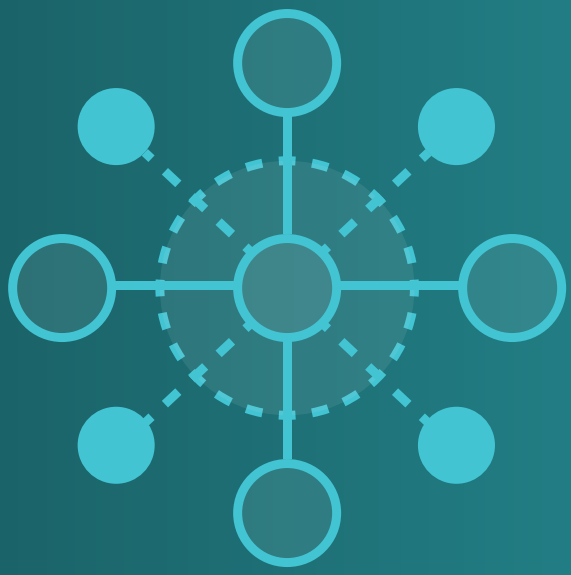
portnox®

WHITE PAPER



The Next Generation of ZTNA

Continuous, context-aware, and built for the enterprise

Executive Summary

Enterprise organizations are operating in an access landscape that has fundamentally changed. Hybrid work, large-scale cloud adoption, and increasingly distributed infrastructure have expanded the attack surface far beyond the traditional network perimeter. According to IBM, 30% of breaches involved data spread across on-prem, public cloud, and private cloud environments. The average time to identify and contain those breaches took 276 days, with an average cost of $5.05M.[1]

At the same time, the consequences of access misuse—whether through credential compromise, misconfiguration, or lateral movement—have become more severe and more visible. Identity has become the dominant attack surface in modern environments. Verizon reports stolen credentials as the most common initial access method in breaches, with it accounting for 88% of all web application breaches.[2]

Legacy remote access models, particularly VPN-based approaches, were not designed for this level of scale, complexity, or risk. Recognizing that the current environment has evolved beyond the legacy VPN use case, CISO respondents to the most recent Portnox survey shows that 93% plan
to replace legacy VPNs by 2027.[3] While Zero Trust Network Access (ZTNA) emerged as a modern alternative, many early implementations focused narrowly on identity-based authentication and web application access, limiting their effectiveness in large, heterogeneous environments.

This paper presents a refined ZTNA model tailored for enterprise requirements. It outlines the architectural principles necessary to enforce zero trust consistently across applications and infrastructure, emphasizes the importance of continuous trust evaluation, and explains how Portnox ZTNA supports these objectives through a cloud-native, policy-driven approach designed for enterprise scale.

[1] *IBM, Cost of a Data Breach Report 2025*
[2] *Verizon, 2025 Data Breach Investigations Report*
[3] *Portnox, CISO Perspectives for 2026*

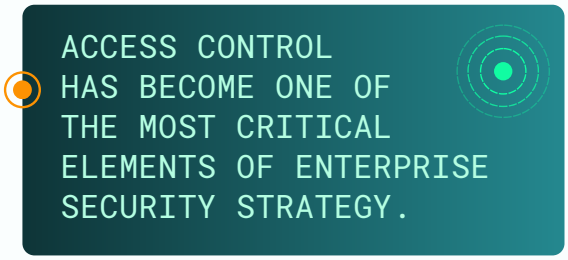
Table of Contents

The Pitfalls of Secure Remote Access

Enterprise environments no longer have clear or static boundaries. Applications and services span public cloud platforms, private data centers, and hybrid environments, while users and systems connect from a wide range of locations and device types. Business operations depend on seamless access to critical resources, yet security teams must manage this access without introducing excessive risk or operational friction.

In this context, access control has become one of the most critical elements of enterprise security strategy, directly influencing risk exposure, compliance posture, and operational resilience. However, many organizations still manage network access and application access as separate domains, governed by different tools, policies, and operational teams.

