


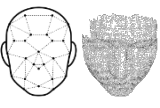




EagleEYE Identity and Access Management (IAM)

EagleEYE, an Identity and Access Management product, includes 3 main modules. Identity Management, Password Management and Privileged Access Management.

Identity Management - IdM, is to ensure that the right users have access to the right resources at the right time, for the right purposes, in order to ensure computer and network traffic security. Fulfills the need for access to appropriate resources and compliance requirements. EagleEYE Identity Management module closes the user authentication vulnerability, which is one of the most important vulnerabilities in cyber security. Access tracking; It is the monitoring screen that shows the servers, clients and applications accessed by staff and all users in real time. The transactions made on the basis of the selected user are followed and examined. It checks for policy violations.

With Strong Validation, access to the computer is done with biometric verification methods. High security vitality verification is provided by finger biometrics and iris. All operations performed on the screen and the applications used are recorded. EagleEYE automatically closes the application or session when the user leaves the screen or an unauthorized person looks at the screen with its face recognition module. Face recognition is done with our software module and any 3rd party camera (standard camera on a portable computer).

EagleEYE biometric authentication components; It consists of facial recognition and tracking and other biometric comparison software, finger biometrics or iris scanners capable of fake finger and vitality detection, and a WEB camera.

 <p>Finger print</p>	<p>Fake fingerprint and liveness detection, encrypted template support, 19794-2/4 and custom templates...</p>	 <p>Face Recognition</p>	<p>2 and 3-dimensional face recognition algorithms. Vitality and fever measurement support, mask control.</p>	 <p>Iris Recognition</p>	<p>Live iris template support, iris and face fusion combined support</p>
 <p>Contactless Fingerprint</p>	<p>Contactless 3D fingerprint. 4 fingers together and very fast...</p>	 <p>Finger Vein Print</p>	<p>Finger vein pattern, vitality recognition and fake finger detection. 10-8 FAR...</p>	 <p>Palm Vein Print</p>	<p>High sensitivity and non-contact pass support with palm vein patterns...</p>



It has open API and WEB service support to add new devices and services with a wide range of device support.

Few applications support multi-factor access (MFA). It is necessary to encourage/enforce strong authentication before automatic password reset.

1. All users are directed to use MFA and even required users to use SA (Strong Authentication). 2. Send PIN from phone / email. 3. With the smartphone application, both login via smartphones (using a factor we carry / own) are supported, and the smartphone is used as a biometric verification device (without using an additional device with our mobile biometric verification application). 4. Existing OTP systems can be integrated. 5. Fingerprint, contactless fingerprint, finger vein print, palm vein print, face and iris technologies are supported to eliminate 2FA security problems. 6. Strong validation (SA) is done by viability check.

Password Management module is a secure vault application that securely stores and manages sensitive information such as passwords, documents and digital identities of employees.

Password Management is a fast and secure solution for users to reset their passwords and/or open blocked accounts without assistance from the service desk in institutions. It supports multiple authentication methods and service desk integration, reducing the workload of IT teams and increasing security.

Users and system security is enhanced by Strong Authentication.

Transactions such as password reset, opening blocked accounts are monitored and reported in real time. Automatically problem records are opened, updated and closed in the ticket system. All these processes are easily monitored and controlled with a browser-based interface.

The majority of users have many different passwords. These passwords are written on a note paper on the computer or on the desk and/or stored in a file inside the computer. In applications that are constantly asked to change the password, it becomes very difficult to change the password after a while, the passwords are forgotten / confused and the need for support arises. It is a laborious process for both the user and the support team and causes a waste of time. A secure password cannot be created every time.

Privileged Access module is one of the important digital workflow problems of institutions; accounts with high privileges that are shared among many people, static passwords that create security problems, passwords that are known by many people and who's responsibility is not described, provide solutions to the problems caused by people who have left the institution and still have access. Eliminates password fatigue and security flaws by providing a secure, centralized vault for password storage and access. Increases IT efficiency by automating the frequent password changes required in critical systems. Provides preventive and detective security controls through approved workflows and real-time alerts for password access. Provides security controls and regulatory compliance. It is monitored / managed / controlled that which accounts the personnel use instantly, what changes are made, whether there is an abnormality in access, compliance with rules and policies, and whether security is in danger.

