Network Access Control and End Point Compliance

Cybercrime continues to rise, with the primary aim to compromise an organisation's information that will make a profit for the perpetrators. To avoid the unwelcome publicity provoked by IT failures, securing the network is more important today than ever before. It's also tougher to achieve, as today's networked world means giving end-users instant access to the information they need while meeting external regulatory compliance standards.

Seema Khanna
Technical Director
seema@nic.in

Most organisations don't have a realistic idea of who is connecting to the network, let alone how and what information they might have access to. In many cases, it is unlikely that unauthorised network guests will have malicious intentions, but simply that they don't have adequate IT protection on their computer, which could present hackers with an entry point to the network. While there's an obvious need for organisations to secure their own endpoints, they must also consider the level of access they wish to grant to visitors

End-Point Compliance- An Overview

The term End Point is used in a variety of ways in different contexts. For this paper, an End Point is an individual computer system, workstation or personal computing device. Common endpoints are laptops, desktops, and personal computing devices. An application server can also be considered an End Point when it functions as a network host.

End Point Compliance is the sum total of the measures taken to implement security concerning endpoints/ desktops. These measures include assessing risk to protect endpoints, such as with client antivirus and personal firewall, and protecting the network from the endpoints themselves, such as with quarantine and access control. Also, End Point Compliance logically extends to the management and administration of these security measures, as well as to the risk, reporting, and knowledge management of the state and results of these measures

The need of End Point Compliance

The growing number and variety of threats to endpoints has made endpoint protection an essential tool. Current threats include viruses, Trojans, worms, the use of endpoints as DDoS zombie hosts, and spyware. New threats and new types of threats emerge on a regular basis. These threats take advantage of a growing number and variety of endpoint vulnerabilities. These vulnerabilities include the familiar, such as buffer overruns; the more insidious, such as keystroke-loggers and instant-messaging worms.

Organisations end up with extreme vulnerability to a bewildering array of threats that increase each day. Endpoints are where the typical organisation conducts most of its day-to-day operations, and disruption to endpoints is a huge impact to an organisation. Since endpoints are now a primary target of these threats, organisations are forced by necessity to confront Endpoint protection and compliance as a core issue.

Importance of End Point Compliance

There are two main blocks in the networked world. The Data Center, where the resources (intranet and information for public use) are kept and the users (end nodes). The end node could be a simple user or resource provider. Today, securing a data center is a default action whereas the act of securing desktops has been an area which has been majorly overlooked due to various reasons. In the past few years this weak link has been exploited successfully by a hacker. End points are millions in number and majority of them are non IT users thereby making them a good target to initiate the process for compromise. Hence, it is extremely important to protect end points with minimum discomfort to the user.

Modus Operandi

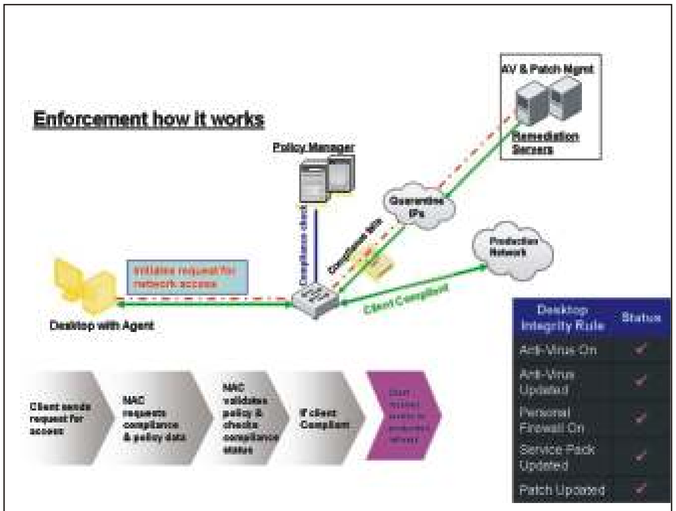
NAC solutions permit access to authorised computers by evaluating and enforcing the computers' security state based on whether they comply with the organisation's security policy. Endpoint computers are permitted access to network resources when they conform to policy, and are denied or quarantined from access when they do not conform. Effective NAC solutions rely on the ability of the network to positively enforce compliance and affirmatively block or quarantine access to unauthorized computers.

Traditional security solutions, such as firewalls, anti-virus, anti-spyware, patch management, or VPNs are no longer sufficient to prevent devices connecting to the network with unpatched software, out-of-date anti-virus and improper security settings. Not keeping devices up to date is probably the largest hole in the security fight today.

There are various ways to implement endpoint compliance countermeasures. Any administrator with access can flip a switch to turn off a service or shut down a port without understanding the true ramifications of doing so. The real challenge with implementing security for any living and breathing network is almost never a question of "how" to lock something down, but rather, "how-best" to lock something down so that it still does what you need it to do.

Due to extensive reach and use of network, organisations now need proactive End Point security measures that can protect against zero-day attacks and even unknown threats. They need to take a structured approach to End Point security, implementing a comprehensive solution that not only protects from threats on all levels, but also provides interoperability, seamless implementation, and centralised management.

An ideal solution to be deployed in a diverse network should have inbuilt antivirus and antispyware signature-based protection. It should also provide protection from targeted attacks and attacks not previously seen. It should analyse application behaviors and network communications to detect and block suspicious activities, as well as administrative control features that allow administrators to deny specific device and application activities deemed to be high risk for their organisation.



Mechanism of End Point Compliance

While you may not be able to control everything your end-users do, you can take control of the last mile and implement better policies and technologies that make sure all devices accessing the network are healthy and secure. *i*