DISPEL

Third Party Access

Granting need-based access for a finite period of time.

Your third party partner needs to update equipment, and requests access to your OT network. There's no way around it—to avoid shadow IT, you give her access to your corporate VPN and jumphosts, and hope she doesn't poke around.

To mitigate risk, you've given her questionnaires about herself and devices. But the problem is still there: she is using the same path as your operators, and when she's done, it's up to you to revoke her access. Rinse and repeat every time, for every third party.

What you want: A secure remote access tool for third parties that does not touch your corporate network, and safely removes them after.

How We Do It

Our automatic deployment of virtual infrastructure lets administrators build and destroy third-party access pathways on demand. For those who don't trust the third party's devices, we also deploy virtual desktops.

Virtual Desktops

On-demand Windows or Linux virtual desktops, customizable with your applications and restrictions.

Logging and Monitoring

All our machines speak syslog, so you can see all activity and connection traffic. Optionally, record virtual desktop sessions.
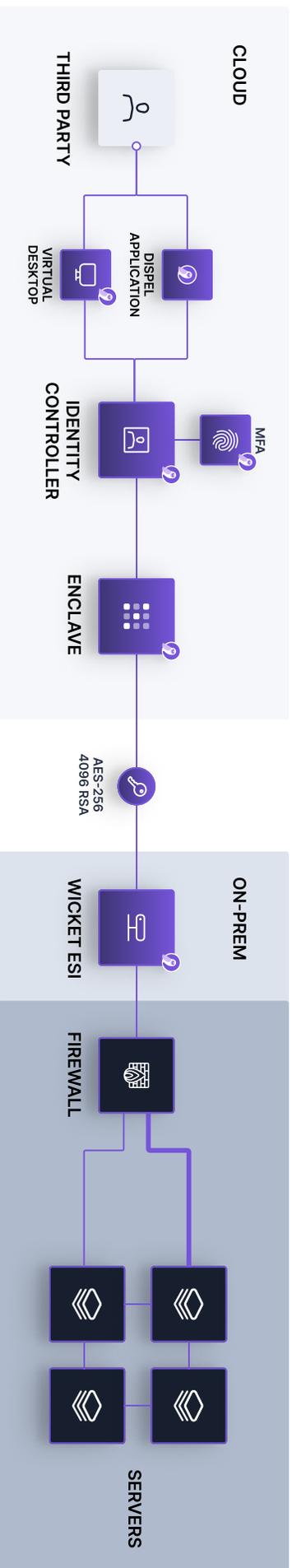
Time-Based Access

Schedule Enclaves to automatically terminate, ensuring control over access not only where, but when.
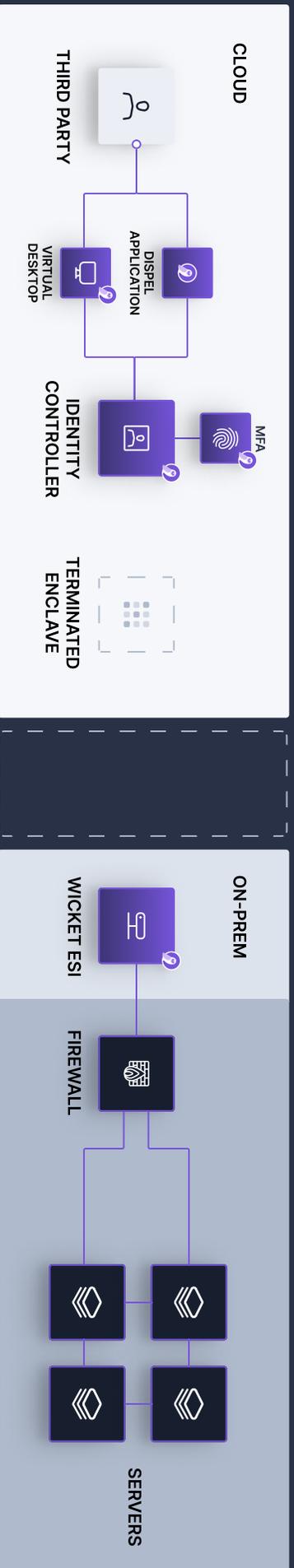
Standardized System

Deployment is fast, and access is painless. No more worries about shadow IT.

Easily Build A Secure System to Work with Third Parties

CLOUD

THIRD PARTY

DISPEL APPLICATION

VIRTUAL DESKTOP

IDENTITY CONTROLLER

MFA

ENCLAVE

AES-256 4096 RSA

ON-PREM

WICKET ESI

FIREWALL

SERVERS

Automatically Terminate the Enclave and Connections to Your Critical Systems

CLOUD

THIRD PARTY

DISPEL APPLICATION

VIRTUAL DESKTOP

IDENTITY CONTROLLER

MFA

TERMINATED ENCLAVE

ON-PREM

WICKET ESI

FIREWALL

SERVERS