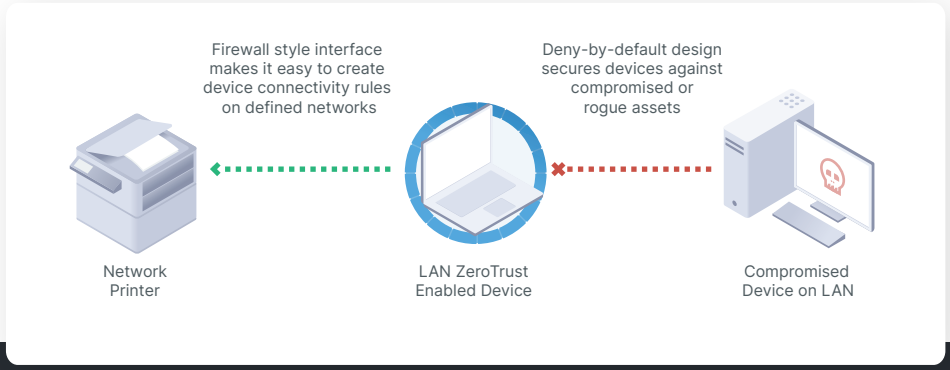
todyl

LZT LAN ZeroTrust

Stop lateral movement, APTs, and the spread of threats while securing internal networks

In the work from everywhere world, isolation and segmentation on the Local Area Network (LAN) are critical. Traffic on internal networks cannot be assumed safe, whether on corporate, public, or home networks. IoT devices on networks are increasingly used as entry points due to their notoriously poor security. The proliferation of ransomware and persistent threats creates new challenges in distributed and on-prem environments. More than ever before, it's critical to have a defense-in-depth strategy that segments and secures internal networks to prevent threats from spreading and threat actors from moving laterally.

Todyl's LAN ZeroTrust (LZT) is a unique technology built with a firewall-inspired interface that makes controlling internal traffic easier. It leverages a deny-by-default design where devices on internal networks can no longer freely communicate without explicit policies. LZT greatly reduces threat actor's ability to move laterally with granular segmentation of internal networks.



Benefits

Simplified Segmentation
Easily segment internal networks without overhauling architectures, VLANs, or other complex solutions

Granular, Identity-Based Access Control
Devices require explicit rules to communicate and are based on identity, reducing the attack surface area and preventing lateral movement

Rapid Lockdown
With the touch of a button, all communication ceases between devices on the LAN, preventing the spread of threats

Highlights

Next-Generation of Network Access Control
LZT is location aware, providing granular policy control of LAN traffic based on a user's location.

Conditional Access to Sensitive Resources
Adds another layer of protection for sensitive applications and services by requiring users to authenticate for access.

Meet Compliance Requirements
Combining multi-factor authentication (MFA) with LZT helps meet compliance requirements, such as CMMC.

Hides Users on Shared Networks
Users working from home, hotels, airports, and other shared networks are protected against local network threats since LZT makes these devices essentially invisible.