



Identity Security Platform

MFA, SSO, PAM, Self-Service and ITDR — In One Unified Approach

Identity-first Security

MIRKET

Unified Identity Security Platform

Mirket delivers every component of end-to-end identity security — **MFA, SSO, PAM, Self-Service Portal and ITDR** — within a single integrated platform. With full **passwordless authentication** it eliminates password-based vulnerabilities, while creating a simple and fast access experience for users. Through its hybrid architecture and multi-tenant design, MSSPs can manage multiple customers from a single point with isolated tenant structures.



Multi-Factor Authentication (MFA)

We see that hackers find stealing credentials more practical than exploiting security flaws. This is not only because credentials are easier to obtain, but also because they allow attackers to operate within legitimate accounts and bypass security controls more easily. This is exactly why **Multi-Factor Authentication (MFA) matters so much**.

Mirket MFA, is a state-of-the-art multi-factor authentication solution designed to elevate organizations' digital security to the highest level. By securing user access with multiple verification layers that go beyond passwords, Mirket MFA provides a strong defense against modern cyber threats. The solution covers a broad range of use cases — from local user accounts to corporate networks, and from VPN connections to critical server access. Its multi-factor authentication methods form a comprehensive protective shield for safeguarding digital identities.



16 billion
exposed credentials

(Cybernews, 2025)



88%
Share of cyberattacks that
rely on stolen credentials

(Verizon)



99%
Of incoming attacks can be
blocked using multi-factor
authentication

(Microsoft)

Mirket MFA, strengthens organizations' security infrastructure with the following capabilities:

- Mirket MFA offers broad integration with enterprise systems through support for **RADIUS, LDAP Proxy, ADFS, SAML, OAuth, OpenID Connect and REST API**.
- It enables seamless integration with diverse identity sources such as local users, **Active Directory, LDAP (OpenLDAP), Microsoft Entra ID and Google Workspace**.
- Mirket MFA enforces multi-factor authentication across all critical access points, including **RDP, SSH, VPN, OWA/ECP, operating system logon (OS logon), privilege escalation operations, ActiveSync, web applications, legacy applications and SaaS applications**.
- Mirket MFA supports a variety of authentication methods such as **push notification, biometric authentication, TOTP, passwordless authentication, SMS and e-mail**.
- With mobile app support across **iOS, Android and Huawei platforms**, Mirket MFA delivers a secure and user-friendly authentication experience, and works seamlessly with third-party authenticator apps.

Mirket MFA, Mirket MFA provides a powerful and versatile solution for securing user access across different environments, helping organizations reduce risk and preserve operational integrity.

Platforms & Gateways

Hybrid SaaS Platform On-Prem RADIUS
LDAP Auth Proxy

MFA Methods

Passwordless Mirket Token Online OTP
Offline TOTP Push SMS / E-Mail Biometric
FIDO2/U2F

Agents

OS Logon OWA Agent Active Sync ADFS

Self Service User Portal (SSP)

User Experience and Account Security

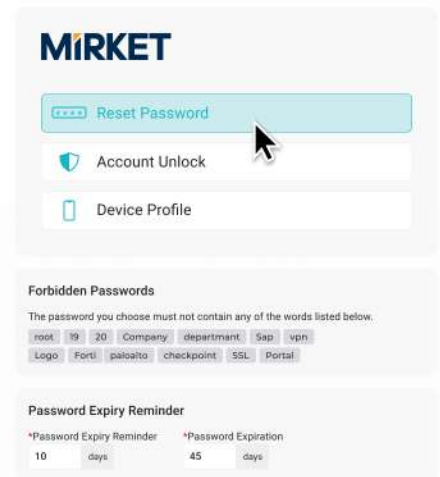
Empower users to manage their own security settings, reducing the need for IT support while increasing overall security. Make it easy for users to handle their essential security tasks:

- **Password Reset:** Reset or update passwords quickly.
- **Account Unlock:** Secure, MFA-based account recovery.
- **Device Access:** Review and revoke device authorizations.

Operational Efficiency

The self-service portal lets users independently perform routine security tasks such as password resets, account unlocks and device management. This reduces the IT workload, lowers operational costs and improves the user experience.

