mamori.io

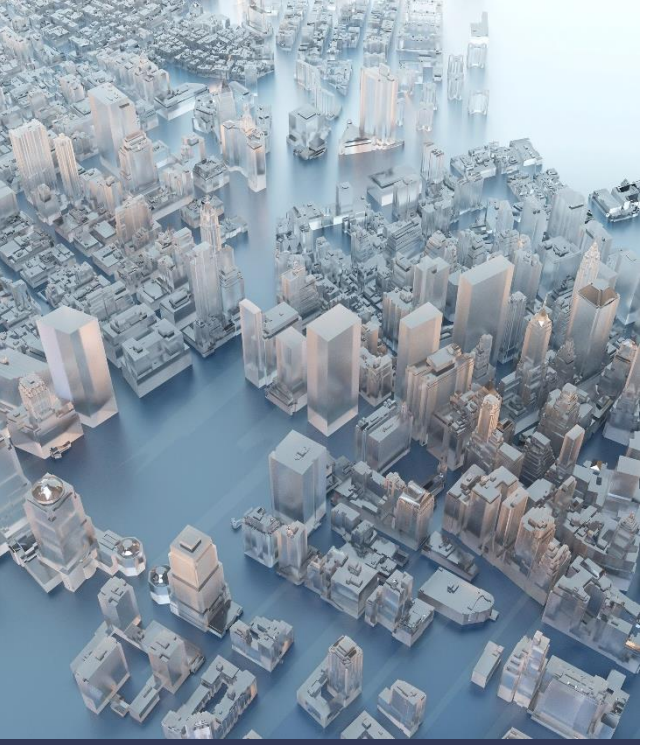
module overview

M4 PAM

mamori.io

mamori for privileged access (M4PAM)

Protects servers, databases and data from unverified access and operations.



M4PAM

solution features

technical safeguards for

- Ransomware protection
- Data privacy compliance
- Privileged access

mamori.io

mamori for privileged access management

protects

Servers, databases and data from unverified access and operations.

technical safeguards for

- security & data privacy compliance
- credential & key theft attacks
- data loss protection
- SQL injection protection
- zero trust (SSO 2FA) & least privilege security implementations

key features

- SSO & 2FA for SSH & databases
- key based SSH access
- record and playback sessions
- data privacy policies
- session & SQL firewall
- access on-demand workflow
- integrate with devops automation
- interactive access dashboards

