APPGATE®

AppGate SDP IoT Connector

Extend Zero Trust to Unprotected IoT Devices

Most robust security strategies account for a wide variety of devices. Yet many older Internet of Things (IoT) connected devices are often left unmanaged and unprotected. As these devices are connected to the same network as users, servers, and sensitive data, they can be a weak link in an organization's security strategy.

AppGate's SDP IoT Connector leverages the core principles of Zero Trust to secure unmanaged devices, restricting lateral movement and reducing an organization's attack surfaces. It provides granular control of how and when devices connect to a network, as well as which network resources they can connect to. IoT Connector is a part of AppGate, a unified security platform that enforces consistent access policies across user devices, servers, and IoT devices to shore up any vulnerabilities across all network touch points.

BENEFITS

Protect complex, distributed resources

Reduce attack surface by limiting over-privileged device access

Enforce access control policies across users, servers, and IoT devices

Reduce operational complexity with simple-device management

Decrease audit scope to lower compliance costs

Unified zero trust security across all legacy & modern IoT devices

| cameras | printers | phones | smart devices | smart cars | smart screens | smart medical devices | ATM |

| Consolidated logging, threat visualization, and monitoring | Customizable policies for greater control | One centralized policy enforcement system | Infrastructure-agnostic platform that supports any architecture |

Key Features

Devices are confined to pre-set segments to reduce the vulnerabilities of unmanaged devices, including phones, cameras, sensors, and other IoT devices.	Enables organizations to fully leverage the power of smart devices in a way that is secured and managed appropriately.	Offers secure, granular control of resources depending on how, when and where devices are connecting to the network.	Explores creative connectivity options to extend access to partners and third parties while maintaining full network access control.

How It Works

AppGate Connector is a gateway between connected IoT devices and the network. Devices make access requests to AppGate Controller, and the platform sends an authentication challenge, then evaluates credentials and applies access policies based on the user, environment and location.

A dynamic 'Segment of One' network is created for each device session. Once a connection is made, all access to the resource travels from the device through an encrypted network gateway to the server. Access is logged through the LogServer, ensuring there's a permanent, auditable record of user access.

APPGATE CONTROLLER

mTLS TUNNEL

APPGATE
CONNECTOR

APPGATE
GATEWAY

APPGATE
CLIENT

DATA CENTER
RESOURCES

APPGATE