



CYBERARK[®]
A PALO ALTO NETWORKS COMPANY

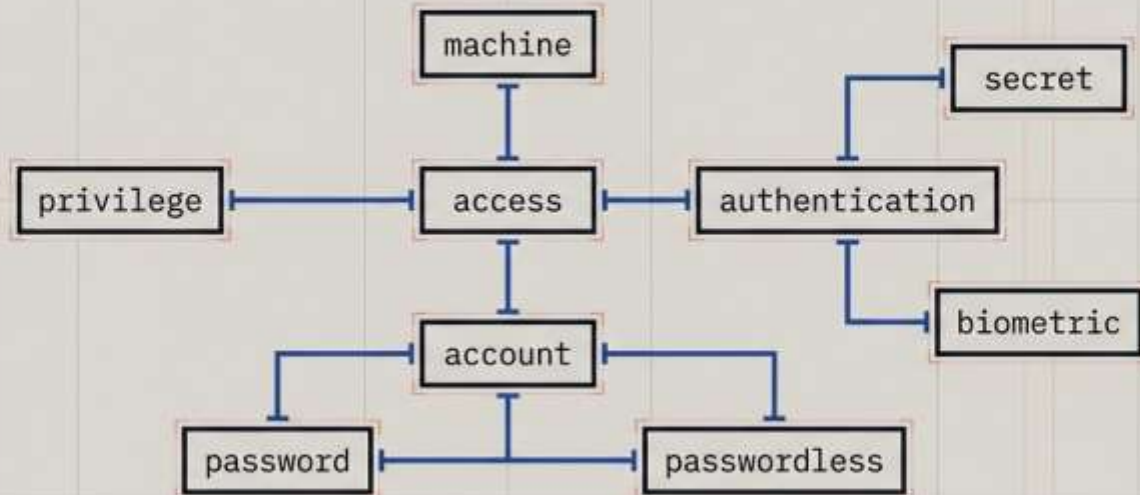
The future of privilege: Dynamic identity security in real time

April 23th 2026

Sinan Altinsoy, Solutions Engineer



The Language of Digital Access Control

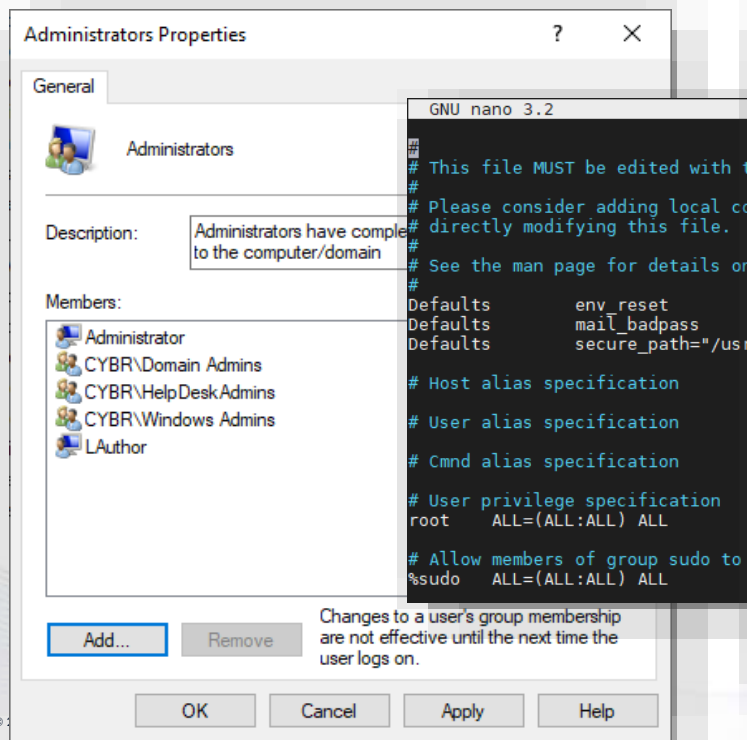


A Conceptual Primer
on Modern Identity
Architecture.

