

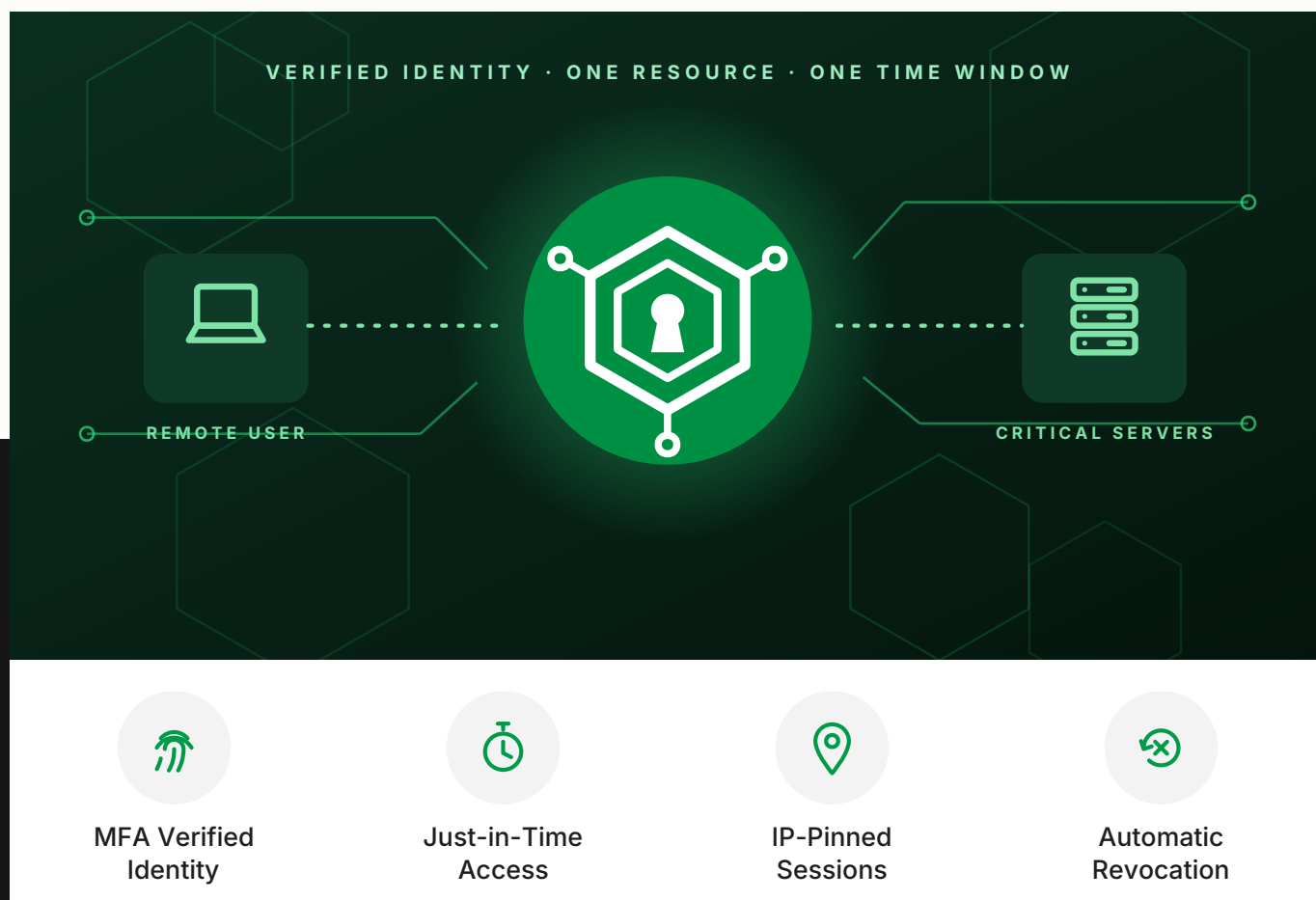
Krypton Zero Trust **Network Access**

Secure, Time-Bound Access to Critical Systems

Your servers and critical systems are the backbone of your organization — but they are reachable only from inside the office network.

- Emergencies don't wait for office hours. Admins, vendors and remote teams need a safe way to reach servers and blocked resources — from anywhere.
- Opening firewall ports or sharing VPN credentials exposes the entire network, and temporary permissions are rarely revoked once granted.

Eliminate standing access risks and secure your critical systems with identity-verified, IP-pinned, time-bound access — granted in seconds, revoked automatically.





The Problem with Open Access

- ✗ VPNs expose the entire network to one login
- ✗ Standing access is rarely revoked
- ✗ Firewall changes take hours or days
- ✗ Credentials shared with vendors and visitors
- ✗ No record of who accessed what, and when
- ✗ Trust based on location, not on identity



Built on Zero Trust

Krypton ZTNA applies Zero Trust security to every access request:

- ✓ Never trust, always verify
- ✓ Least-privilege access only
- ✓ Identity + source IP verified on every login
- ✓ Every grant is time-bound
- ✓ Complete audit visibility

Key Features



Secure Portal Login

Username, password and OTP delivered on WhatsApp or email verify every user



Verified Source IP

Access opens only for the user's validated public IP — credentials alone are not enough



One-Click Server Access

Choose a server on the portal and connect — the door opens instantly for your IP



Time-Bound Access Windows

Every grant carries an expiry, enforced by the system — never by human memory



Instant Mobile Approvals

Admins get a notification on their phone and approve or deny requests in one tap



Self-Service Requests

Users request servers or blocked resources (e.g. YouTube) for a specified duration



Role-Based Administration

Super Admin adds more admins and creates every kind of user, including third parties



End-to-End Encryption

All confidential data is fully encrypted in transit and at rest



Central Server Inventory

Hardware and software details of every server, available on the ZTNA portal



Automatic Revocation

Access is removed the moment the time window ends — zero standing privileges

Real-World Use Cases



Emergency Admin Access

From outside the office

Admin on leave logs in with MFA, picks a server and connects — access opens for his public IP only, for a given time.



Time-Bound Web Access

Through the firewall

A designer requests YouTube for a set duration. Admin approves on phone; access is removed automatically when the time ends.



Third-Party / Vendor Access

Scoped & supervised

Visitors get their own ZTNA login from the Super Admin and can access only the servers they have been granted.

Ideal for Critical Environments



Production
Servers



System Admin
PCs



Database
Systems



RDP & Remote
Access



Blocked Web
Resources



Vendor & Visitor
Access



Branch
Connectivity



Sensitive Folders
& Drives

Roles & Administration



Super Admin

Adds more admins, creates all kinds of users — employees, contractors and third parties.



Admin

Approves or denies access requests instantly and manages assigned servers and users.



User

Requests and uses access strictly within assigned permissions — nothing else is visible.

Why Choose Krypton ZTNA?

- ✓ No network-wide exposure — ever
- ✓ Zero standing privileges
- ✓ Works with Fortinet & existing firewalls
- ✓ Fully encrypted, end to end
- ✓ Access in seconds, not days
- ✓ IP-pinned, time-bound sessions
- ✓ Complete audit visibility
- ✓ Built on Zero Trust architecture



A Must-Have for every Server & Critical System

Secure your organization against credential misuse, network exposure, unauthorized access and permissions that never expire