This fragmentation creates gaps in visibility and enforcement. ZTNA solutions may restrict access to specific applications but often lack awareness of how devices connect to the network itself—particularly for unmanaged, IoT, or non-user-driven connections. Conversely, traditional Network Access Control (NAC) solutions enforce network-level access but may not extend cleanly into modern, cloud-hosted applications.



A unified access control approach brings these domains together. By applying the same trust signals, policies, and enforcement principles across both network and application access, organizations can enforce zero trust consistently—regardless of how, where, or what is connecting.

The Limits of VPNs and Early ZTNA

VPNs were originally designed to extend internal network access to remote users. In large enterprises, this model introduces significant risk by granting broad connectivity to environments that were never intended to be fully exposed. Even when segmented, VPNs enable lateral movement and rely heavily on static assumptions about trust.

Operational complexity further limits VPN effectiveness. Managing tunnels, firewall rules, and routing policies across distributed environments increases administrative overhead and the likelihood of misconfiguration. These challenges are magnified as organizations scale globally and adopt hybrid infrastructure models.

ZTNA solutions were introduced to address these shortcomings by shifting access decisions from the network to individual applications. However, early implementations rely primarily on identity as the core trust signal. While authentication is necessary, identity alone does not account for device posture, environmental context, or changing risk conditions during an active session. This is particularly critical as credential-based attacks remain one of the most common breach vectors across enterprise environments.

At enterprise scale, these limitations become more pronounced. As device diversity increases and access policies grow in number, point-in-time identity checks are insufficient to support durable zero trust enforcement.

Why Enterprise ZTNA Deployments Fall Short

ZTNA promised least-privilege access enforced at the application level, reducing exposure and limiting lateral movement. In practice, many enterprises have found that early ZTNA deployments introduce new challenges when applied across complex environments.

Overreliance on one-time authentication can leave gaps when device security state changes after access is granted. Highly granular policies—when not paired with strong architectural controls—can also lead to policy sprawl and operational complexity that mirrors legacy access models.

These outcomes underscore a critical requirement: ZTNA must function as a continuous trust framework, not a point-in-time access decision. Leading zero trust frameworks are explicit: NIST says trust must be continually evaluated, and CISA says each user, device, application, and transaction must be continually verified. Without continuous evaluation and enforcement, zero trust principles are difficult to sustain in large, dynamic enterprise environments.

What Enterprises Require from ZTNA

For ZTNA to be effective at enterprise scale, it must be implemented across the organization's environment, and must extend beyond simple application gating. Zero trust adoption is widespread but execution remains incomplete—many organizations' zero trust deployments do not cover the entire environment. Enterprise environments are dynamic by nature, with constantly changing users, devices, locations, and risk conditions. As a result, ZTNA must operate as a continuous trust framework rather than a static access control mechanism.

An enterprise-ready ZTNA model evaluates multiple trust signals throughout the access lifecycle. These signals include user identity, device posture, and contextual factors such as location, network conditions, and observed risk indicators. Access decisions must adapt dynamically as conditions change, rather than remaining fixed for the duration of a session.

> ZTNA MUST FUNCTION AS A CONTINUOUS TRUST FRAMEWORK, NOT A POINT-IN-TIME ACCESS DECISION.

ZTNA must also support heterogeneous environments. While managed endpoints can provide rich telemetry through persistent agents, enterprises must account for scenarios where agents are impractical or impossible, such as with contractors, IoT devices, or unmanaged systems. Consistent policy enforcement across both agent-based and agentless access scenarios is essential.

Finally, enterprise ZTNA must avoid reintroducing implicit trust through architecture. Centralized enforcement points or broad network connectivity create bottlenecks, increase blast radius, and undermine zero trust principles. Enforcement should occur as close as possible to the protected resource, supporting scalability, resilience, and precise control.