NotebookLM

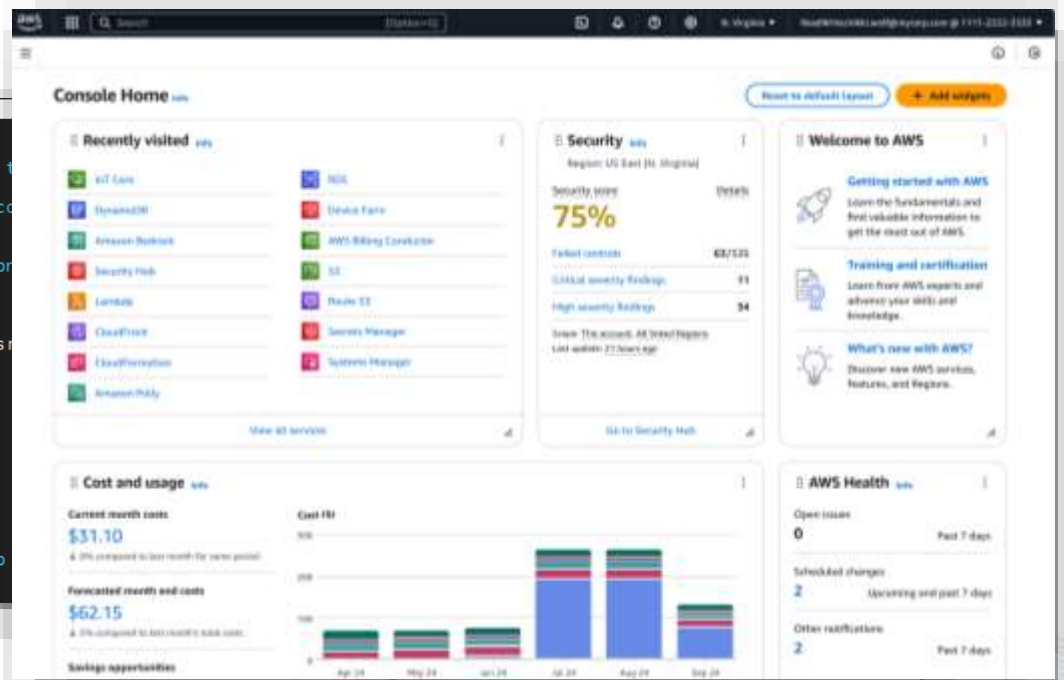
Privileged Access

In an enterprise environment, privileged access is a term used to designate special access or abilities **above and beyond that of a standard user.**



The image shows the Windows 'Administrators Properties' dialog box. The 'General' tab is active, showing the group name 'Administrators' and a description: 'Administrators have complete control of the computer/domain'. The 'Members' list includes Administrator, CYBR\Domain Admins, CYBR\HelpDeskAdmins, CYBR\Windows Admins, and LAuthor. A terminal window (GNU nano 3.2) is overlaid on the dialog, showing the contents of the group's permissions file. The file contains instructions on how to edit it and lists various permissions for different users, including 'root' and '%sudo'.

```
GNU nano 3.2
# This file MUST be edited with a
# text editor. See http://linux.die.net
# Please consider adding local control
# directly modifying this file.
# See the man page for details on
# permissions.
Defaults env_reset
Defaults mail_badpass
Defaults secure_path="/usr/local
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root ALL=(ALL:ALL) ALL
# Allow members of group sudo to
%sudo ALL=(ALL:ALL) ALL
```



The image shows the AWS Management Console Home page. The page is divided into several sections: 'Recently visited' (listing services like AWS IAM, IAM, AWS Billing Conductor, etc.), 'Security' (showing a 75% security score and various security findings), 'Welcome to AWS' (with links for getting started, training, and what's new), 'Cost and usage' (displaying current and forecasted monthly costs, and a bar chart for cost per hour), and 'AWS Health' (showing open issues, scheduled changes, and other notifications).

