ASGER is a unified privileged access security platform built on a **Zero Trust** architecture, designed to centrally govern and protect access to enterprise-critical and operational infrastructure. It consolidates all privileged interaction points into a single, intelligent control plane—eliminating siloed access tools and reducing the attack surface across **IT and OT** environments.

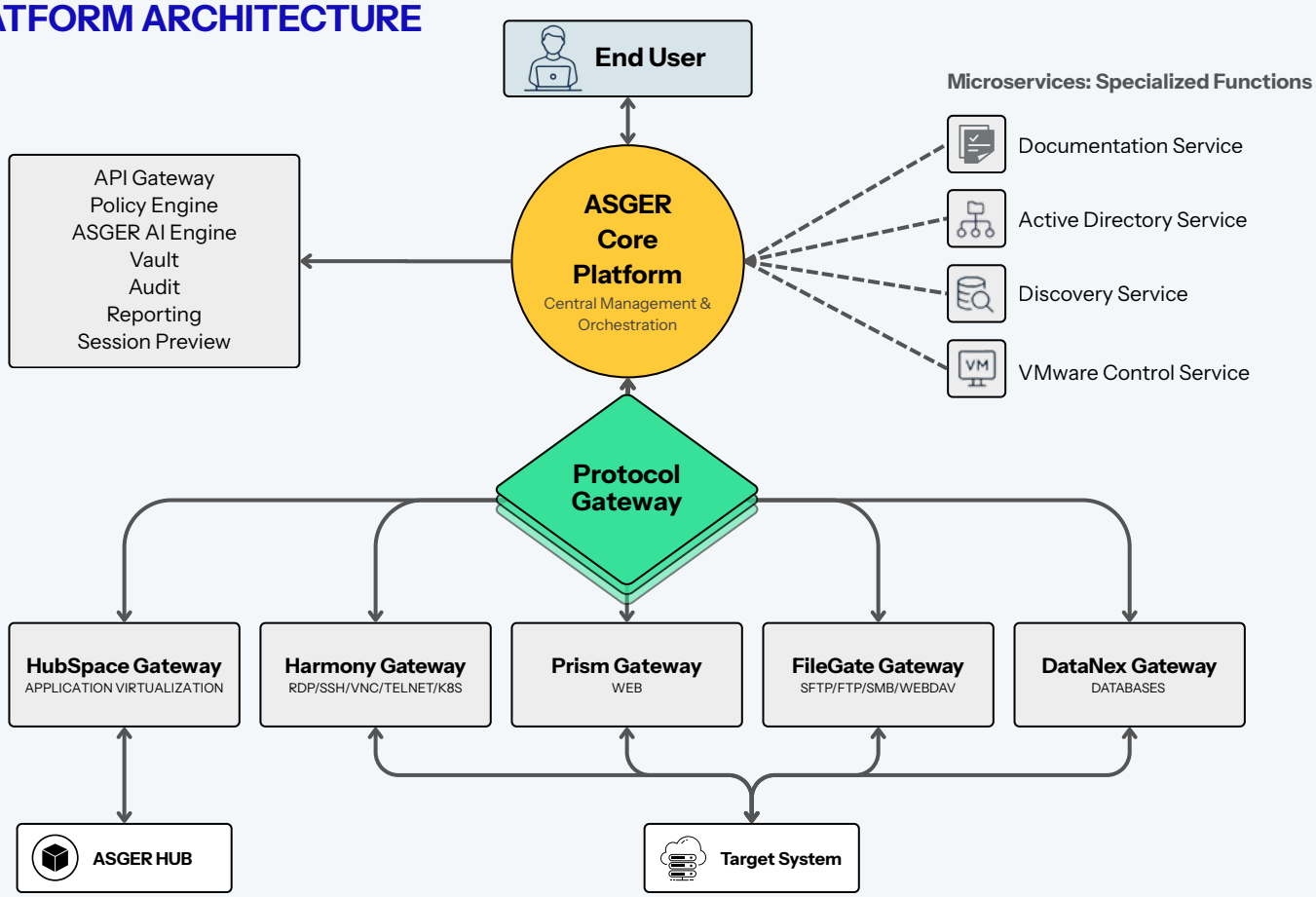
ASGER seamlessly integrates core operational capabilities such as secure remote access **(RDP, SSH, VNC, Telnet)**, database access management **(DataNex)**, secure file transfer **(FileGate)**, browser isolation **(Prism)**, and container orchestration **(HubSpace, Kubernetes)**. With multi-layer protocol awareness and policy-driven controls, ASGER ensures consistent security enforcement across diverse systems and workflows.