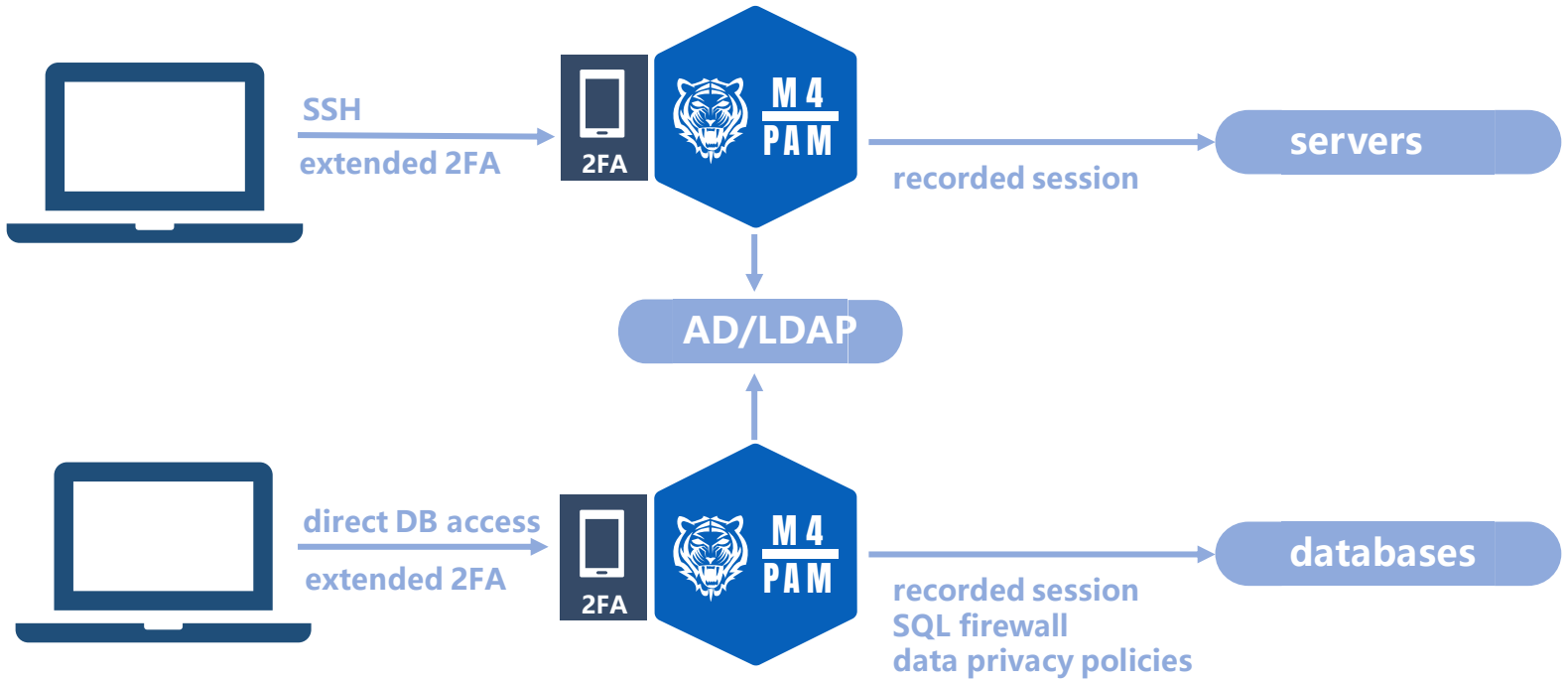
key benefits

- Difficult to impersonate an account because of 2FA, SSO and key based SSH.
- Simplifies administration. Each server has a few service accounts, and mamori manages user access to those accounts.
- Users can visualize their own permissions and request if needed.