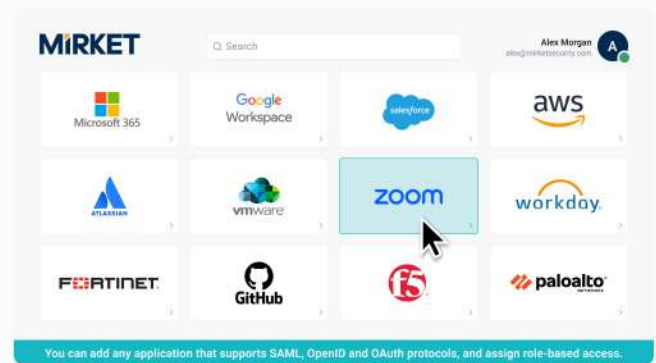
- **Less Dependency:** Users resolve common issues on their own.
- **Automation for Recurring Tasks:** Streamlines frequently performed operations.
- **Lower IT Costs:** Frees up resources for critical tasks.



Single Sign-on (SSO)

With Mirket's intelligent and integrated Single Sign-On platform, simplify access across all environments, strengthen your security posture and boost user productivity.

- Advanced MFA Integration
- Single Sign-On (IdP & SP Initiated)
- Authentication Standards (SAML, OAuth, OpenID Connect)
- Role-Based Access Control (RBAC)
- Directory Services Integration (AD, LDAP, Azure AD)
- Detailed Logging & SIEM Integration



Privileged Access Management (PAM)

Mirket PAM brings privileged access under central control, prevents users from accessing target-system credentials and makes every session traceable end to end. The solution consolidates access, authentication, authorization and session auditing on a single platform, delivering full control over critical systems.

How Does PAM Work?

1. User Access

The user initiates access centrally through the PAM platform.

2. Authentication

The authentication process is secured with MFA.

3. Authorization Control

Access requests are evaluated through defined policies and role-based authorization (RBAC).

4. Secure Access

The user connects to the target system through a controlled session, without ever seeing the credentials.

5. Session Security

All session activity is monitored in real time, recorded and intervened in when necessary.

Ayrıcalıklı Erişim Yönetimi

- Password / Secret Vault
- Policy-Based Password Rotation
- Asset & Local User Discovery
- Asset/Scope Structure
- Policy-Based Access Control
- Role-Based Access Control (RBAC)
- Identity Source Integration
- Agentless Proxy Architecture
- Native RDP & SSH
- Isolated & Secure Browser
- Asset Groups
- Glass Break Access
- High Availability
- Privilege Escalation MFA Enforcement
- Lateral Movement Prevention (Whitelist/Blacklist • Kill Session)

Oturum Güvenliği ve Denetim

- Video Session Recording
- Real-Time Session Monitoring
- Session Join (Read-Only / Read-Write)
- Session Termination & Intervention
- Session Transcript & Command Search
- Bidirectional Clipboard Control
- File Transfer Control
- SIEM / Syslog
- Audit & Compliance Reporting
- Scheduled Reports
- Smart Playback
- Session History
- Password Policies
- Deduplication



AI-Powered Threat Detection and Response (ITDR)

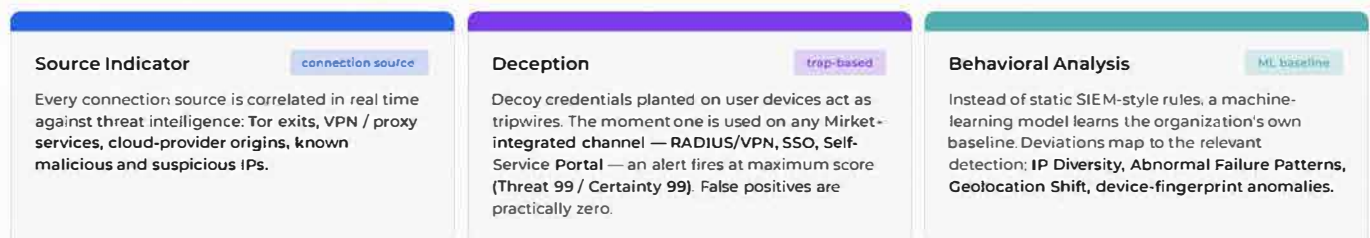
A significant share of modern attacks no longer starts with an exploit — it starts with a valid credential. An attacker signing in with a correct username and password is indistinguishable from a legitimate user to classic security layers. Mirket ITDR identifies the attacker not at the moment of access, but through the behavior they exhibit — and responds automatically.