Privileges, Identities and Risk Are Growing Exponentially

HUMANS

75%

Companies have Over-Privileged Users

Uncontrolled Privilege

MACHINES

82:1

Machines Vastly Outnumber Humans

Hidden Access to the Highest Risk Systems & Data

AGENTS

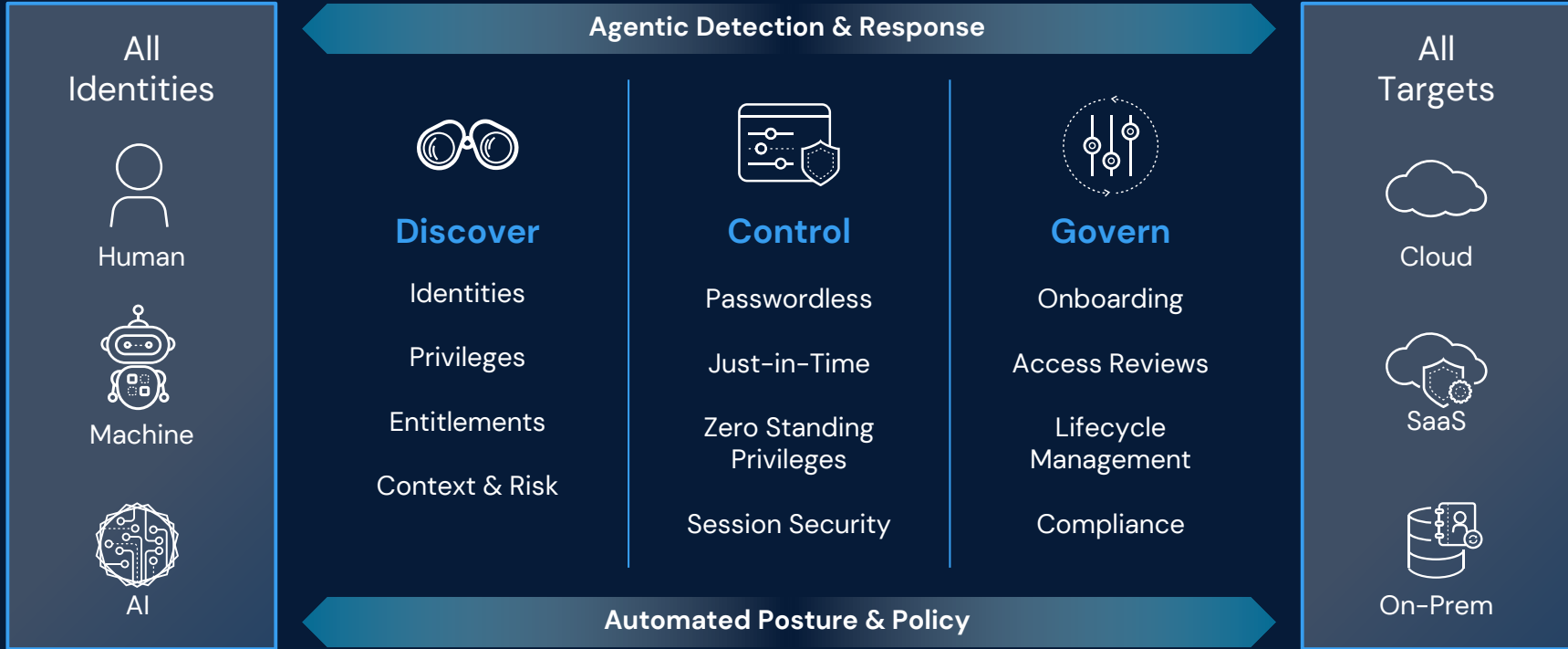
94%

Companies Lack Security Controls for AI

AI Adoption is Outpacing Controls

Identity weaknesses played a material role in almost 90% of Unit 42 investigations over past year