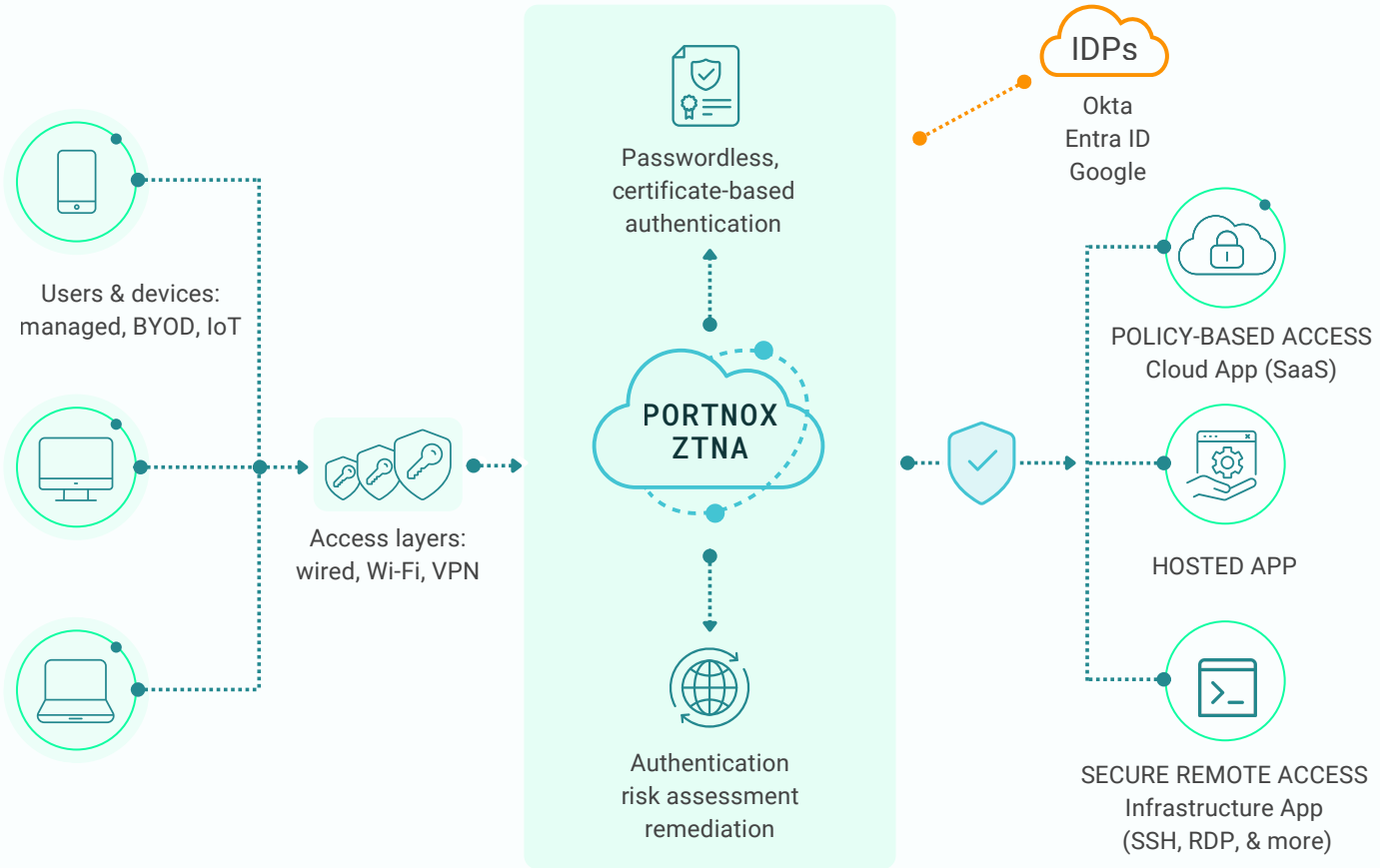
The Portnox Approach to ZTNA

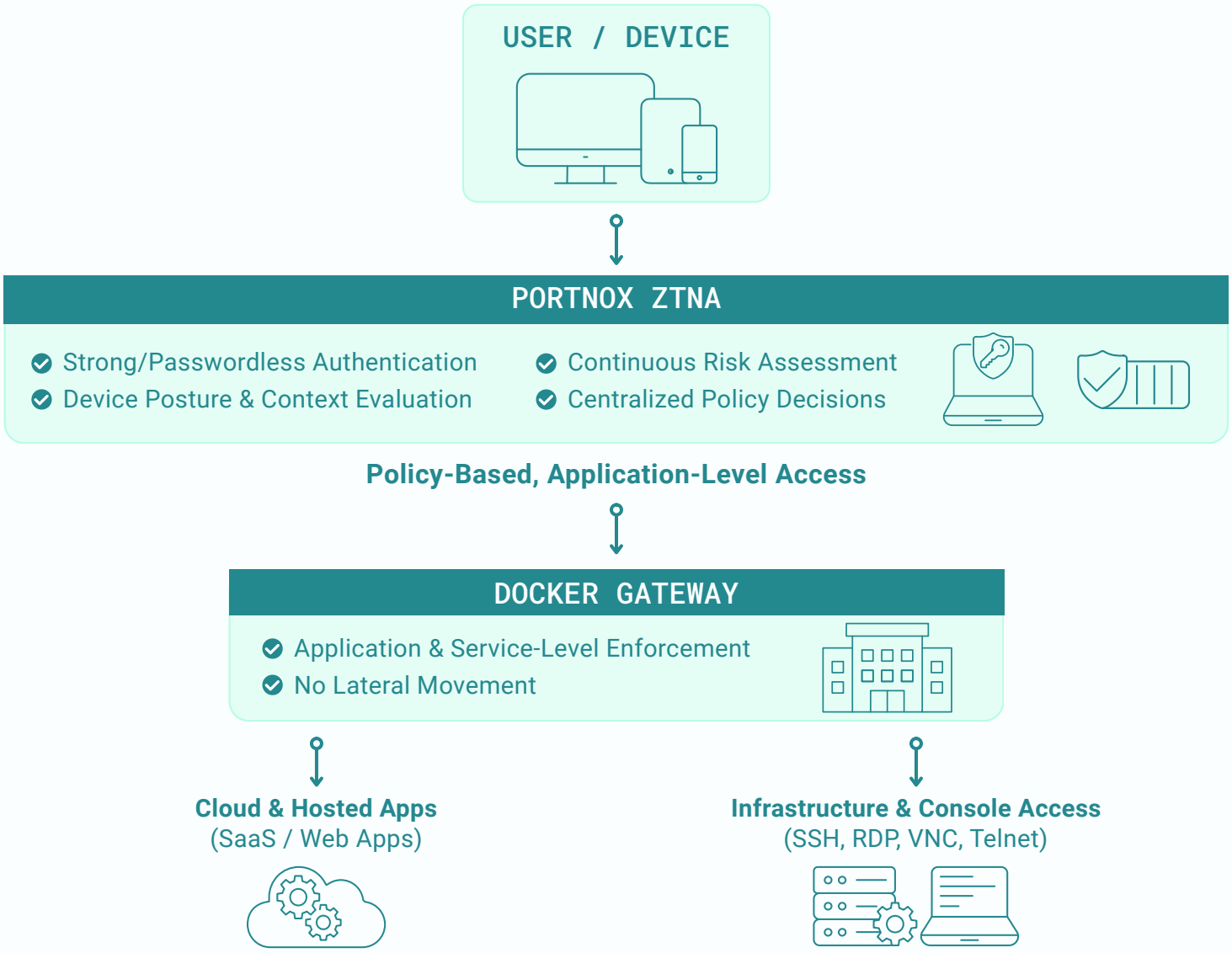
Portnox ZTNA was designed to meet these enterprise requirements by combining continuous trust evaluation with a distributed, policy-driven architecture.