Identity-based attacks unfold in three phases — every detection is tagged to the phase it belongs to

Provides full 24/7 protection



Three distinct detection methodologies



Detection coverage the full identity attack chain

Mirket ITDR ships with a continuously expanding catalog of detections covering every phase of the identity attack chain — from the first appearance of harvested credentials, through automated credential-stuffing traffic, to post-compromise account-takeover behavior.

Detections are organized into families according to how they identify the threat:



As attack techniques evolve, new detections are delivered automatically with the platform — no rule-writing, tuning or maintenance is required on the customer side.

Dual-axis risk scoring & automated response

Every detection produces two independent scores (0-99): Threat — potential impact — and Certainty — confidence. High-threat / low-certainty events surface for analyst review; events high on both axes flow into automated response.

Notify the security team

When a detection exceeds the notification thresholds — e.g. Certainty ≥ 50 and Threat ≥ 60 — the security team is automatically alerted by e-mail with full event context: the affected user, the channel the attempt came through, the source, both scores and the matching detection type.

Block automatically

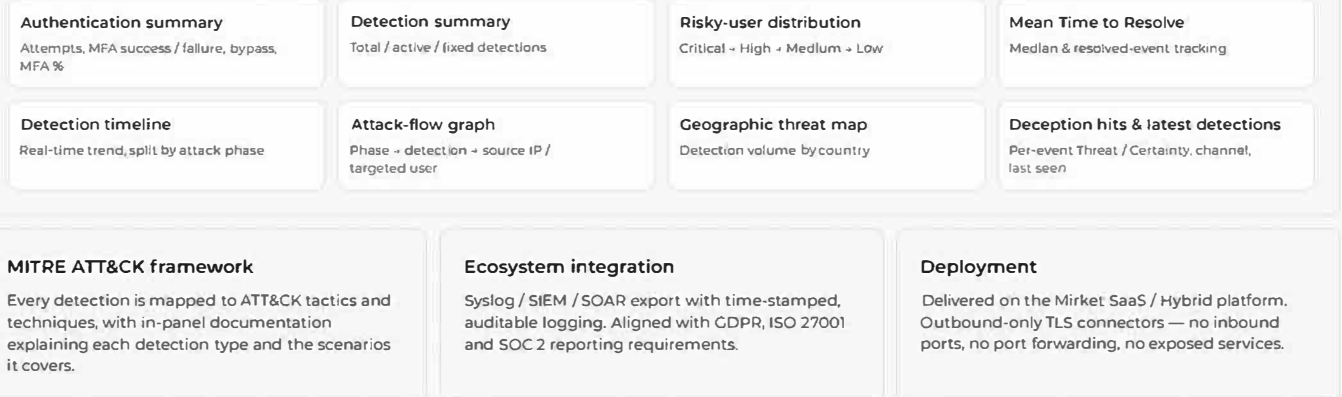
When both scores cross the critical band — e.g. Certainty ≥ 75 and Threat ≥ 87 — the response is enforced without waiting for human intervention: the account is locked and the active session is terminated before the attacker can act on the compromised identity.

Thresholds are defined per action and per axis — they never need to match — and can be differentiated by group or role from the admin panel.

Sightline

Identity security posture - one screen

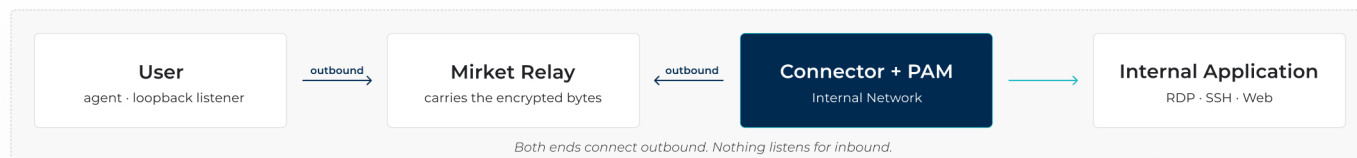
Sightline combines authentication activity with threat-detection insight in a single, continuously visible view of the organization's identity security posture.



Zero Trust Network Access (ZTNA)

Connects the user to the application,
never to your network.

