ACCESS CONTROLLER OVERVIEW

Granular Control Over Privileged Access

Provide authentication, authorization, auditing for access across the perimeter-less network

IT and Security teams struggle to secure their networks as traditional Privileged Access Management (PAM) evolves to cover both standard and privileged users who now require access controls for potentially sensitive applications and systems. It is no longer enough to control only privileged access, all access must be controlled and managed in a zero-trust world. **Thycotic Cloud Access Controller, Thycotic Remote Access Controller, and Thycotic Database Access Controller** allow organizations to expand their control to a more granular level. These solutions extend IT teams' abilities to address emerging PAM challenges by protecting access to SaaS applications, cloud infrastructure, and ensuring remote workers stay productive and secure.

Gain Complete Visibility

See which servers, applications and websites are being used.

Detect Risky Behaviors.

Ensure only employees and trusted 3rd parties gain necessary access.

Secure Infrastructure and Applications

Grant and revoke access easily, and control fine grained actions.

Reduce risk of insider threats, misuse of rights and data exfiltration due to breaches.

Never worry about managing SSH keys on your servers.

Manage Least Privilege

Manage identities and access for employees and third parties.

Enforce company policy across all users.

Implement separation of duties.

Simplify Authentication

Centralize multi-factor authentication.

Use geofencing, geoproximity, biometrics to make the login experience smooth.

Balance security and ease-of-use and reduce user friction.

Automate Auditing

Reduce time and effort spent on compliance initiatives.

Generate necessary reports in one step.

Get Started Rapidly

Deploy quickly without the need for agents.

Eliminate the need to modify servers.

Easy onboarding through a streamlined dashboard.

Access Controllers Benefits

Consolidate Security Technology

Implement effective security controls with fewer vendors

Unburden IT Teams

Control access for all users easily with a simplified interface and streamlined design

Meet Compliance Mandates

Avoid significant financial penalties

Become a Self-Sufficient Security Champion

CLOUD ACCESS CONTROLLER

Protection for Your Cloud Assets.

Secure Cloud Access –Ensure every IaaS and SaaS user has the necessary privileges required for their role.

Granular Role Based Access Control – Precisely define what each user can click, read, or modify within any web application.

Manage Shared Accounts – Easily enforce separation of roles and duties on standard and shared accounts.

Record Web Sessions – View video session recording of the employee performing sensitive actions.

Intelligent Blocking – Detect unusual behavior and block any unauthorized access.

REMOTE ACCESS CONTROLLER

Enforce Zero Trust for Remote Workers and Third Parties.

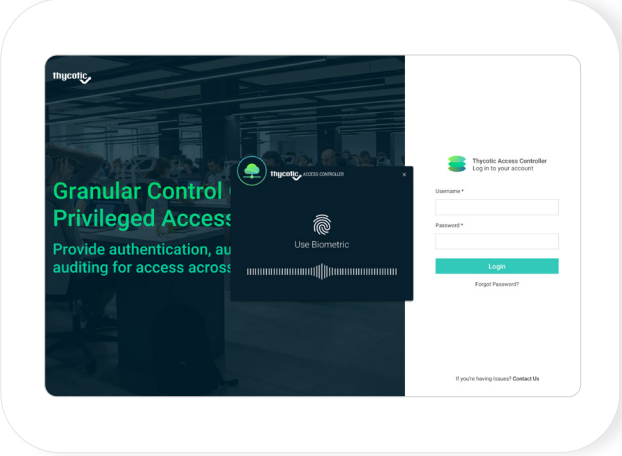
Secure Remote Access– Set granular permissions, users, and structure to map to your organization.

Grant 3rd Party Permissions – Allow vendors and contractors to access the IT resources they need.

Connect Through Browser – Deploy without opening RDP, SSH ports to the public Internet

Authenticate (MFA) – Admins can grant remote workers secure, multi-factor enabled access.

Audit – Report on activity in a central portal to ensure workers comply with company policies.



DATABASE ACCESS CONTROLLER

Granular Control and MFA for Databases.

Secure Databases–Protect your most sensitive information by controlling web access to databases.

Manage Privileged Users –Enforce appropriate access levels and provide time-based access.

Verify Identity – See who is accessing databases and govern their access.

Authenticate (MFA) –Manage authorization and auditing for the entire session and layer on MFA.

Audit – Record database access sessions, report and log actions, generate alerts.

Thycotic is focused on the most vulnerable attack vector – privilege. With Thycotic you can adopt a multi-layered approach that covers your privilege security needs from endpoints to credentials, ensuring protection at every step of an attacker's chain.