Portnox Cloud   Conditional Access

Passwordless authentication & risk mitigation for your enterprise applications.

Today, people are working anywhere and everywhere – remotely, on-site, or hybrid – and from any device. This means they're accessing their business-critical applications from potentially insecure networks and unprotected devices. This greatly expands every company's threat surface, and creates a number of security challenges for IT.

But have no fear – with Portnox Cloud you can now protect all your enterprise applications, whether they reside in the cloud or on-premises. Portnox's Conditional Access solution extends the same powerful passwordless authentication, role and location-based access control, endpoint risk posture assessment, and automated remediation capabilities you've come to know and love – now for applications!

Passwordless Authentication

The vast majority of data breaches start with compromised passwords – level up your security with certificate-based authentication and never worry about a phishing e-mail ever again. Portnox can act as your PKI and make distribution simple with self-enrollment and agent deployment. Or, you can BYOC (Bring Your Own Certificate) and never have your IT team handle another "password reset" ticket again

Endpoint Risk Mitigation

Now you can take device security even further - our risk policy engine will assign a risk score to devices based on criteria you set. Block access based on a wide variety of essential security policies, such as:

- Require smartphones to have a passcode
- Require laptops to have antivirus running and up to date
- Require drive encryption like FileVault or BitLocker
- Block devices with unsafe open ports

Automated Remediation & Compliance

Portnox Cloud brings automated remediation options to our already robust risk policy engine. Imagine if IT never has to explain - again - that you can't have an unauthorized USB drive plugged in to your laptop and log in to an application like Salesforce or Peoplesoft that contains extensive confidential information.

Depending on the operating system, Portnox Cloud can automatically:
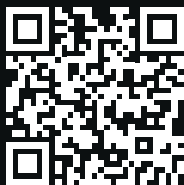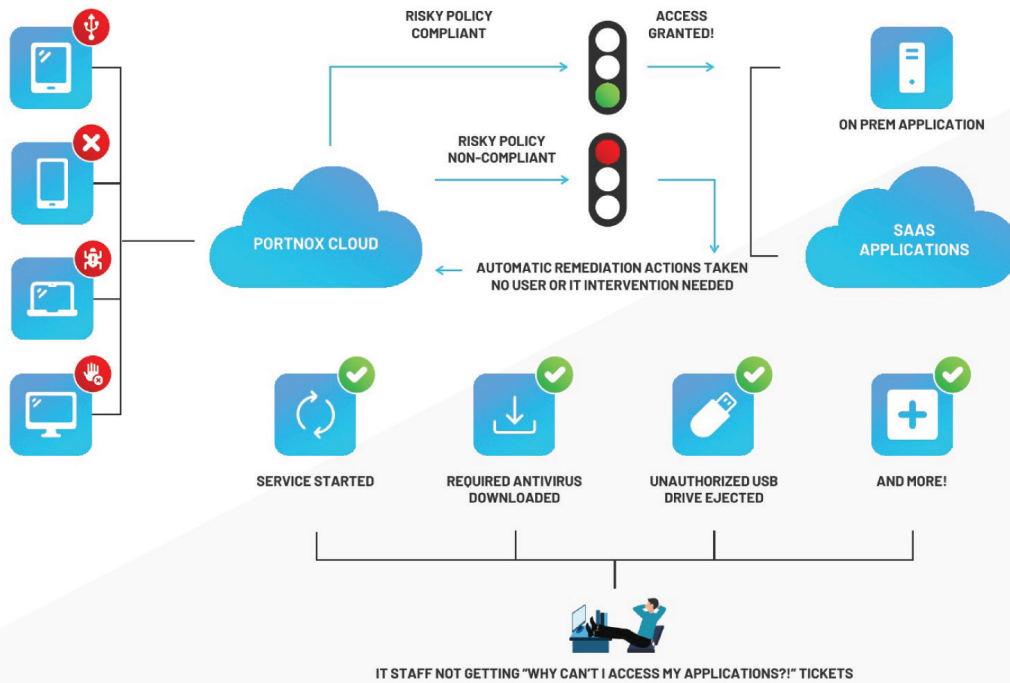
- Start a service
- Remove a peripheral device
- Start a firewall
- Remove an application
- Update Antivirus
- Add a registry key
- ...and many more!

You can have peace of mind that your applications are not at risk. Plus, your IT team will get fewer administrative tickets, and your users will connect to the applications they need seamlessly - everyone wins!

Key Features:

Secure SaaS application access (CASB)

Secure access to on-prem applications

Passwordless authentication

Endpoint risk posture assessment

Application-specific risk profiles

Policy enforcement & automated remediation

Audit tracking & logging

Integration with existing identity provider

OpenID Connect

SIEM integration

MDM integration

RESTful API

Conditional Access for Applications in Action

RISKY POLICY COMPLIANT → ACCESS GRANTED! → ON PREM APPLICATION

RISKY POLICY NON-COMPLIANT

PORTNOX CLOUD

AUTOMATIC REMEDIATION ACTIONS TAKEN
NO USER OR IT INTERVENTION NEEDED

SAAS APPLICATIONS

SERVICE STARTED

REQUIRED ANTIVIRUS DOWNLOADED

UNAUTHORIZED USB DRIVE EJECTED

AND MORE!

IT STAFF NOT GETTING "WHY CAN'T I ACCESS MY APPLICATIONS?!" TICKETS

portnox

Try Portnox Conditional Access for Applications Today!

Start your free 30-day trial today at www.portnox.com/free-trial-ztap/

About Portnox

Portnox offers cloud-native network and endpoint security essentials that enable agile, resourceconstrained IT teams to proactively address today's most pressing security challenges: the rapid expansion of enterprise networks, the proliferation of connected device types, and the increased sophistication of cyberattacks. Hundreds of companies have leveraged Portnox's award-winning security products to enforce powerful network access, endpoint risk monitoring and remediation policies to strengthen their organizational security posture. By eliminating the need for any onpremises footprint common among traditional information security systems, Portnox allows companies — no matter their size, geo-distribution, or networking architecture — to deploy, scale, enforce and maintain these security policies with unprecedented ease.