portnox®

PORTNOX CLOUD

Zero Trust Network Access (ZTNA)

Enterprise-grade zero trust access for applications and infrastructure

Modern enterprises need secure access to cloud applications and the infrastructure behind them. Traditional VPNs were never designed for today's distributed environments—and they introduce unnecessary risk by extending broad, network-wide trust.

Portnox Zero Trust Network Access (ZTNA) replaces legacy VPN access with a cloud-native, identity- and device-aware model that delivers secure, granular access to applications, services, and administrative infrastructure—without exposing the network.

Only the right users. Only the right access.

Portnox ZTNA eliminates implicit network trust by enforcing access policies at the application and service level—not the network layer. Instead of granting broad connectivity, users receive access only to the specific resources explicitly authorized by policy.

This approach significantly reduces attack surface and prevents lateral movement, even if credentials are compromised.

Secure access to:

- Cloud and SaaS applications
- Hosted and on-prem applications-prem applications
- Infrastructure and administrative services (SSH, RDP, and more)

Passwordless, identity-first authentication

Portnox ZTNA supports passwordless authentication using certificate-based and identity-driven methods. Eliminating passwords reduces exposure to phishing, credential theft, and account compromise while delivering a better experience for users and administrators.

KEY CAPABILITIES

- **Secure Remote Access**
- **Passwordless Authentication**
- **Continuous Risk Evaluation**
- **Policy-driven Compliance**
- **Automated Remediation**
- **Fully Cloud-native**

SECURITY OUTCOMES

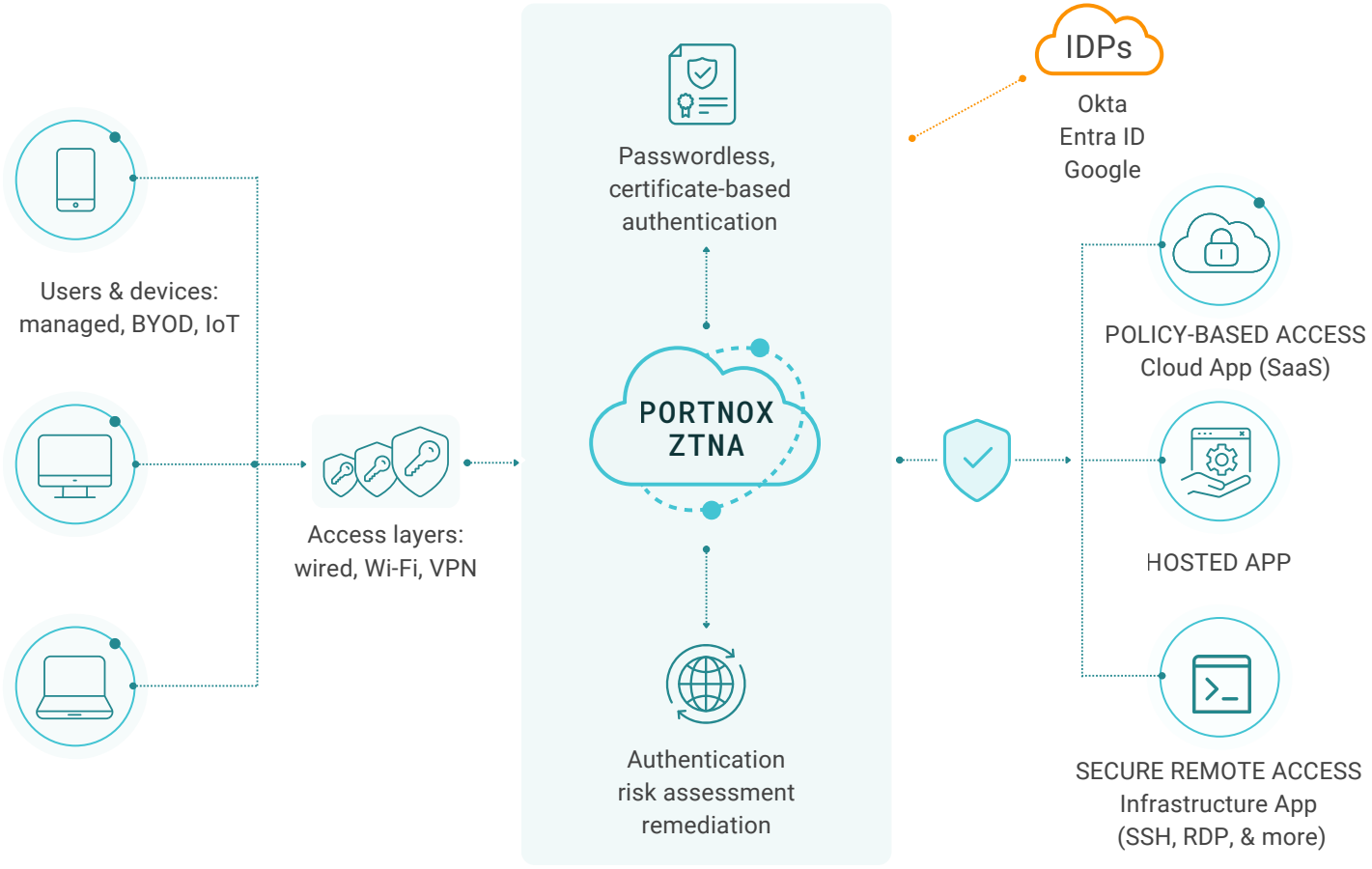
- Eliminate implicit network trust—only verified users and compliant devices can access resources
- Reduce attack surface with passwordless authentication and granular, identity-based policy controls
- Prevent lateral movement through continuous risk assessment for users and devices
- Gain full visibility into user activity with session recording for console apps, including RDP, SSH, and more
- Scale and deploy quickly with ease powered by cloud-native architecture
- Centralize visibility through unified platform built for zero trust access control

Continuous trust evaluation

Portnox continuously evaluates user identity, device posture, and risk throughout each session. If a device falls out of compliance—such as missing patches or disabled endpoint protection—access can be automatically restricted or revoked in real time.

This continuous evaluation model helps organizations prevent breaches *before* they happen, not after.

NON-COMPLIANT DEVICES ARE AUTOMATICALLY REMEDIATED THROUGH POLICY-DRIVEN WORKFLOWS, MINIMIZING I.T. EFFORT AND USER DISRUPTION.



PORTNOX ZTNA: SECURE ACCESS, SIMPLIFIED.

Portnox ZTNA provides a practical, scalable foundation for zero trust access—reducing attack surface, limiting lateral movement, and modernizing enterprise access without unnecessary complexity.

Unlike VPNs or identity-only ZTNA solutions, Portnox enforces access at the application and service level and continuously evaluates trust throughout the session.

www.portnox.com/portnox-cloud/ZTNA