Identity Security Platform: Unified and Security First

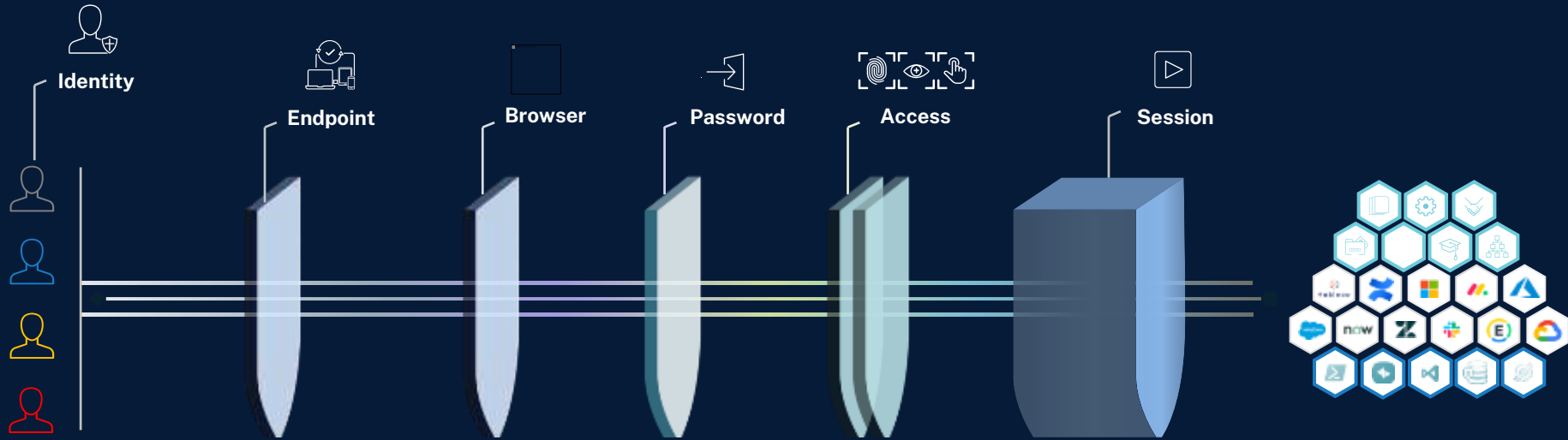




Platform Overview



Reimagine Workforce Access: How We Do it Better



• Endpoint Privilege Manager

• Prisma Browser

• Workforce Password Management

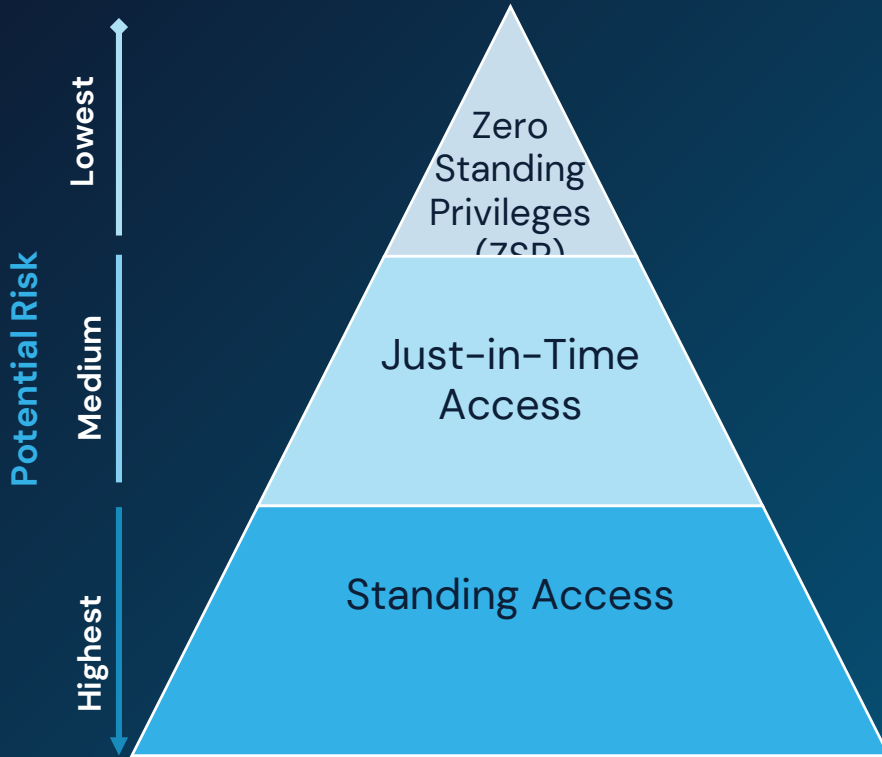
• Secure Web Sessions

- Lifecycle Management
- Directory Services
- Identity Flows
- Identity Compliance

- Single Sign-on
- Adaptive MFA
- User Behavior Analytics
- Application Gateway



Pragmatic Approach to Mitigating Risk



Zero Standing Privileges

- Access rights are no longer only granted just-in-time.
- Least privilege access rights are created and deleted on-the-fly for each session.

This greatly reduces risk of compromised access and impact of the access

Just-in-Time Access

- Access can only be elevated just-in-time, but at regular intervals
- There are no restrictions on commands and permissions

JIT Access reduces the risk of compromised access. But does not reduce the impact of the access.

Standing Access - Secured by PAM - Vaulted & Isolated

- User accounts always exist in target systems. Access is 24x7.
- There are no restrictions on commands and permissions

Even with Identity Security controls and approval workflows in place risk is mitigated but the risk is still present.

Ephemeral Domain User

Access Policy

Create an access rule

Profile

Members

Access window

Local groups:

- Administrators
- Power Users
- Remote Desktop Users
- Add custom group

Ephemeral domain user ⓘ
Access Windows-based machines via RDP as a member of one or more domain groups.

⚠ For information about security and RDS licensing considerations related to ephemeral domain users, see the [docs](#).

Note: Ensure the selected groups have permissions to access the target

test_group ⓘ

Press Enter to add another group

Reconnect with the same ephemeral user (RDP sessions only) ⓘ

Cancel Create

Users list

Active Directory Users and Computers

Name	Type	Description
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers l...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Key Admins	Security Group...	Members of this group ...
Enterprise Read-only Domain Controllers	Security Group...	Members of this group ...
eyalr	User	
Group Policy Creator Owners	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
hadass	User	
Key Admins	Security Group...	Members of this group ...
merav	User	
merav_group	Security Group...	
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...
Read-only Domain Controllers	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...
test_group	Security Group...	
tinaboTRsfKzN4dFgJ	User	Auto generated VM user

Benefits: Risk Reduction

Adopt new use cases and scale risk reduction to new environments



Prevent credential theft with Zero Standing Privileges

System access with vaulted accounts:

- Remove permissions and dynamically assign them on demand through CyberArk.
- If credentials are stolen, attackers have no permissions.