Secure Privileged Credentials & Data

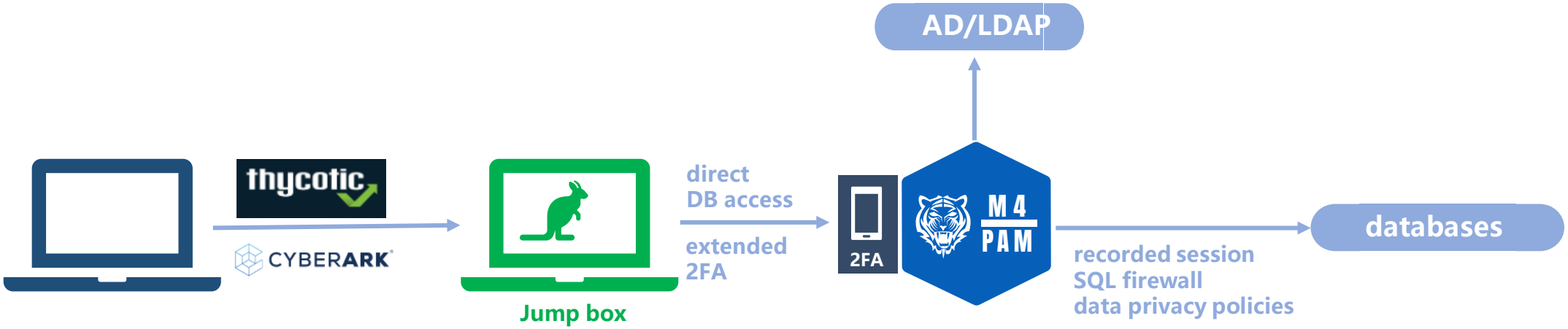
mamori.io

2FA/AD logins, sessions recorded & data privacy policies applied transparently



Compliment existing PAM

Existing PAMs protect passwords and servers. Mamori protects data



mamori.io

comparison with traditional PAM solutions

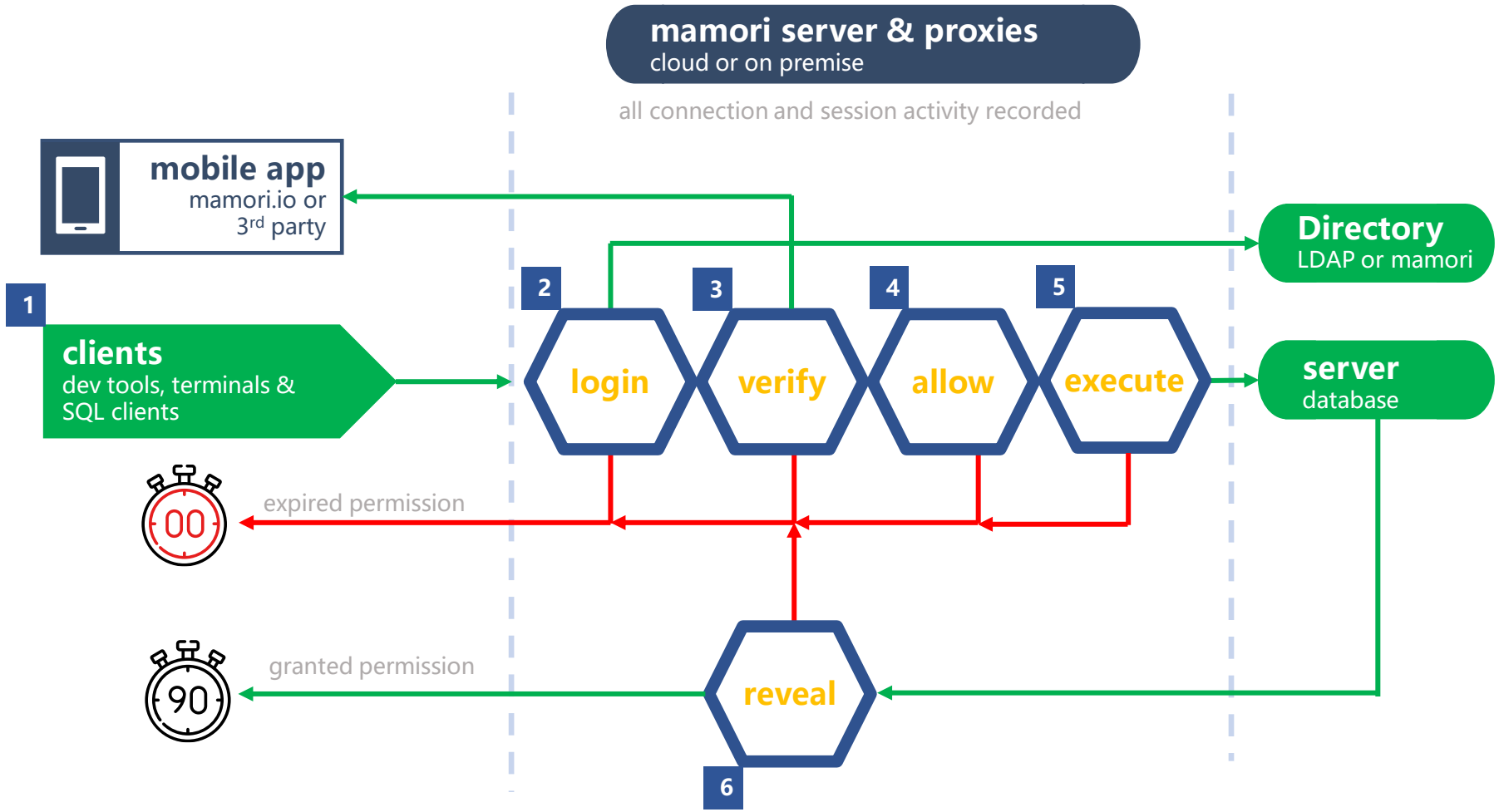
complement or replace

	M4 PAM	PAM solutions (thycotic / CYBERARK)
Access request – systems	✓	✓
data	✓	
Credential Management	DB only	✓
SSO & 2FA on resource access	✓	
RDP - access	✓	✓
session recording	✓	✓
SSH - access	✓	✓
recording	✓	✓
Database & Data - access	✓	
SQL Activity recording	✓	
DB Data masking & reveal	✓	
Application Data masking	✓	