By integrating identity verification with ongoing device posture assessment and contextual risk evaluation, Portnox enables organizations to enforce least-privilege access without extending implicit network trust. Access decisions are continuously evaluated, allowing policies to adapt as conditions change rather than relying on point-in-time authentication.

Portnox supports both agent-based and agentless access models, ensuring consistent enforcement across managed endpoints, unmanaged devices, and non-user-driven connections. This flexibility allows enterprises to apply zero trust principles uniformly across users, applications, and infrastructure without introducing operational complexity.

Delivered through the Portnox Cloud platform, Portnox ZTNA separates centralized policy definition from application- and service-level enforcement. Policies are defined and governed centrally, while enforcement occurs at the access boundary of each protected resource. This approach eliminates reliance on network tunnels, reduces lateral movement risk, and aligns access control with the realities of modern, distributed enterprise environments.





Enterprise-scale ZTNA Architectural Principles

At enterprise scale, architectural rigor determines whether ZTNA remains sustainable over time. Centralized policy definition provides governance, auditability, and consistency, while distributed enforcement ensures that access control scales naturally with infrastructure growth.

By localizing enforcement close to protected resources, enterprises reduce latency, minimize potential choke points, and limit the blast radius of access decisions. This architecture supports high availability and operational resilience without reintroducing network-level trust assumptions.

Portnox's cloud-native design enables this separation of control and enforcement, allowing organizations to maintain centralized visibility while enforcing access decisions precisely where they are needed.

Operational Visibility and Governance

For enterprise organizations, ZTNA success must be measurable and auditable. Security teams require visibility into who is accessing which resources, from what devices, and under what conditions. This visibility supports not only threat detection, but also compliance and governance requirements.

Effective ZTNA platforms provide centralized logging, reporting, and policy review capabilities that enable continuous monitoring and validation. When treated as an ongoing program rather than a one-time deployment, ZTNA becomes a durable component of enterprise security architecture.

Fast, Frictionless Access Control

While many ZTNA platforms offer broad protocol support, enterprise differentiation lies in architectural sustainability and operational maturity. Portnox ZTNA emphasizes continuous trust evaluation, device-aware access decisions, and enforcement at the application and service boundary rather than reliance on static, identity-only controls.

Delivered as a cloud-native, vendor-agnostic solution, the Portnox Cloud platform — including Portnox ZTNA — integrates with existing enterprise identity and security ecosystems without requiring disruptive re-architecture. Its design supports large, distributed organizations seeking to modernize access control while maintaining governance and operational efficiency.

Secure Access with Zero Trust

For enterprise organizations, ZTNA is not simply a replacement for legacy remote access technologies—it is a foundational element of modern security strategy. Effective ZTNA enables precise control over access to critical resources, reduces attack surface, and supports consistent enforcement across complex environments.

Portnox ZTNA delivers an enterprise-focused approach to zero trust by combining context-aware access decisions, continuous trust evaluation, and scalable architecture. When implemented as part of a broader zero trust strategy and integrated with Network Access Control (NAC), it provides CISOs with a practical, sustainable foundation for securing enterprise environments at every connection.

Portnox is a global leader in enterprise access control for every identity. Its unified, cloud-native platform helps organizations secure human, machine, device, and AI identities across networks, applications, and infrastructure with continuous enforcement, real-time visibility, and passwordless access. By enabling organizations to identify risk, enforce policy, isolate threats, and revoke access in real time, Portnox helps modern enterprises reduce complexity and strengthen security across distributed environments. Trusted by enterprises worldwide and securing nearly one million devices, Portnox delivers modern access security for every identity, everywhere. Learn more at Portnox.com and on LinkedIn.