Operational access with JIT workflows:

- No standing credentials for attackers to steal.



Prevent malware spread with improved adoption

Improved UX for access to Databases and K8s and improved adoption of session isolation:

- Users connect through CLI/IDE client of choice.
- OOTB support for MySQL, MSSQL, MongoDB, PostgreSQL, Oracle, etc.

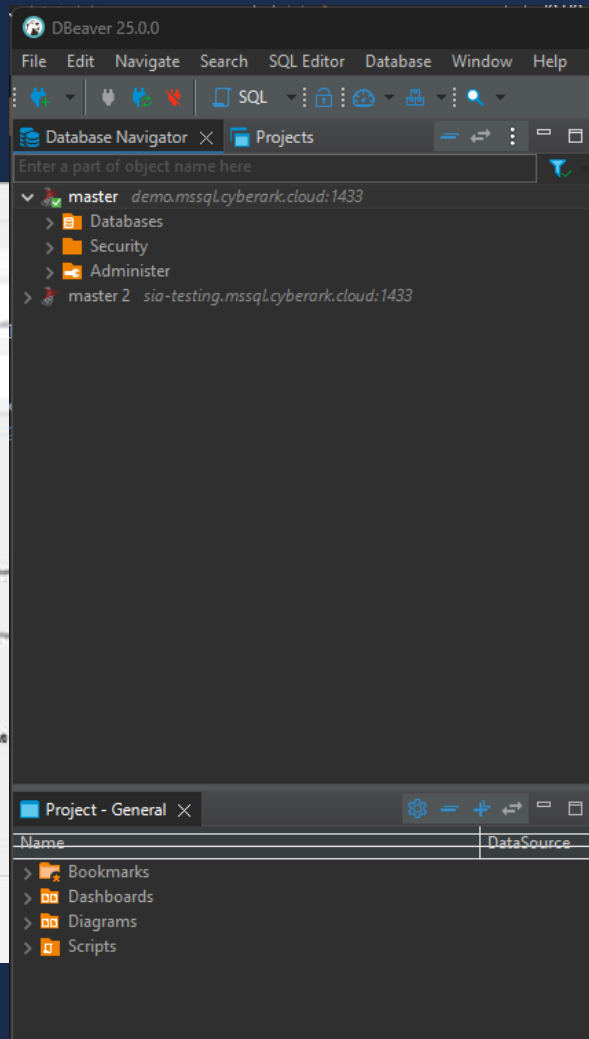
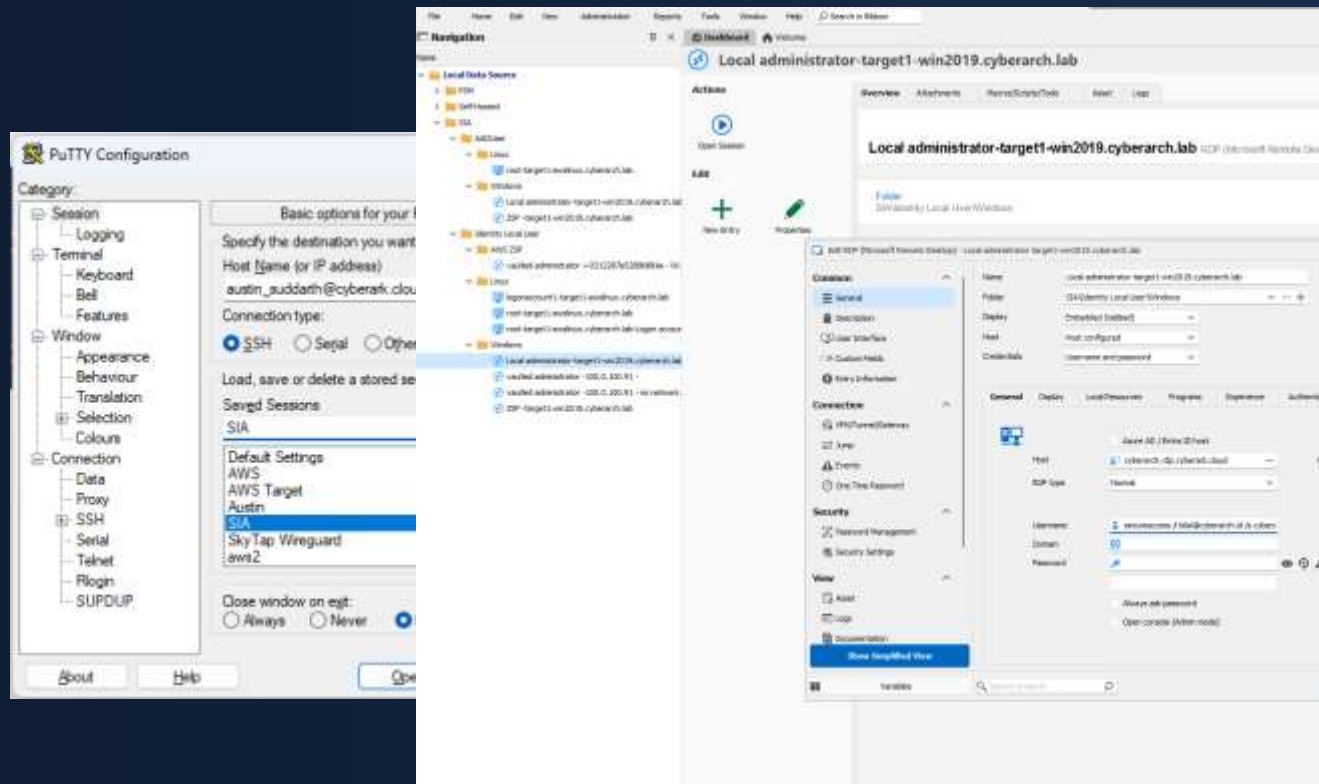


