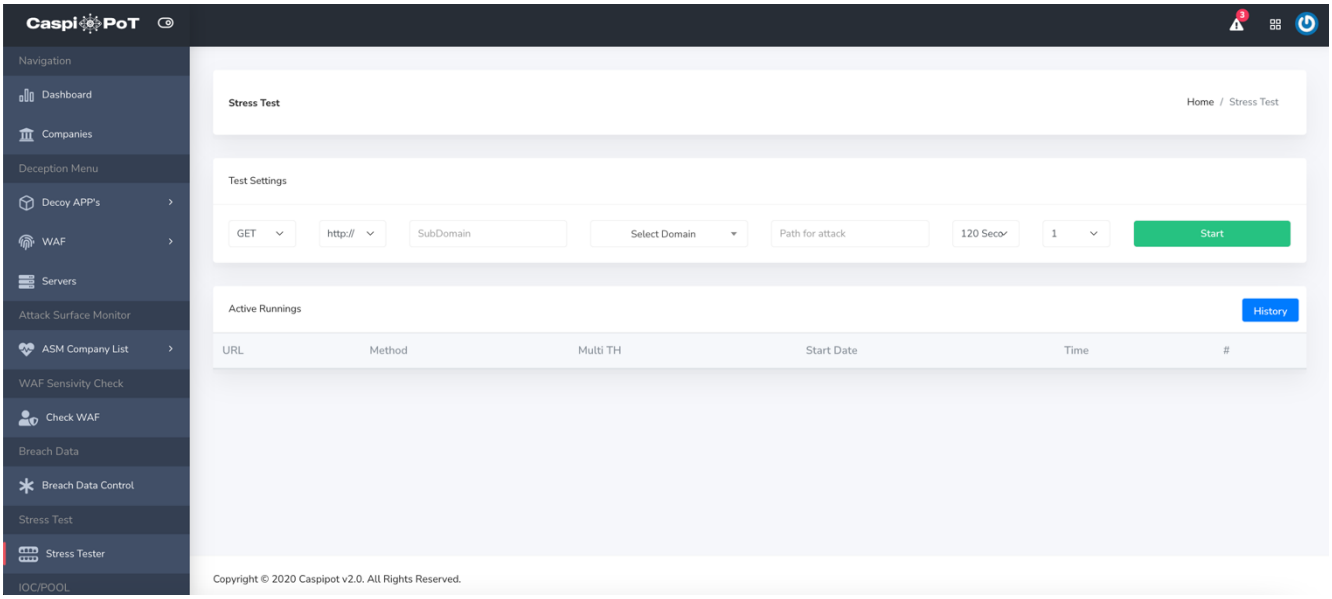




Stress Tester Usage Guide

Stress Tester services via the **Caspipot manager panel || Stress Tester** field should be reached.

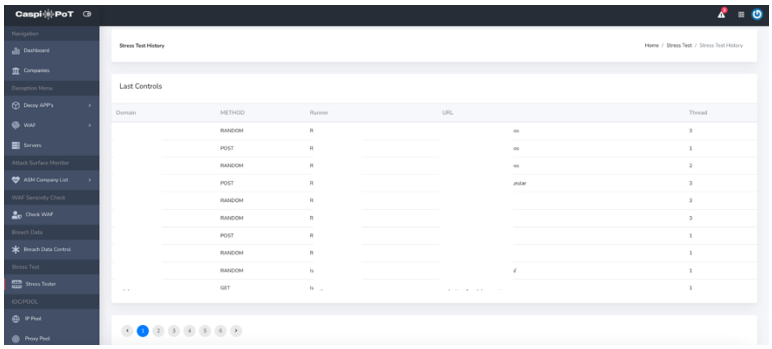
The Stress module is designed to measure the resilience of the current system by sending distributed **http/https requests** to a **specified target**. During the tests, a user-specified main **domain**, **subdomain** or **designated folder** can be attacked.



During the attack, it transmits **GET**, **POST**, **HEAD**, **OPTIONS**, **PUT**, **DELETE** sample requests.

The company domains selected to start a new test consist of a list of domains added from the company settings defined in the existing company's account.

