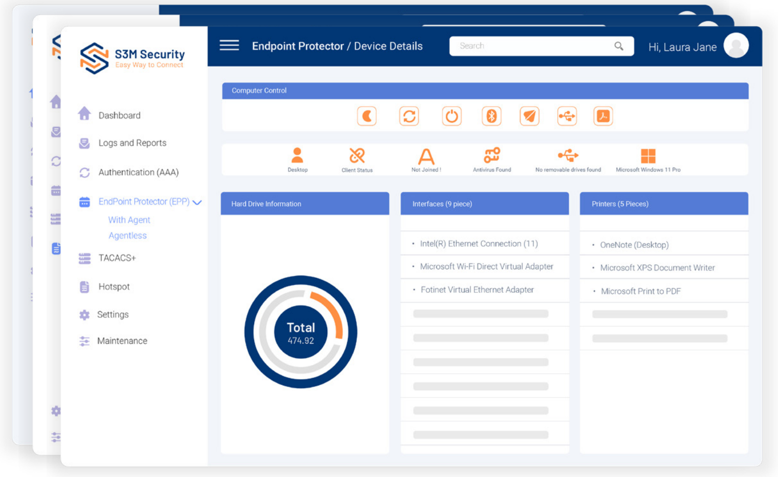
S3M Security
Easy Way to Connect

Access Control • Network Automation • Device Healthcheck



Interfaces (9 piece)

- Intel(R) Ethernet Connection (11)
- Microsoft Wi-Fi Direct Virtual Adapter
- Fotinet Virtual Ethernet Adapter

Printers (5 Pieces)

- OneNote (Desktop)
- Microsoft XPS Document Writer
- Microsoft Print to PDF

EPP MODULE

Endpoint protection is a crucial aspect of network security. It involves securing all entry points to a network, such as laptops, smartphones, and other devices, to prevent unauthorized access and cyber-attacks. By implementing endpoint protection measures, organizations can significantly reduce the risk of security breaches and protect sensitive data.

> With EPP Module, it is possible to work without domain dependency in the agent architecture.

During the application phase, connection to the remote device is provided with Powershell and SSH. Data collection and editing can be performed by running WMI, Powershell, SSH and CMD commands. Network access of unsuitable devices can also be changed with dynamic VLAN switching methods from active network devices with SNMP and SSH access.

Hardware and software inventory collection system

Thanks to the internal device hardware and software inventory collection system, the changesmade in the hardware can be observed and reported by the system administrators. This featurehas a very important place in the security approaches of companies to easily view and reportdevice and material changes, unusual movements in these hardware materials, and perhapssuspicious events, which are made unannounced by the system administrators and maypotentially lead to security threats.Besides all that, EPP module provides an insight to the organizations by observing the resourceusage of the devices. In this way, potential unnecessary expenditures are prevented. In thisway, a fully equipped endpoint security is provided for organizations that can save both timeand money.

2-stage management

EPP Module uses a 2-stage management and verification mechanism in agentless architecture, either standalone or in a hybrid structure. In the first stage, the basic authentication functions and basic controls of the device are provided, while the user and device that passes this stage are included in the authorized group. Instead of preventing the user from working and waiting like other manufacturers, after the authorization mechanism, special checklists belonging to the user's group are started to be applied and repeated. During the application phase, connection to the remote device is provided with Powershell and SSH. Data collection and editing can be performed by running WMI, Powershell, SSH and CMD commands. Network access of unsuitable devices can also be changed with dynamic VLAN switching methods from active network devices with SNMP and SSH access.

sales@s3msecurity.com | support@s3msecurity.com