Endpoint compliance

Highlights

Enhanced endpoint security verifies devices for:

- Anti-virus, anti-spyware software.
- Personal firewall software.
- Specific OS versions.
- Patch levels.
- Browser types.

Maintains security state of endpoint devices.

Use pre-defined or custom policies to protect your network.

Quarantine, remediate, deny or grant access to non-compliant devices.

Supports Windows, Mac, Linux, iOS, Android and Google Chrome.

Leverages Trusted Computing Group's endpoint security specifications.

Overview

In the Everywhere Workplace, demand has skyrocketed for access to applications in the cloud and data center via personally-owned devices (BYOD). This access is great for productivity but presents security challenges. It's Even with the best intentions, employees, contractors and third parties may be using devices infected with malware or spyware. Of course, there's also the risk of threat actors using stolen devices or credentials.

Ivanti's enhanced endpoint security feature queries every device before – and during – a connection to the network to ensure that it meets corporate security policies. Enhanced endpoint security makes sure that jailbroken or rooted devices, or devices with unpatched operating systems, don't connect to your hybrid IT resources. Even better, non-compliant devices can be quarantined or remediated, reducing the chance of malware propagation.

How it works

- Endpoint devices are checked prior to and during a remote access session based on pre-defined or custom policies that administrators define.
- Enhanced endpoint security performs endpoint health and security checks to ensure a device meets corporate security requirements.
- Administrators can choose from a variety of pre-defined and custom policies.
- Pre-defined policies check for third-party applications such as the presence of antivirus and antispyware, OS versions, hard disk encryption status, patch levels and browser types.
- Custom rules can include inspection checks such as absence or presence of specific files, certificate checks, TCP ports, processes, registry key settings, NetBIOS name, MAC addresses or certificate of the client machine and third-party inspection methods (custom DLLs).

Policies at-a-glance

Policies can be deployed individually or combined for advanced host checking. Wildcards and environment variables can be used. Host Checker policy results can be stored and reused at a later time to validate one or more devices.

Remediation based on a policy can be automatic (where changes are made on the remote device) or manual (where the user is notified that their device is out of compliance). Devices can be also be quarantined, limiting access until the device is corrected. Reports can be generated that show which devices are compliant, non-compliant, remediated or not assessed during specified intervals.

Pre-defined policies
Anti-virus software installed
Operating System (OS) version
Firewall software installed
Anti-spyware software installed
Hard disk encryption
Patch management
CVE checks

Custom policies
Remote integrity verifiers.
Check for third-party or custom DLLs.
Verify open/closed ports
Confirm running/stopped processes
Check for file presence on remote device
Confirm registry keys are set
Check NetBIOS name, MAC addresses and machine certificate validity.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com