All privileged activities are continuously monitored and captured through Session Recording, providing full visibility and forensic-level traceability. The **ASGER AI Engine** applies machine-learning-based behavioral analytics to detect anomalies in real time, enabling proactive threat detection and actionable intelligence before risks escalate.

Integrated **Vault** services eliminate static credentials through **automated rotation** and **Just-In-Time (JIT)** access, significantly reducing credential exposure. Fine-grained policy orchestration enforces the principle of least privilege, ensuring users and systems receive only the access they need—only when they need it.

With built-in audit trails, compliance-ready reporting, and alignment with industry standards such as **SOC 2, ISO 27001, and PCI-DSS,** ASGER empowers organizations to meet regulatory requirements while strengthening their overall security posture—without sacrificing operational efficiency.

PLATFORM ARCHITECTURE



HubSpace Gateway

HubSpace runs browsers and developer tools in isolated containers, enables secure web automation, and blocks malicious access with container-level firewall and DNS filtering.

Harmony Gateway

Protocol-level proxy for RDP, SSH, VNC, Telnet and Kubernetes. Isolates users from target systems, provides TLS 1.3 encryption, and enables session recording and broadcasting.

Prism Gateway

Browser isolation proxy for securing access to web applications and sensitive internal sites. Features remote browser execution, URL filtering, and session recording.

FileGate Gateway

Secure file transfer gateway (SFTP/FTP/SMB/WEBDAV) with real-time malware scanning, path-based access control, and upload/download restrictions.

DataNex Gateway

DataNex enables secure database access with native terminal support, blocks dangerous SQL commands in real time, masks sensitive data automatically, and prevents unauthorized database switching.

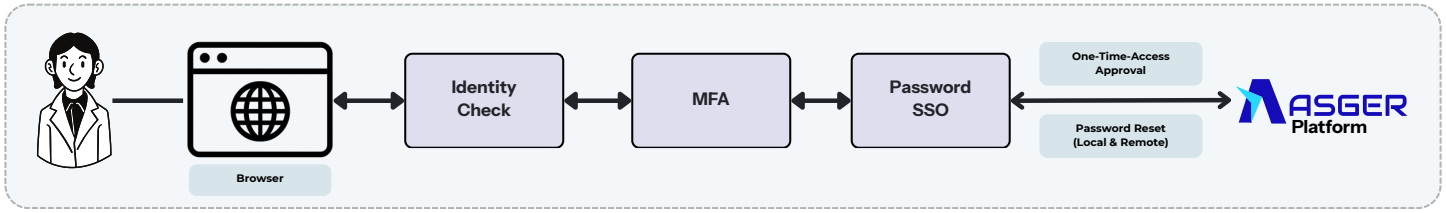
IDENTITY-DRIVEN ACCESS SECURITY & ADAPTIVE AUTHENTICATION

Multi-Factor Authentication (MFA):
Supports a broad range of authentication mechanisms, including TOTP-based authenticator applications, SMS, email verification, and security questions, enabling layered identity assurance and flexible enforcement across different access scenarios.

Adaptive & Context-Aware Authentication:
Dynamically applies authentication policies based on real-time contextual signals such as time of access, geographic location, device posture, IP address and network segment, and calculated risk level, ensuring risk-adaptive access decisions.

