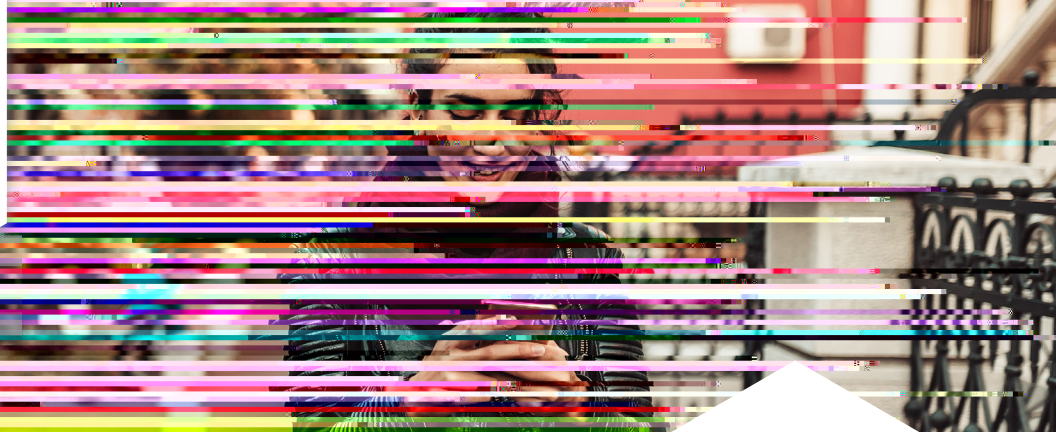




ENTRUST



Entrust Identity - Adaptive Risk-Based Access and Authentication

Market Challenge

- Organizations are struggling to manage the risk of identity theft and data breaches
- Traditional authentication methods are often cumbersome and user-unfriendly
- Users are frustrated by complex login processes and security questions

Solution

- Entrust Identity provides a secure, user-friendly authentication solution
- Adaptive risk-based access and authentication adjusts security based on user behavior and context
- Supports a variety of authentication methods, including biometrics, mobile devices, and traditional passwords
- Provides a seamless user experience while maintaining high security standards
- Reduces the risk of identity theft and data breaches
- Improves user productivity and satisfaction
- Integrates with existing systems and applications
- Offers comprehensive reporting and analytics
- Provides 24/7 customer support and training

BENEFITS

- Reduces the risk of identity theft and data breaches
- Improves user productivity and satisfaction
- Supports a variety of authentication methods, including biometrics, mobile devices, and traditional passwords
- Provides a seamless user experience while maintaining high security standards
- Reduces the risk of identity theft and data breaches
- Improves user productivity and satisfaction
- Integrates with existing systems and applications
- Offers comprehensive reporting and analytics
- Provides 24/7 customer support and training

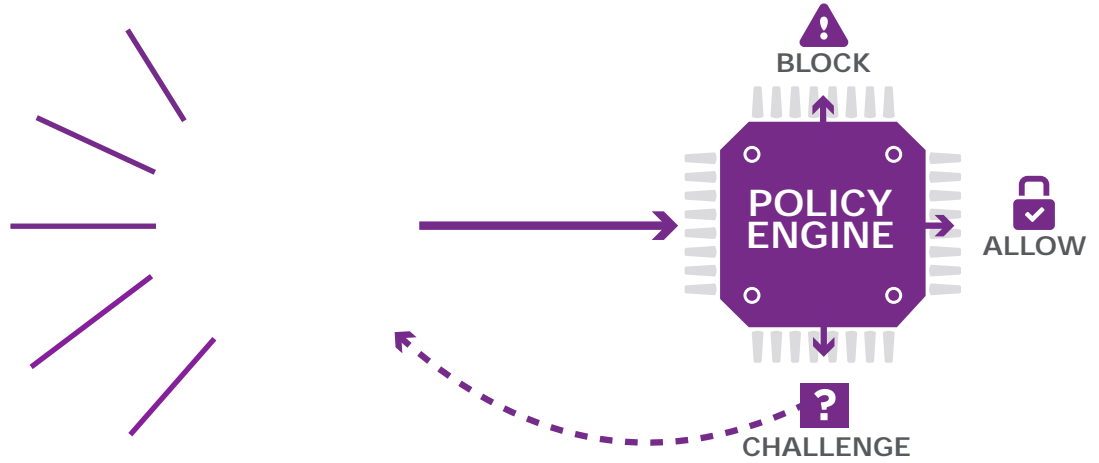
At a glance

Entrust Identity provides a secure, user-friendly authentication solution that adapts to the risk of identity theft and data breaches. It supports a variety of authentication methods, including biometrics, mobile devices, and traditional passwords. This solution improves user productivity and satisfaction while maintaining high security standards. It integrates with existing systems and applications and offers comprehensive reporting and analytics. Entrust Identity provides 24/7 customer support and training.

- Adaptive risk-based access and authentication
- Supports a variety of authentication methods
- Provides a seamless user experience
- Reduces the risk of identity theft and data breaches
- Improves user productivity and satisfaction
- Integrates with existing systems and applications
- Offers comprehensive reporting and analytics
- Provides 24/7 customer support and training



Entrust Identity - Adaptive Risk-Based Access and Authentication



HOW IT WORKS

When a user attempts to access a resource, the system evaluates the user's identity and the context of the request. This includes factors such as the user's location, the time of day, and the device being used. The system then compares these factors against a set of predefined policies to determine the level of risk associated with the request.

Based on the risk assessment, the system can either allow access, block access, or challenge the user. For example, if the risk is high, the system may require the user to provide additional authentication factors, such as a one-time password or a biometric scan. If the risk is low, the system may allow access without any additional authentication. 

The system continuously monitors the user's activity and adjusts the risk level in real-time. For example, if the user is performing a sensitive operation, the system may increase the risk level and require additional authentication. If the user is performing a routine operation, the system may decrease the risk level and allow access without any additional authentication.

Policy engine

• Ինչպես որոշել, թե արդյոք հարկադրված է օգտագործել անվտանգ միջավայրում:

Device certificate

• Կարող եմ օգտագործել իմ սարքի վրա ստեղծված անվտանգ միջավայրում:

IP geolocation

• Կարող եմ օգտագործել իմ սարքի վրա ստեղծված անվտանգ միջավայրում:

• Կարող եմ օգտագործել իմ սարքի վրա ստեղծված անվտանգ միջավայրում:

• Կարող եմ օգտագործել իմ սարքի վրա ստեղծված անվտանգ միջավայրում:

• Կարող եմ օգտագործել իմ սարքի վրա ստեղծված անվտանգ միջավայրում:

• Կարող եմ օգտագործել իմ սարքի վրա ստեղծված անվտանգ միջավայրում:

