appgate

USE CASE

APPGATE SDP CONNECTOR FOR IOT

Extend Zero Trust to Unprotected IoT Devices

A remote access security strategy should account for all exposed devices, yet many connected IoT devices are often left unmanaged and unprotected. As these devices are connected to the same network as users, servers, and sensitive data, they present a weak link in an organization's otherwise sound security strategy.

Appgate SDP IoT Connector leverages the core principles of Zero Trust to secure unmanaged devices, restricting lateral movement and reducing an organization's attack surface. The Connector provides granular control of how and when devices connect to a network, as well as which network resources they can connect. The IoT Connector is fully integrated with Appgate SDP, a unified security platform that enforces consistent access policies across user devices, servers, and unmanaged devices to shore up any vulnerabilities across all network touch points. This cohesive approach provides security and operational agility for conditional maintenance to these devices.

BENEFITS

- Protect distributed, hard to secure resources
- Reduce attack surface by limiting over-privileged device access
- Enforce access control policies across users, servers, and IoT devices
- Streamline operations with common SDP access across all enterprise devices
- Dramatically reduce audit scope to simplify compliance

UNIFIED ZERO TRUST SECURITY ACROSS ALL LEGACY & MODERN IOT DEVICES

Cameras | Legacy Systems | Phones | Sensors | Automobiles | Kiosks | Medical Devices | Financial Terminals

Consolidated logging, threat visualization, and monitoring

Customizable policies for greater control

Inbound & outbound secure access for complete control

Infrastructure-agnostic platform that supports any architecture

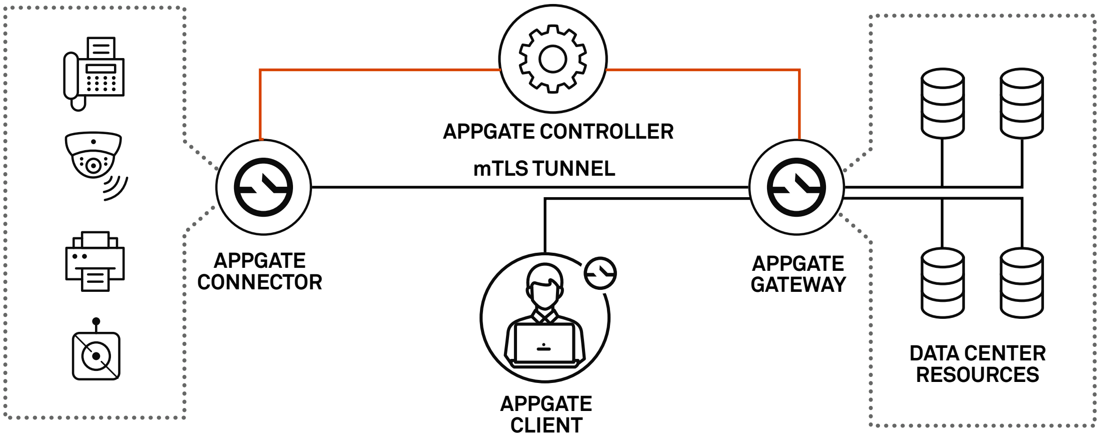
KEY FEATURES

Devices are restricted to specific segments to prevent over-entitlement and lateral threats regardless of device type, network, or location	Enables organizations to extend Zero Trust principles to specific devices independent of underlying architecture	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

The Appgate Connector is a gateway between connected IoT devices and the network. The Appgate Connector initiates access requests to an Appgate Controller. The Controller responds with 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. All access is logged through the LogServer, ensuring there's a permanent, auditable record of user access.



DEPLOYMENT OPTIONS

The Appgate IoT Connector is available as a physical appliance or a virtual machine (VM). The Ax-M is a USF (ultra-small form factor) physical appliance. For more information about the Ax-M, please reference the datasheet.

appgate