True: caspipot.com
True: blog.caspipot.com
True: caspipot.com/blog/
False: caspipot.com/?parametre=parametre

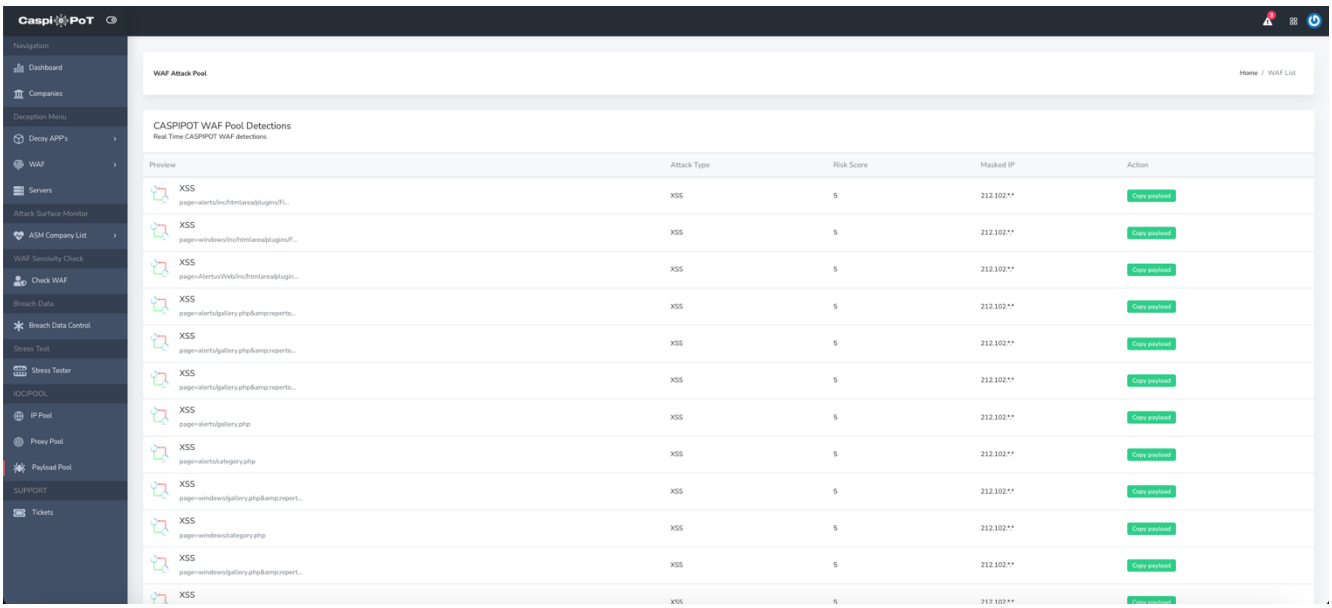


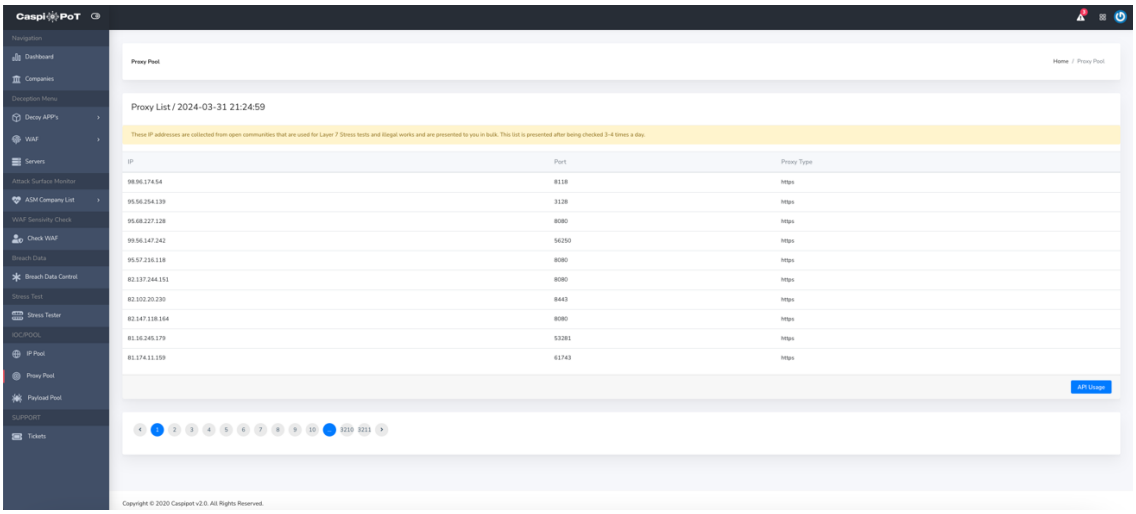
Upon completion of the stress test, you can list the **history** of all tests.

