

Secure Remote Access System



The S3M EndGuard agent infrastructure offers an end-to-end encrypted, centrally managed, and cost-effective remote access experience without the necessity for third-party software.

Problem Description:

Enterprise Security Vulnerabilities in Remote Access

As hybrid and remote work models become increasingly prevalent, IT and security teams encounter substantial challenges in accessing endpoints.

Third-party remote access applications:

- It broadens the attack surface by establishing unregulated tunnels within the corporate network.
- It exacerbates the challenges of patch and configuration management owing to supplementary software dependencies.
- By remaining outside centralized logging and auditing processes, one creates a loss of visibility.

Furthermore:

- The distinct licensing of NAC, remote desktop, and file transfer solutions elevates the total cost of ownership (TCO).
- Switching between various vehicles adversely affects incident response times (MTTR).

Solution:

Secure Remote Access Integrated with S3M EndGuard

S3M Secure Remote Access is a comprehensive solution that operates natively on the EndGuard Agent, providing secure, enterprise-grade remote access without additional software.

- ✓ Runs within the existing EndGuard Agent infrastructure
- ✓ Eliminates the need for extra installation and licensing
- ✓ Enables fast, one-click secure connection

All session traffic is end-to-end encrypted and can be monitored in real time via the central management console, resolving visibility and control issues of third-party tools.

During remote access:

- Software, updates, and configuration files can be transferred securely.
- IT teams can manage systems remotely without physical access.
- Operational processes become faster and more seamless.

Key Attributes



✓ No supplementary software necessary.

EndGuard Agent operates natively and does not necessitate third-party tools such as TeamViewer or AnyDesk.

✓ No additional expenses are necessary.

It is part of your license; no separate remote access license is needed.

✓ Secure Document Distribution

Delivering MSI, EXE, configuration files, and updates through an encrypted channel.

✓ Central Session Records

Each remote access session is recorded on an individual user basis and incorporated into the audit trail.

✓ Role-Based Access Control

EndGuard Agent operates natively and does not necessitate third-party tools such as TeamViewer or AnyDesk.

✓ Prompt Action

IT and SecOps teams reduce MTTR by directly accessing the endpoint during an incident.

How does it function?

Secure Remote Access in Four Steps

Establish a secure connection within seconds via the S3M EndGuard infrastructure, eliminating the need for complex VPN setups or third-party tools.

Step 1 – Initiating the Session:

Start a session with a single click by selecting the target endpoint from the central management console.

Step 2 – Secured Connection:

An end-to-end encrypted connection is automatically established through the EndGuard Agent (no VPN required).

Step 3 – Intervention and Transfer:

Operations are performed via remote desktop, with necessary files shared through a secure channel.

Step 4 – Documentation and Review:

All activities are logged centrally, and the session is securely terminated.

S3M Secure Remote Access Solution Diagram