- 0 inbound ports opened on the customer side
- 0 route entries added to the client
- L7 authorization at the application layer



Classic VPN

- × Operates at L3 — the network layer
- × Creates a virtual interface (utun / tun / tap)
- × Adds entries to the client's routing table
- × Once connected, the entire internal network becomes reachable
- × "Connect once, go anywhere"
- × The IPsec / WireGuard tunnel terminates at the gateway
- × The gateway must listen exposed to the internet
- × Logs only that a connection was established

Mirket ZTNA

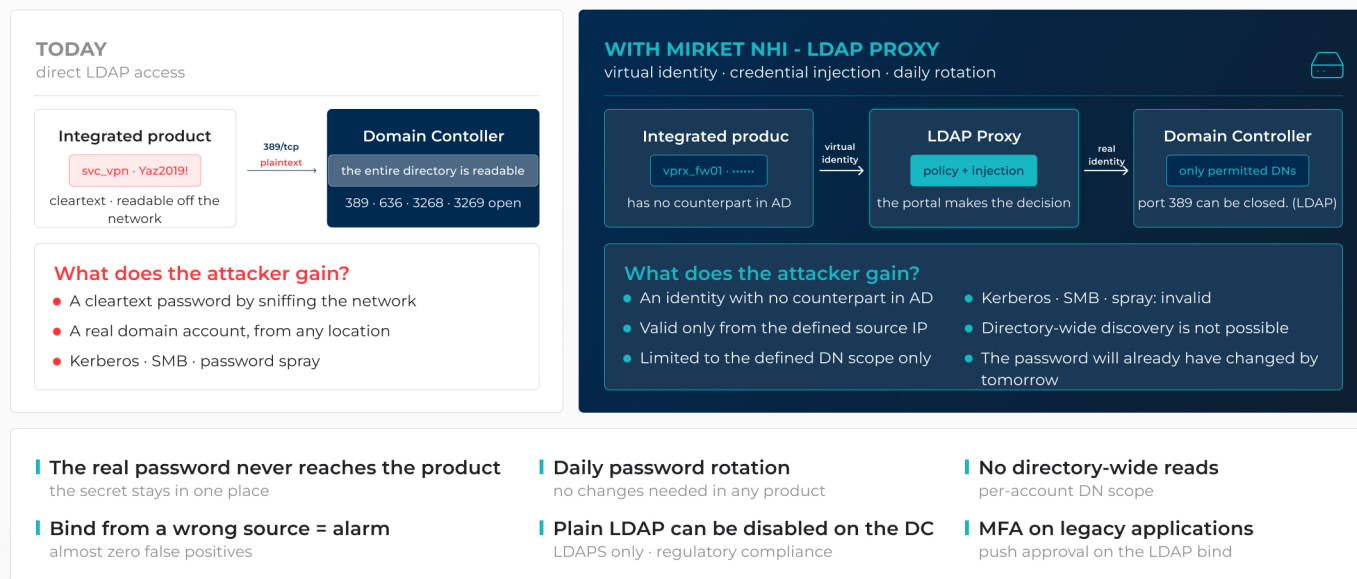
- ✓ Operates at L7 — the application byte-stream layer
- ✓ No virtual interface — only a loopback listener
- ✓ Leaves no trace in the routing table
- ✓ Only individually permitted targets
- ✓ PAM authorization on every session
- ✓ Noise_IK end-to-end — the relay cannot decrypt the content
- ✓ The connector connects outbound — zero inbound ports
- ✓ Video recording + full command transcript

On-premise platform · Session data never leaves your environment

LDAP Proxy for Active Directory (NHI)

The password crossing the network is no longer even a domain account.

Products connect using virtual identities defined in Mirket; the real Active Directory password is never handed to any product.



On-Premise Platform Licences

Mirket licenses provide integrated identity and access security components.