CYBERARK[®]
A PALO ALTO NETWORKS COMPANY

Secure Infrastructure Access (SIA)



Native RDP/SSH/DB Clients



ARK CLI

```
Windows PowerShell
PS C:\Dev> ark login
? Identity Security Platform Username (austin.suddarth@cyberarklab.com)
? Identity Security Platform Secret *****
? Please pick one of the following MFA methods
? Email sent to xxxx@cyberark.com. Click the link or manually enter the code to authenticate. Login tokens are hidden
Identity Security Platform Token
{
  "username": "austin.suddarth@cyberarklab.com",
  "endpoint": "https://aam4614.my.idaptive.app",
  "token_type": "JSON Web Token",
  "auth_method": "identity",
  "expires_in": "2025-04-23T23:49:22.903837",
  "metadata": {
    "env": "prod"
  },
  "origin_verify": null
}
PS C:\Dev> ark exec sia sso short-lived-password
67QL1j5M1ZB0upm7pdp/ys1UubHGcURFupOSy8eSVEu8=
PS C:\Dev> |
```

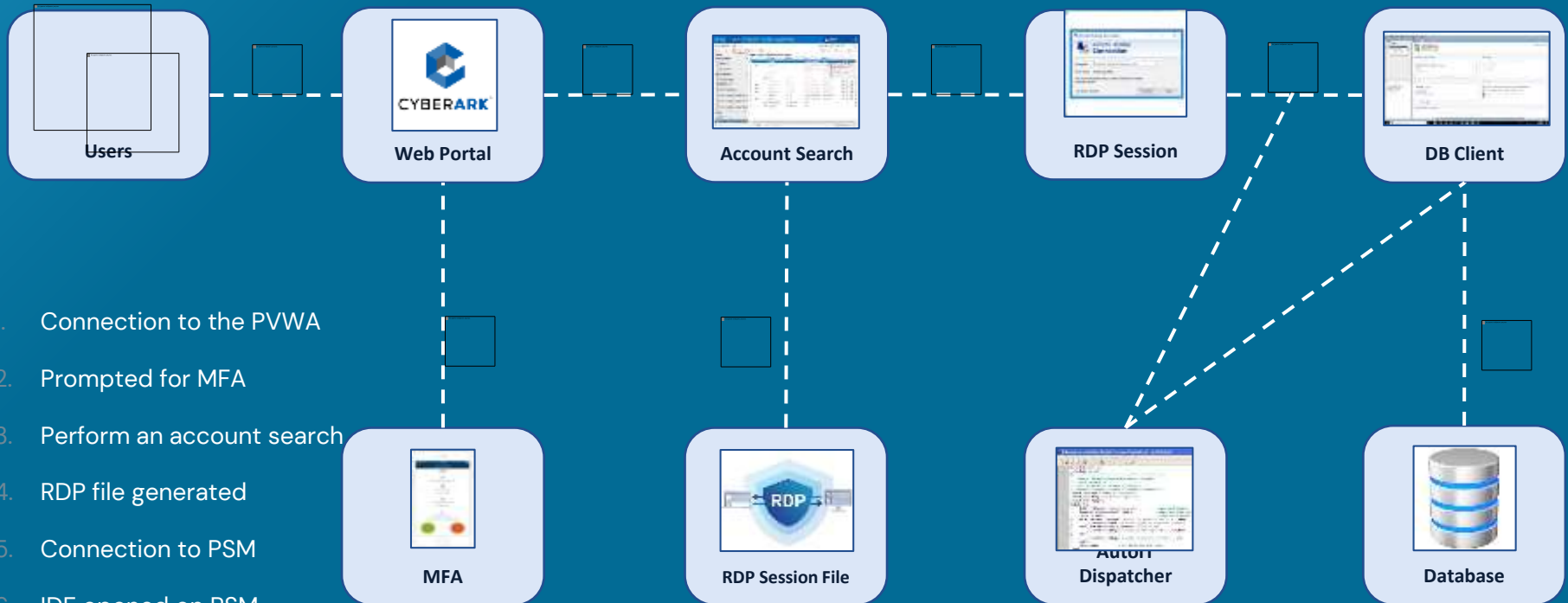
Log in directly to the database: `psql "host=mytenant.postgres.cyberark.cloud user=user@cyberark.cloud.12345@postgres@mypostgres.fqdn.com "`