IOC's Data Usage Guide

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

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



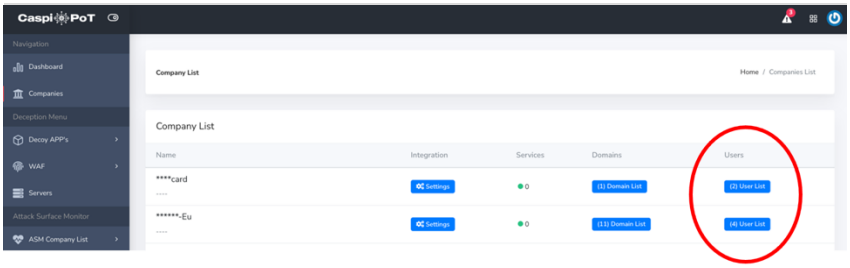


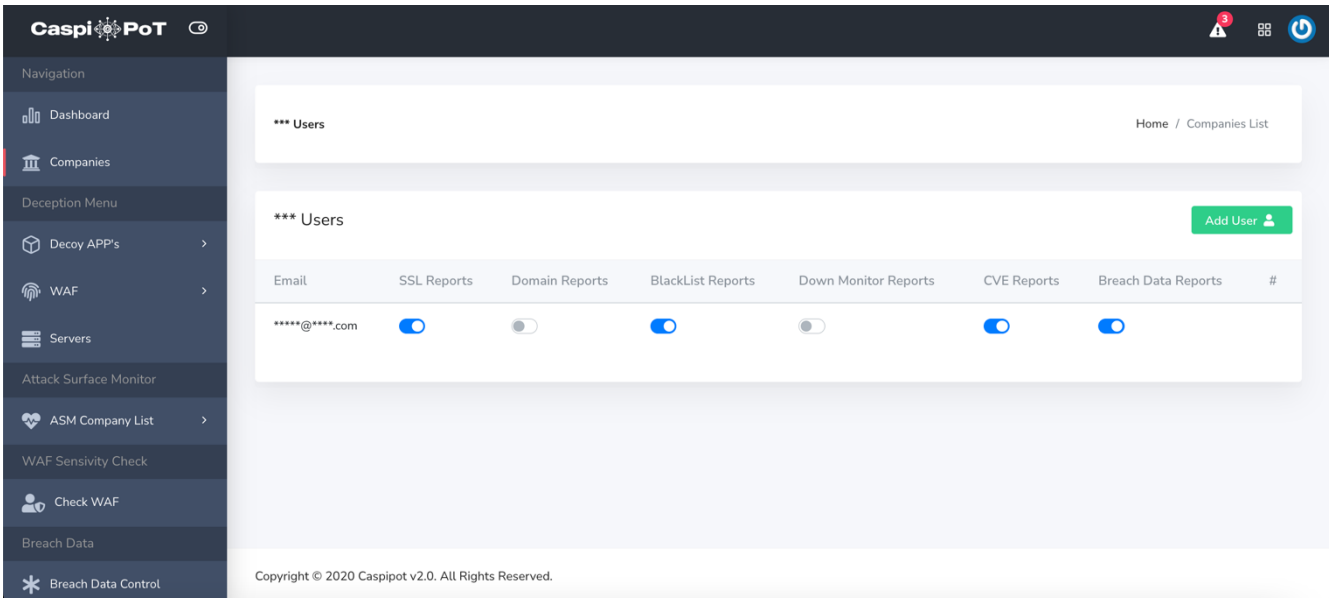
Use the ***Export CSV*** *or* ***API*** *integration* to collect for a new IOC's.

ADMINISTRATION GUIDE

User & Reports

You can make arrangements for user management, adding new users and sharing of reports from the **Caspipot Manager Panel || Companies >> Users List**

