Device Visibility & Access Control

Organizations cannot secure what they cannot see. Modern networks include managed endpoints, unmanaged devices, IoT, OT, remote users, cloud-connected assets, and third-party systems. Brite helps customers improve device visibility and access control through asset discovery, endpoint management, network monitoring, NAC-aligned strategies, and security policy enforcement.

By identifying connected devices, monitoring behavior, and supporting access control policies, Brite helps reduce the risk posed by unknown, unmanaged, or compromised assets.

Why Device Visibility & Access Control?

Discover Unknown Assets
Identify devices connected to the environment, including systems that may not be fully managed or protected.

Enforce Safer Access
Apply policy-based controls that limit access for unauthorized, non-compliant, or risky devices.

Detect Suspicious Behavior
Monitor device activity and communication patterns to identify signs of compromise or misuse.

Device Discovery
Identify and classify endpoints, servers, IoT, OT, and other assets connecting to the customer environment.

Dynamic Asset Inventory
Maintain better visibility into hardware, software, and network-connected assets over time.

Network Access Control Support
Support NAC and access control strategies that restrict unauthorized or non-compliant devices.

Traffic & Behavior Monitoring
Monitor network and endpoint activity for abnormal behavior that may indicate compromise.

Automated Response Actions
Where integrations allow, quarantine, isolate, or restrict risky devices through coordinated response workflows.

Brite

Brite.com
1.800.333.0498
SalesInfo@Brite.com