database proxy

direct database

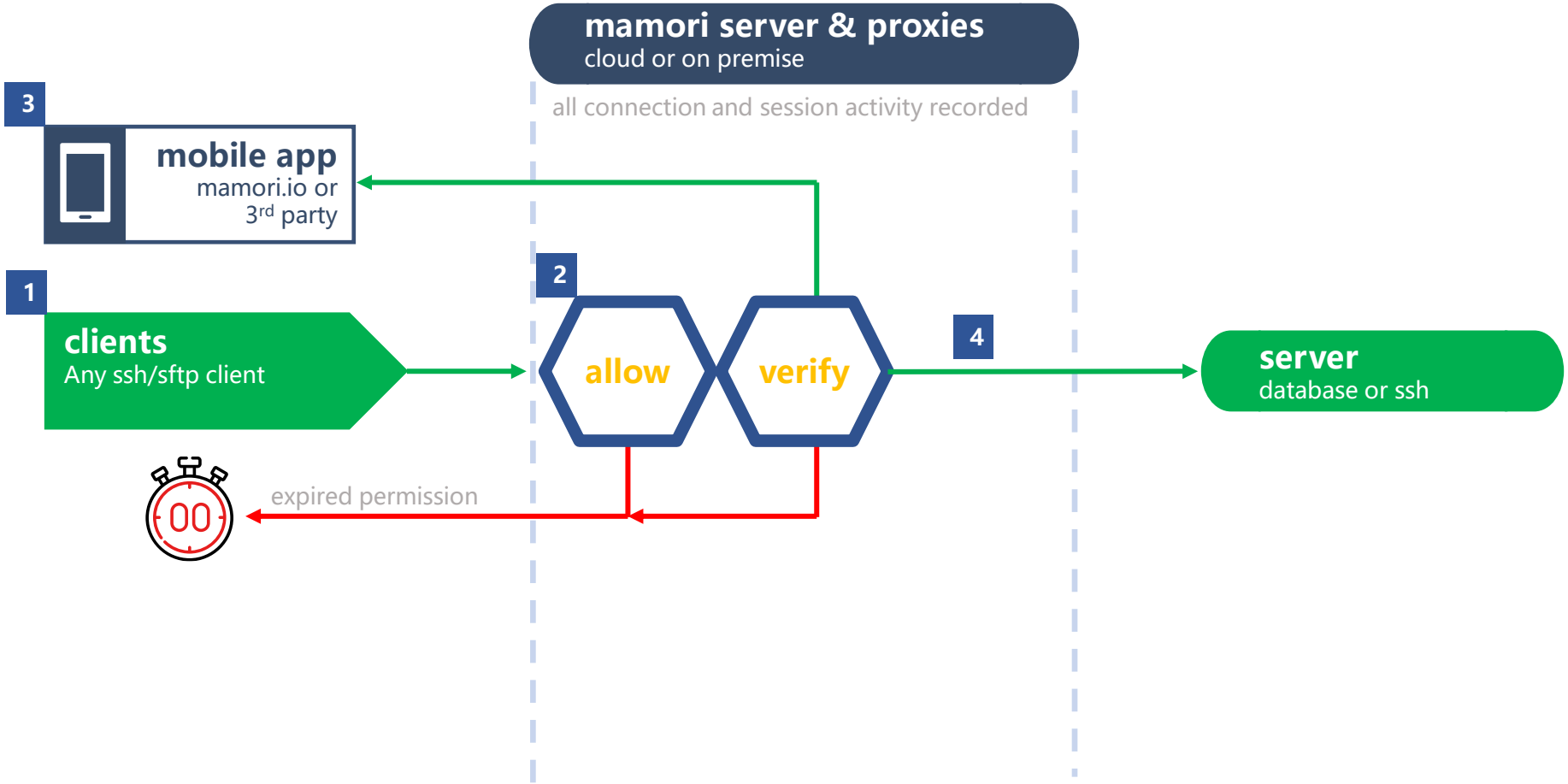
1. Connect to DB with an identity not a database credential
2. Directory Login
3. Multi-factor verification
4. Resource access check
5. Statement & object access permission check
6. Data and Row permission check



ssh proxy

ssh/sftp

1. **SSH to target**
2. **Public key check**
   client public key verified with user's public key on mamori server
3. **Multi-factor verification**
4. **Session to granted service account on target server is created**



Configuration

Server Configuration

1. Integrate directories & extend with 2FA
2. Add resources (databases, SSH and RDP logins)
3. Setup roles and access on-demand policies
4. Setup security policies
5. Setup data privacy policies

No agents
No changes databases or server
Nothing deployed on user machines

End-user Configuration

1. User configures 2FA via mamori web portal
2. User connects to resources via M4PAM server