Zero Trust

Zero Trust is not a single product — it is a security strategy built around continuous verification, least privilege access, and strong visibility across users, devices, applications, and data. Brite helps organizations move toward Zero Trust by strengthening identity controls, validating device posture, improving network visibility, and applying policy-based access across hybrid environments.

Through managed cybersecurity services, endpoint protection, identity access controls, network security, and device visibility solutions, Brite helps customers reduce implicit trust and limit the impact of compromised accounts, unmanaged endpoints, and lateral movement.

Why Zero Trust?

Strengthen Access Decisions
Verify users, devices, and access requests before allowing connections to critical business systems.

Reduce Lateral Movement
Limit what attackers can reach if an account, endpoint, or network segment is compromised.

Improve Security Visibility
Gain a clearer understanding of who and what is accessing the environment across users, devices, cloud, and network resources.

Identity & MFA Enforcement
Implement and manage multi-factor authentication, SSO, and identity policies to reduce credential-based risk.

Device Posture Validation
Assess endpoint compliance, security tooling status, and patch posture before granting access to sensitive resources.

Network Visibility & Control
Discover, classify, and monitor connected devices to identify unknown, unmanaged, or risky assets.

Segmentation Support
Help design and support access boundaries that limit unnecessary communication between users, systems, and critical assets.

Managed Policy Oversight
Continuously tune access, endpoint, and security policies as customer environments and threats evolve.

Brite
Brite.com
1.800.333.0498
SalesInfo@Brite.com