It organizes all your privileged identities by storing them in a centralized vault. It allows you to securely share your passwords with members of your team on a need-based basis. It automatically resets the passwords of servers, databases, network devices and other resources.

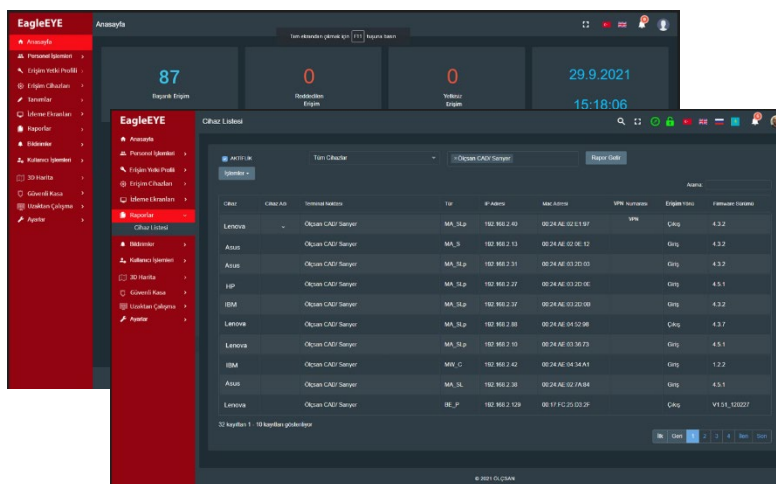
Controls access to IT resources and applications based on roles and job responsibilities. Initiates direct connections to remote IT resources, websites and applications. Makes video recording and auditing of all privileged accounts, has a complete record of all actions.

Advantages & Technical Superiorities

- EagleEYE does not allow unauthorized users to access end devices and system.
- Takes Authentication to the highest level of security using Strong Authentication.
- In the system, users can access methods and devices with different security levels with a hybrid policy.
- It also supports standard 2FA, MFA methods.
- It allows users to easily register and manage the system from the interface.
 - It comes with an ergonomic user interface.

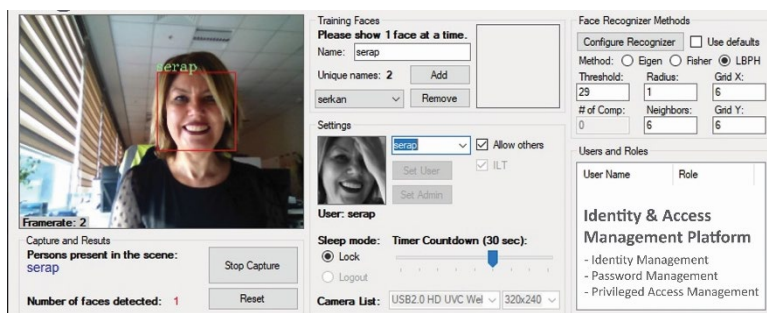
EagleEYE achieves high performance and efficiency by using multi-core architecture. It performs face recognition and screen security functions without slowing down the operations of the computer at the endpoint where it is installed, without requiring an additional device and hardware according to its hardware features.

EagleEYE is a application designed for secure computer and application access, screen security and user authentication.



Why is EagleEYE more secure?

- Protects both your screens and applications.
- Provides high accuracy with biometrics.
- It prevents password rollover and password weaknesses.



Face Tracking App

Authentication of people with a standard fingerprint scanner and/or WEB camera has weak points.

Standard fingerprint scanners and cameras do not have fake finger/photo detection capabilities.

EagleEYE; It is integrated with 3rd party applications such as SIEM, SOAR, Threat Intelligence. It can be also easily integrated into any commercial and open source applications.