One-Time Access (OTA):
Enables approval-driven, time-bound privileged access for high-risk, emergency, or exceptional operations, eliminating standing privileges and significantly reducing exposure windows.

Enterprise-Grade Identity Integration:
Provides seamless integration with Active Directory and OpenLDAP, with native support for SAML, RADIUS, and LDAP, ensuring full interoperability with existing enterprise identity and access management ecosystems.



EMPOWERING TEAMS WITH SECURE VAULT COLLABORATION

Personal Vaults

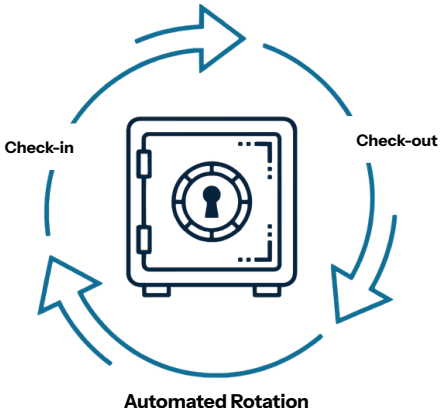
Enable users to securely manage their own credentials, API keys, and sensitive personal data, reducing credential sprawl and eliminating reliance on insecure password management tools.

One-Time Share

Create time-bound, encrypted, and passcode-protected links to share credentials with internal teams or external vendors—without granting direct access to the vault.

Record Collaboration

Teams can securely share credentials and secrets within structured shared folders, using role-based access controls (View, Edit, Share, Manage) and maintaining a complete audit trail of all actions.



Automated Password Rotation

Out-of-the-box support for scheduled and policy-driven credential rotation across a wide range of platforms, including:

- Operating Systems: Windows, Linux, macOS
- Directory Services: Active Directory, Azure AD
- Cloud Platforms: AWS IAM and more
- Network & Security Appliances: Cisco, Fortinet, Palo Alto and more
- Databases: PostgreSQL, MySQL, and more

Business Value: Removes reliance on manual password handling, standardizes credential security across the organization, and proactively mitigates risks caused by outdated or compromised credentials.

COMPLETE SESSION VISIBILITY, RECORDING & REAL-TIME CONTROL

Immutable Session Recording

Tamper-proof, high-quality video recordings combined with detailed text-based logs capture every session activity, including keystrokes, command execution, command history, and terminal output.

Live Session Monitoring & Instant Termination

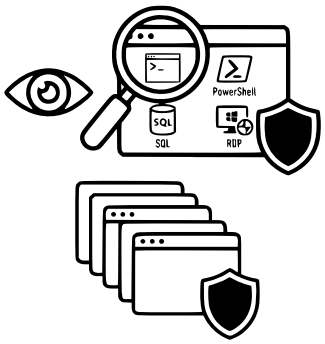
Administrators can monitor active sessions in real time, collaborate with users when needed, and immediately terminate suspicious or unauthorized activity.

Real-Time Command & Action Enforcement

Policy controls are enforced directly within live sessions. Administrators can define rules to block high-risk commands or actions (such as rm -rf or DROP TABLE) in real time—preventing damage before it occurs.