Log in to the database from Ark: `ark exec sia db psql --target-username postgres --target-address mypostgres.fqdn.com`

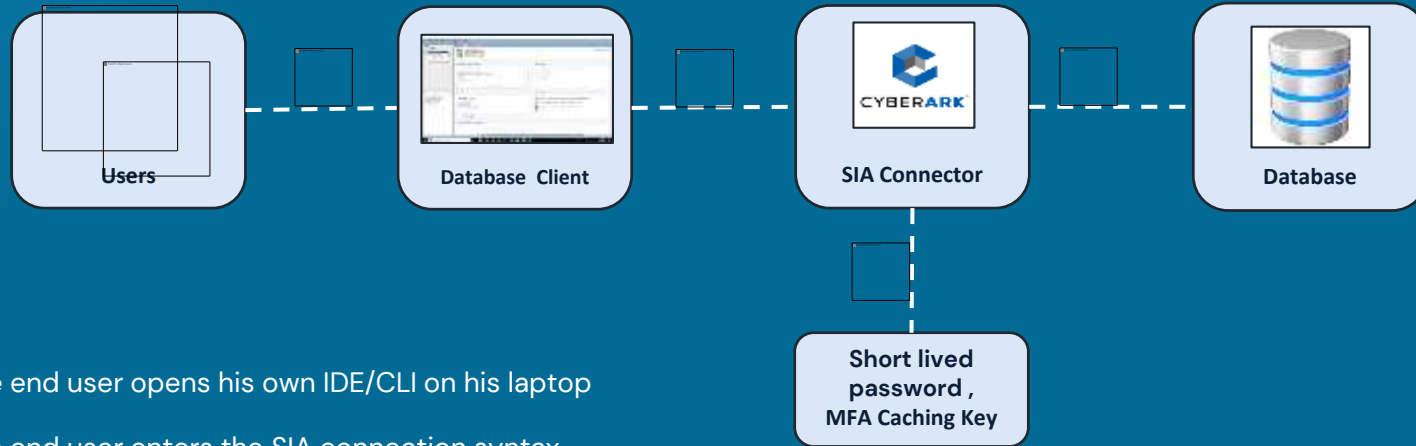
SSH: `ark exec sia sso short-lived-ssh-key`

RDP: `ark exec sia sso short-lived-rdp-file -ta targetaddress -td targetdomain -tu targetuser`

