Agent-based:

Which should be preferred?

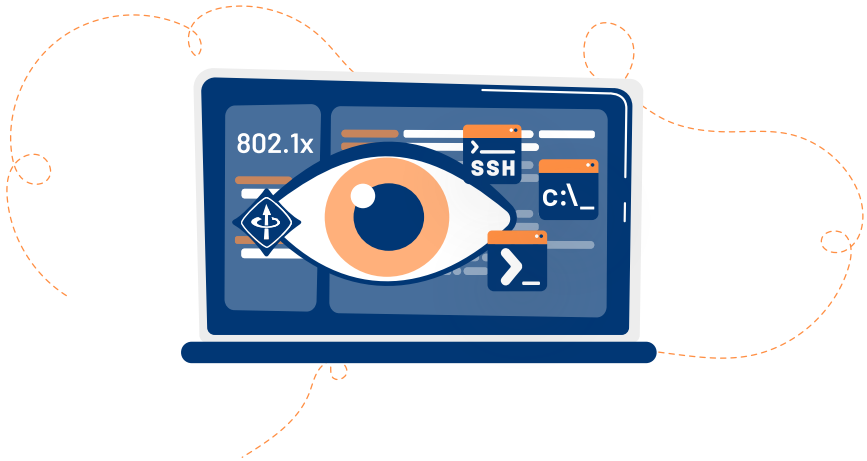
S3M Security
Easy Way to Connect

Introduction

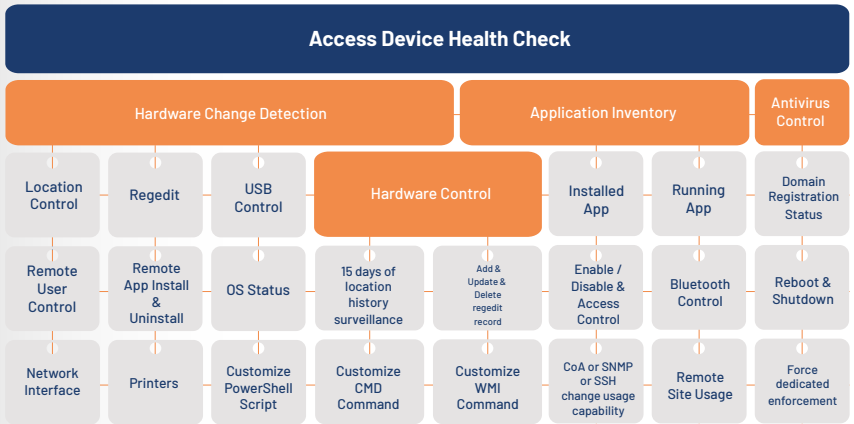
- Network access control (NAC) is a critical component of any organization's security infrastructure. NAC systems enforce policies that determine which devices are allowed to access the network, and what resources they can access once they are connected. One key decision that organizations need to make when implementing NAC is whether to use an agent-based or agentless solution. In this whitepaper, we will examine the differences between these two approaches, their advantages and disadvantages, and which one is best suited for different use cases.

Agent-based NAC:

An agent-based NAC requires the installation of a software agent on every device that needs network access. The agent typically performs a variety of tasks, such as verifying the device's identity, checking for security updates, and ensuring that the device complies with the organization's security policies before allowing access to the network.



HYBRID ARCHITECTURE



Advantages:

- The primary advantage of an agent-based NAC is its ability to provide detailed information about the device requesting access to the network. This level of granularity allows organizations to create very specific access policies based on factors such as the device type, operating system, and software installed on the device. This fine-grained control can be particularly valuable in highly regulated industries, such as healthcare and finance.

- Another advantage of an agent-based solution is that it can provide continuous monitoring of the device's security posture while it is connected to the network. This means that if the device falls out of compliance with the organization's security policies, it can be immediately disconnected from the network.

Disadvantages:

- The primary disadvantage of an agent-based NAC is the need to install and maintain software agents on every device that requires network access. This can be a significant logistical challenge for organizations with large, distributed networks. The agents can also consume system resources on the device, potentially impacting performance.

- Another potential disadvantage of an agent-based solution is that it may not be compatible with all types of devices. For example, some IoT devices may not support the installation of software agents, making it difficult to enforce security policies on these devices.

Agentless:

Which should be preferred?

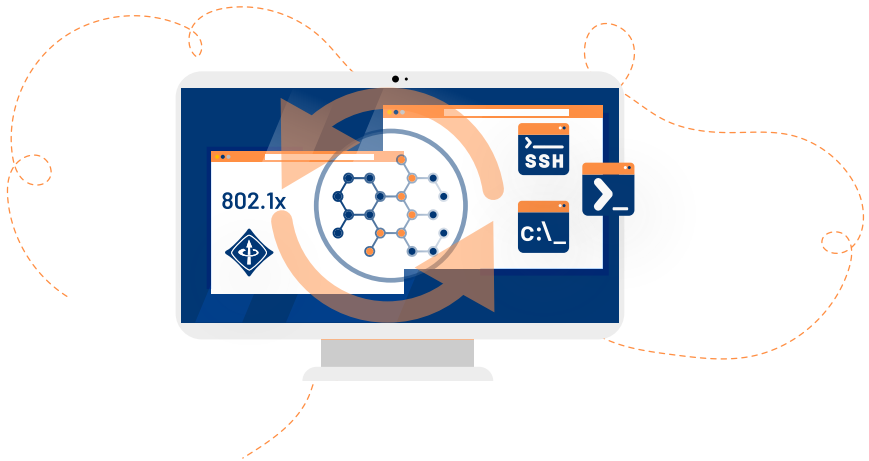
S3M Security
Easy Way to Connect

Introduction

- Network access control (NAC) is a critical component of any organization's security infrastructure. NAC systems enforce policies that determine which devices are allowed to access the network, and what resources they can access once they are connected. One key decision that organizations need to make when implementing NAC is whether to use an agent-based or agentless solution. In this whitepaper, we will examine the differences between these two approaches, their advantages and disadvantages, and which one is best suited for different use cases.

Agentless NAC:

An agentless NAC does not require the installation of software agents on devices that require network access. Instead, the solution typically relies on network-level authentication protocols such as 802.1X to authenticate devices and enforce access policies.



Advantages:

- The primary advantage of an agentless NAC is that it does not require the installation and maintenance of software agents on devices. This can be a significant advantage for organizations with large, distributed networks, as it eliminates the need to install software on potentially thousands of devices.
- Another advantage of an agentless solution is that it is generally easier to deploy and configure than an agent-based solution. This can be particularly valuable for organizations with limited IT resources.

Disadvantages:

- The primary disadvantage of an agentless NAC is that it typically provides less detailed information about the device requesting access to the network. This can make it more difficult to create fine-grained access policies based on factors such as the device type, operating system, and software installed on the device.
- Another disadvantage of an agentless solution is that it may be less effective at enforcing security policies on devices that are not fully under the control of the organization. For example, personal devices that are owned by employees may not be fully compliant with the organization's security policies, making it difficult to enforce those policies without the installation of software agents.

Conclusion:

- The decision to use an agent-based or agentless NAC will depend on the specific needs of the organization. An agent-based solution can provide fine-grained control over access to the network and continuous monitoring of devices while they are connected, but it may be more difficult. So why would companies have to choose between the two - when Hybrid NAC technology has already been created? With the S3M Security Endpoint Protector solution, agent-based or agentless architecture can be used together, their advantages can be benefited and the disadvantages can be reduced as much as possible.