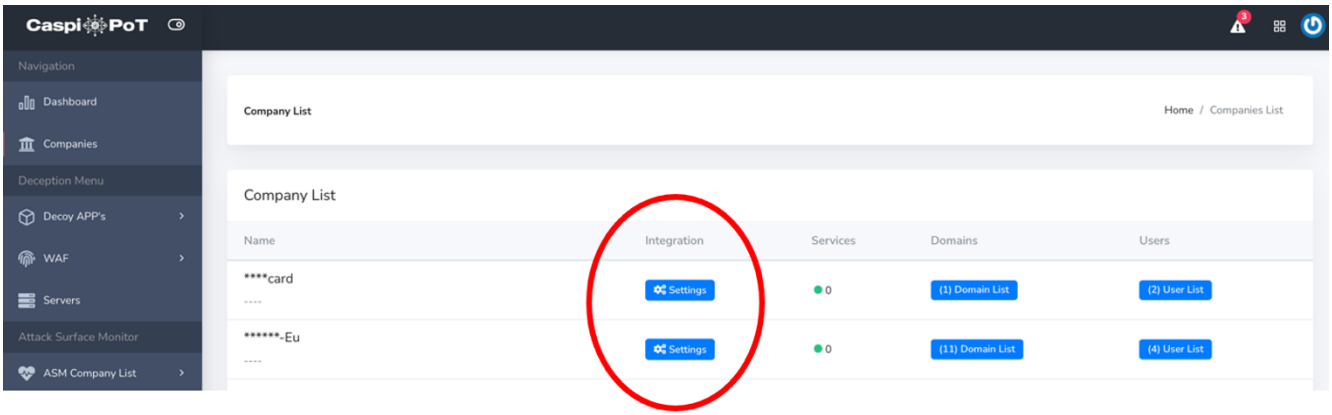




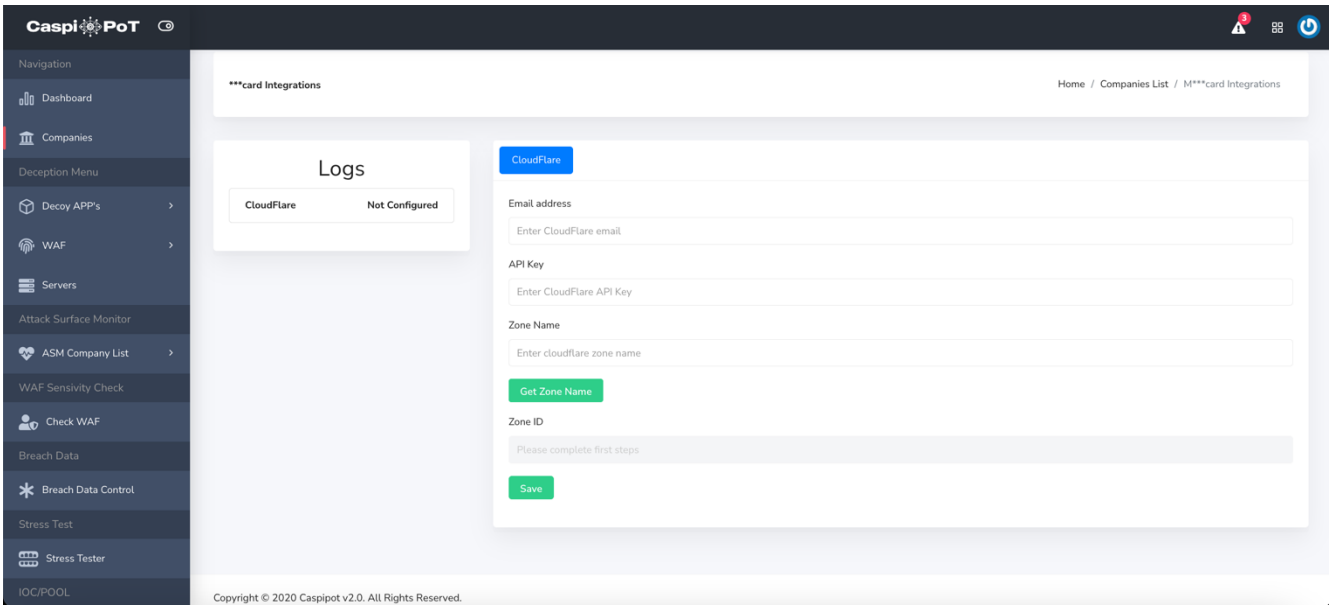
All reports are generated daily and sent to defined users via e-mail.

3rd. Party Integration

You can make 3rd party integration from the **Caspipot Manager Panel || Companies >> Integration >>> Settings**



By selecting the appropriate solution for your products, you can activate the service by entering the requested information completely.



Tickets

To send any support request or information via **the Caspipot Manager Panel || Usage&Support >> Tickets** field should be reached.

www.caspipot.com

CaspiPoT