# .BRAND as the DNS Trust Anchor for Zero Trust

Zero Trust has become the dominant cybersecurity framework because it recognizes a core reality: implicit trust is a vulnerability. Hybrid work, multi-cloud architectures, and modern threat actors have erased traditional network perimeters. Every user, device, and application must be continuously authenticated—regardless of its location.

Yet even the most mature Zero Trust models share a persistent gap: the public domain namespace. DNS was built for openness, not security. It still operates largely in plaintext and remains exposed to spoofing, hijacking, cache poisoning, and lookalike domain attacks. As long as critical identity and access points live on public top-level domains (e.g., .com, .net, .uk), attackers can deploy convincing copies that bypass user awareness and undermine authentication.

This structural weakness creates a fundamental inconsistency: Zero Trust demands verified identity, but its root identifiers often remain spoofable.

## The Structural Solution: A .BRAND TLD

A .BRAND top-level domain is an enterprise-owned, enterprise-controlled namespace. Only the brand—and no third party—can register domains under it. This exclusivity creates a non-spoofable origin for authentication, access, and administration.

With a .BRAND TLD, high-risk and high-trust entry points can move under an authenticated, exclusive namespace:

- Workforce and customer SSO at login.brand
- Zero Trust Network Access (ZTNA) and VPN at vpn.brand
- Administrative consoles at admin.brand
- API gateways at api.brand
- PKI and certificate services at pki.brand
- Email infrastructure authenticated under *.brand with DMARC, SPF, DKIM, and DNSSEC

As attackers cannot impersonate *.brand, the DNS layer finally works for—not against—Zero Trust.

## Security Impact

Organizations adopting a .BRAND TLD see three immediate advantages:

1. Phishing resistance increases: Modern authentication mechanisms such as WebAuthn and passkeys bind to domain origin. If the origin is *.brand, attackers cannot reproduce it.

2. Policy becomes simpler and enforceable: Instead of chasing malicious domains across the open internet, Zero Trust policy becomes a single allow-list—trust only *.brand.

3. SOC signal quality improves: The namespace becomes clean, deterministic, and centrally controlled. Certificate mis-issuance is minimized, DNS integrity is consistent, and anomalies are easier to detect.

# .BRAND as the DNS Trust Anchor for Zero Trust

## Business Impact

Enterprises using .BRAND can expect:

- Reduced credential theft and impersonation
- Lower security operations overhead
- Faster incident detection and containment
- Stronger compliance posture
- Clearer user guidance ("If it's not *.brand, don't click.")

## Evidence from Round 1

ICANN last opened the application window in 2012 for a time-limited window. Fourteen years later, 453 .BRAND TLDs currently exist on the internet and adoption patterns show accelerating use for identity, access, and internal infrastructure.

Eighty-nine .BRAND TLDs now use their TLD for Zero Trust-aligned functions such as identity endpoints, remote access, PKI, admin surfaces, APIs, and email infrastructure. Adopters include Microsoft, Google, Amazon, Barclays, AXA, Citic, BMW, Leclerc, Abbott Laboratories, Sky, and others.

Across leading adopters, three trends emerge:

- High-stakes industries are leading the shift due to regulatory and fraud-related pressures.
- Organizations with complex ecosystems—APIs, distributed infrastructures, broad partner networks—gain disproportionate benefit.
- AI-driven impersonation risk is accelerating adoption as identity-verified infrastructure becomes essential.

## Making the Change

Shifting to a .BRAND TLD is not a cosmetic or marketing decision. It is a foundational redesign of how the enterprise establishes and enforces digital trust.

Successful adoption requires:

- Executive sponsorship
- Defined funding
- Alignment across security, IT, identity, and infrastructure teams
- Clear governance and transition planning
- Most critically: access to a .BRAND TLD

# .BRAND as the DNS Trust Anchor for Zero Trust

## The 2026 ICANN Application Window

ICANN will open its second-ever .BRAND application window from April 30, 2026 through August 12, 2026. Once it closes, the opportunity may not return for a decade or longer.

For organizations pursuing Zero Trust, this is a pivotal—and rare—moment. A .BRAND TLD provides a secure origin attackers cannot imitate, resolving a structural weakness that has persisted for decades.

## Conclusion: A Strategic Decision Point

Organizations face a clear choice: anchor identity on a public, spoofable namespace—or secure identity on a namespace designed for authenticity, integrity, and control.

Zero Trust cannot be fully realized on foundations attackers can copy. A .BRAND TLD eliminates that constraint.

The enterprises that secure their .BRAND during the 2026 window will define the next era of trusted digital infrastructure. Those that miss it will continue operating on a namespace attackers already know how to exploit.

The strongest Zero Trust strategy begins with a trusted origin. 2026 is the moment to secure one.