Feature	On-Premise Platform
Mirket Advanced Multi-Factor Authentication (MFA)	User
API Integration for Custom Applications	✓
LDAP Proxy for Legacy Systems	✓
Exchange (OWA, ECP, ActiveSync)	✓
VPN and Network Infrastructure (RADIUS)	✓
Windows/Linux Logon, RDP & SSH	✓
SaaS Applications (SAML, OAuth, OpenID Connect)	✓
MFA for Privilege Escalation	✓
ADFS MFA Adapter	✓
Detailed Logging & SIEM Integration	✓
Unlimited Resource Integration	✓
Mirket Secure Self-Service Portal (SSP)	User
Self-Service Password Reset & Account Unlock	✓
MFA Device Management & Provisioning	✓
Restricted Words & Password Complexity Policy	✓
Periodic Password Change Policy	✓
MFA-Protected Self-Service Operations	✓
Mirket Single Sign-on (SSO)	User
Advanced MFA Integration	✓
Single Sign-On (IdP & SP Initiated)	✓
Identity Federation Standards (SAML, OAuth, OpenID Connect)	✓
Role-Based Access Control (RBAC)	✓
Directory Service Integration (AD, LDAP, Azure AD)	✓
Detailed Logging & SIEM Integration	✓
Mirket Privileged Access Management (PAM)	User Co
Password Vault & Password Policies	✓
Policy-Based Password Rotation	✓
Policy-Based Access Control & RBAC	✓
<u>Asset/Scope Structure, Asset Groups & Asset Discovery</u>	✓
<u>Account Discovery</u>	✓
Identity Source Integration	✓
Privilege Escalation Approval (MFA / Admin Approval)	✓
Emergency Access (Glass Break)	✓
Agentless Proxy Architecture & Isolated Secure Browser	✓
Native RDP & SSH Access	✓
Video Session Recording, Smart Playback & Deduplication	✓
Real-Time Session Monitoring, Intervention & Session History	✓
<u>Bidirectional Clipboard & File Transfer Control</u>	✓
Detailed Logging, SIEM/Syslog & Compliance Reporting (incl. Scheduled Reports)	✓
Licence Types	User Concurrent User (CC)

Hybrid Platform Licences

Mirket licenses provide integrated identity and access security components.

Feature	Hybrid Platform
Mirket Advanced Multi-Factor Authentication (MFA)	User
API Integration for Custom Applications	✓
LDAP Proxy for Legacy Systems	✓
Exchange (OWA, ECP, ActiveSync)	✓
VPN and Network Infrastructure (RADIUS)	✓
Windows/Linux Logon, RDP & SSH	✓
SaaS Applications (SAML, OAuth, OpenID Connect)	✓
MFA for Privilege Escalation	✓
ADFS MFA Adapter	✓
Detailed Logging & SIEM Integration	✓
Unlimited Resource Integration	✓
Mirket Secure Self-Service Portal (SSP)	User
Self-Service Password Reset & Account Unlock	✓
MFA Device Management & Provisioning	✓
Restricted Words & Password Complexity Policy	✓
Periodic Password Change Policy	✓
MFA-Protected Self-Service Operations	✓
Mirket Single Sign-on (SSO)	User
Advanced MFA Integration	✓
Single Sign-On (IdP & SP Initiated)	✓
Identity Federation Standards (SAML, OAuth, OpenID Connect)	✓
Role-Based Access Control (RBAC)	✓
Directory Service Integration (AD, LDAP, Azure AD)	✓
Detailed Logging & SIEM Integration	✓
Mirket Identity Threat Detection and Response (ITDR)	User
AI & Machine Learning-Based Anomaly Detection	✓
Behavioral Analytics & Dynamic Risk Scoring	✓
Deception Methodology & Real-Time Alerts	✓
Threat Intelligence (Dark Web, IoC, TOR/VPN)	✓
SIEM / SOAR Integration	✓
MITRE ATT&CK Threat Mapping	✓
Licence Types	User Concurrent Session (CC)



Mirket Server Requirements

Servers must meet at least the following specifications.

On-Premise Platform Server Requirements

- Operating System Requirements**
 - Ubuntu Server 22.04 LTS (64-bit)
 - Minimum: a clean installation
 - The system must be fully up to date
- Minimum Hardware Requirements**

Resource	Requirement
CPU	16 vCPU
RAM	16 GB
Disk (if PAM module will be used)	1 TB (SSD recommended)
Disk (if PAM module will not be used)	500 GB (SSD recommended)

Hybrid Platform Server Requirements

- Mirket Gateways Installation Requirements**
 - The server must be running one of the following Windows operating systems:
 - Runs on all systems with Windows Server 2012 R2 or later. (8 GB RAM, 4 CPU, 100 GB disk)
 - Runs on all systems with Windows 10 or later. (8 GB RAM, 4 CPU, 100 GB disk)