PSM Database End User Experience



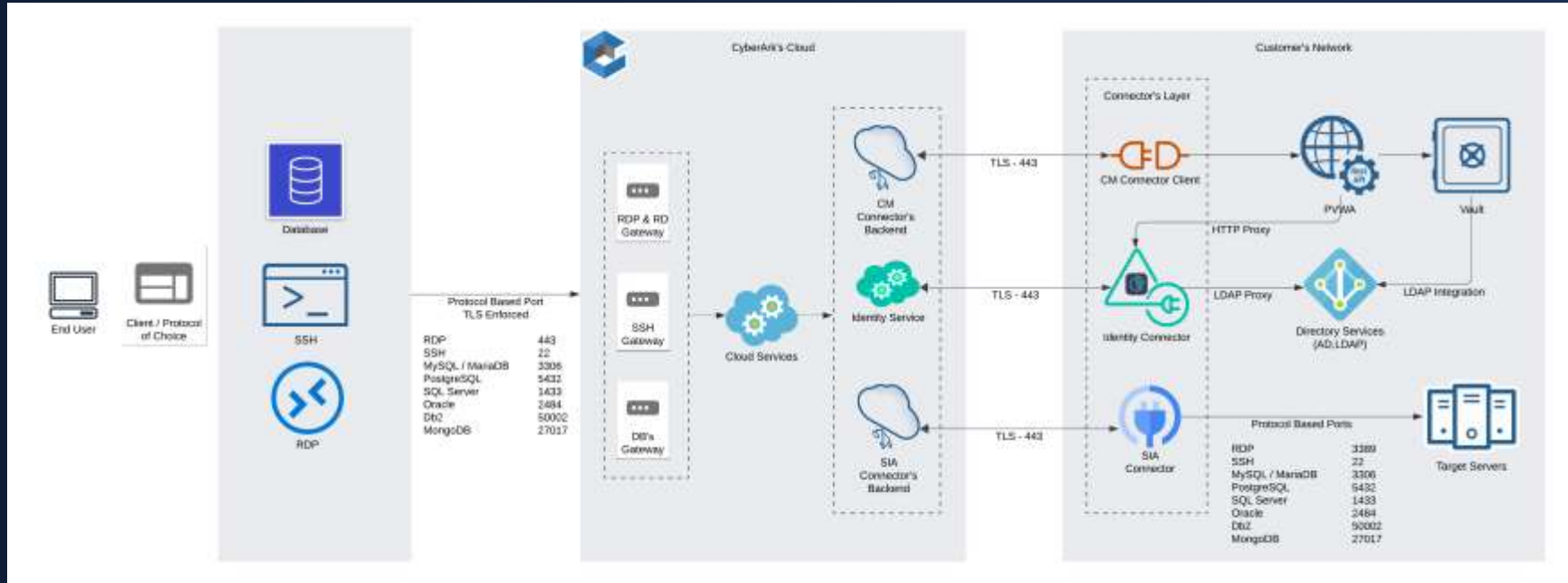
SIA Database End User Experience



1. The end user opens his own IDE/CLI on his laptop
2. The end user enters the SIA connection syntax
3. Provide DB MFA caching key/Short lived password
4. The end user is connected to the database

!ZSP is Supported

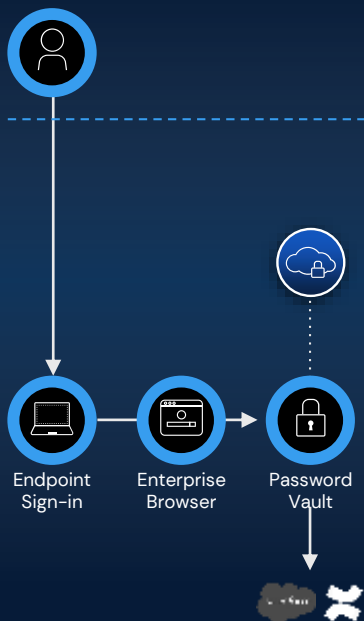
SIA Architecture



Smart Privilege Controls

Privilege Adapts to Intent, Behavior, and Risk.
Apply Privilege Controls to All, Without Slowing Work.

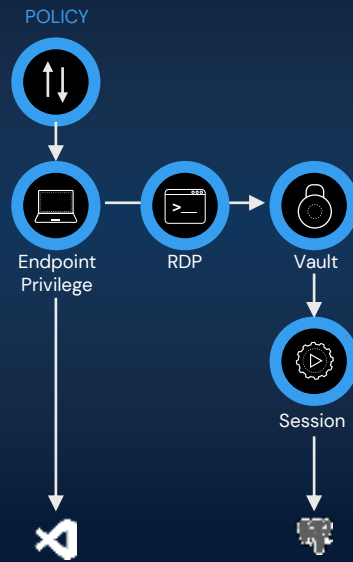
Known user.
Normal Behavior.



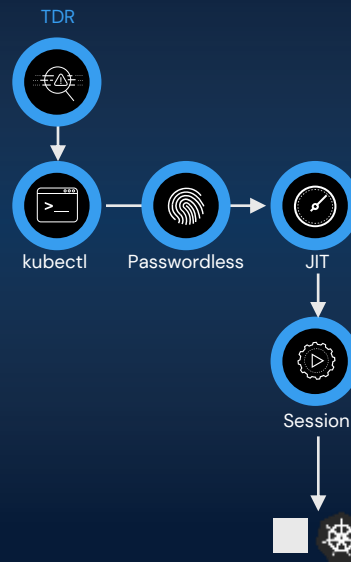
Known user.
Elevated access.



Privilege task.
Temp access.



Anomalous behavior.
Full enforcement.



Thank you