AI-POWERED SECURITY INTELLIGENCE

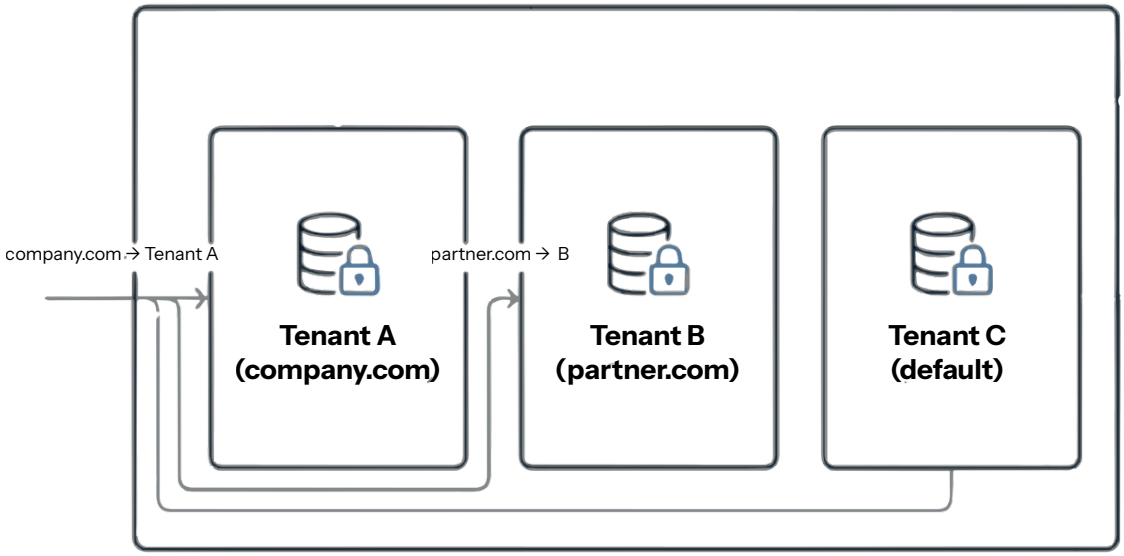
An AI engine that uses deep learning, behavioral anomaly detection, and risk scoring to automatically detect security threats in privileged sessions and enable proactive response.



Deep Learning–Based Visual Event Detection
Identifies high-risk applications such as Command Prompt, PowerShell, Active Directory tools, SQL Management Studio, and Remote Desktop through real-time visual analysis.

Layer Detection Awareness
Detects foreground and background applications, including hidden or overlapping windows, and flags risky multi-tool usage combinations.

TRUE MULTI-TENANCY FOR SCALE, SECURITY, AND ISOLATION



Complete Tenant Isolation: Each tenant operates within its own fully isolated environment, including a dedicated database schema, users, groups, roles, and resources. This ensures strict separation of data and policies while leveraging a shared, scalable underlying infrastructure.

Automatic Domain-to-Tenant Mapping: Users are automatically assigned to the correct tenant based on their email domain (e.g., users from company.com are routed to Tenant A, while users from partner.com are routed to Tenant B). A default tenant can be configured for any unmatched domains.

Delegated Administration Model: A root tenant manages global, system-level operations, while each tenant maintains its own administrators with permissions strictly scoped to their respective environments.

Per-Tenant Licensing & Consumption Control: Licenses (System Admin, Employee, Isolated) can be allocated and managed on a per-tenant basis, enabling flexible commercial models for MSSPs or internal chargeback across enterprise departments.

SOLUTION ADVANTAGES

- **Drastically Reduces the Attack Surface:** Implements Just-in-Time access and a zero-standing-privilege security model to eliminate unnecessary and persistent privileges.
- **Strengthens the Overall Security Posture:** Leverages multi-layered, adaptive authentication combined with proactive, AI-driven threat detection to continuously assess and mitigate risk.
- **Simplifies Compliance and Auditing:** Delivers comprehensive session recording, tamper-proof audit logs, and centralized reporting to meet regulatory and compliance requirements with ease.
- **Increases Operational Efficiency:** Uses a unified, agentless architecture that simplifies deployment, accelerates onboarding, and enables secure remote access for all users.
- **Lowers Total Cost of Ownership (TCO):**Built on a scalable, containerized architecture with broad integrations and true multi-tenancy, reducing infrastructure complexity and operational overhead.

info@sobeyazilim.com.tr
+(90) 312 960 00 19

Mustafa Kemal Mah. Dumlupınar Blv. **ODTÜ** Teknokent Bilişim İnovasyon Merkezi 280/G İç Kapı No: 1118 Çankaya Ankara