neeve

02

Secure, Remote, Low Latency Access to in-Building Video Management Systems

Why

Problem	Solution

Conventional methods for remote access to in-building video management systems pose operational complexity and cyber attack surfaces. Also, network latency can pose a issue for optimal user experience of streaming video

Unmanaged remote access: Connections to VMS and control systems using VPNs and TeamViewer etc circumvent infosec security policies, and creates VPN sprawl

Provides too broad access to OT systems: Remote access is at a network level not device level. No role based access granularity at a per device, per user, per building level

Lacks audit capability: No centralized user management and audit trails

Poor video quality: Streaming video can appear laggy due to network latency inherent in VPN technology

Neeve provides all-in-one solution for secure, remote access to your in-building video management systems
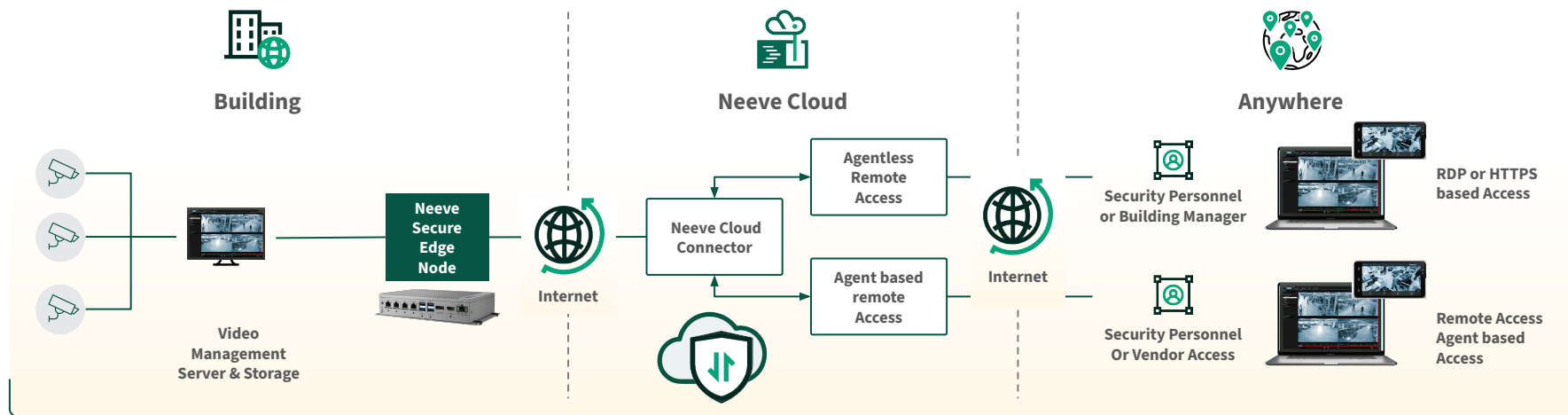
Agent-based remote access: Running an agent on the remote user device (desktop or mobile) can address potential latency issues through SD-WAN optimization

Zero-Trust security: Granular access down to the endpoint level, connects the right user to the right device on the right port in the right building

Simplified user management: Easy to add users and assign privileges based on role (vendor, FM, building engineer, etc.). Single-sign-on can integrate authentication with your internal identity provider

Expand access to additional OT systems: BMS, Lighting, Access Control, Elevator management system, etc.

How It Works: Secure, Low Latency, Anywhere access to On-Site Video Management System

Building

Neeve Cloud

Anywhere

Neeve Secure Edge Node

Internet

Video Management Server & Storage

Neeve Cloud Connector

Agentless Remote Access

Agent based remote Access

Internet

Security Personnel or Building Manager

Security Personnel Or Vendor Access

RDP or HTTPS based Access

Remote Access Agent based Access

Benefits

1

WAN Optimized Remote Access
Running an agent on the remote user device (desktop or mobile) can address potential latency issues through SD-WAN optimization

2

Zero-Trust Security
Granular access down to the endpoint level. Connects the right user to the right device on the right port in the right building

3

Simplified User Management
Easy to add users and assign privileges based on role (vendor, FM, Building Engineer, etc.). Single-sign-on can integrate with your internal identity provider

4

Expand access to additional OT systems
BMS, Lighting, Access Control, Elevator, etc.