

BSA Network Access Control

Best-in-class network access control technology, easily deployed

BSA Network Access Control is an easily deployed Network Access Control (NAC) product that provides a powerful, comprehensive, and cost-effective way to control access to the enterprise network, in real-time. It enables authorizing, authenticating, and evaluating devices and users prior to allowing them access to the network.

The complex and dynamic nature of enterprise networks and the adoption of new IT technologies, such as virtualization, present an enormous challenge for IT managers. Statistically, an additional 20% to 50% of devices reside on enterprise networks without the organization's knowledge. This uncertainty severely undermines the security of the network as security measures are only partially applied. One cannot defend against or manage devices whose existence is unknown.

In order to effectively and successfully deploy and enable access controls against all devices residing on the enterprise network, regardless of their respective capabilities, it is essential to classify devices. For example, knowing whether or not they are capable of user-based authentication (e.g., printer, wireless access points, VoIP phones). The classification determines which verification actions (authorization, authentication, posture evaluation) are to be applied against devices and users accessing the enterprise network before granting them network access.

As part of the Insightix BSA solution suite, the BSA Network Access Control utilizes BSA Visibility to build and maintain, in real-time, a complete and accurate inventory of ALL devices operating on the enterprise network. BSA Visibility enables BSA Network Access Control to operate in real time against ALL devices.

The meaningful network, device, and user intelligence information provided by the unique profiling technology of BSA Visibility enables BSA Network Access Control to select the appropriate verification actions that must be applied against a device as it is being attached to the network. BSA Visibility continuously monitors the network and its connected devices. The real-time network intelligence built and maintained by BSA Visibility enables BSA Access Control to detect and block spoofing attempts that are usually directed at unmanaged devices.

Insightix's patent-pending network access prevention technology, used by BSA Network Access Control, does not require integration with infrastructure components, such as switches or routers, for quarantine and/or enforcement, thereby reducing overhead, which is usually associated with implementing a NAC solution. Network access is evaluated, and prevented if needed, on a device-by-device basis, whether physical or virtual.

With minimal prerequisites and zero physical infrastructure changes, implementing the BSA Network Access Control is easy and fast – its configuration virtually effortless.

BSA Network Access Control is an agentless solution; it does not require any integration with infrastructure components for quarantine and/or enforcement, operates in heterogeneous networks, and is vendor agnostic.



Insightix NAC utilizes agentless visibility functionality... to create a unique NAC solution that applies real time network access controls to everything and anything that connects to the network.

Chris Rodriguez, Research Analyst, Frost & Sullivan



Network Access Control in Action

A new device is attached to the network

- The device is detected in real-time
- The device is immediately quarantined
- The device is profiled and classified (ie. managed or unmanaged, supports user-authentication or not, Windows-based or not, etc.)
- The device's classification determines the verification path it is to go through
- The configuration of the different NAC verification states are then checked for applicability for this device

The system immediately quarantines the device

- The pre-admission device authorization NAC module blocks rogue devices from accessing the network
- Authorized devices may proceed to best NAC verification stage

The user is required to authenticate

- The pre-admission user authentication NAC module operates against device supporting user-based authentication
- Transparent authentication is supported against Microsoft Active Directory infrastructure
- A captive portal is used supporting RADIUS-based authentication

In-Depth Posture Checking and Policy Verification

- Microsoft-based devices can undergo in-depth posture checking (configurable)
- Checking parameters include: service pack, installed patches, A/V, antispyware, personal firewall, installed software, installed services, and registry key values
- If not aligned with access policy, the device would not be granted network access
- Remediation is supported either manually (where the captive portal is used explaining the violations and how they can be remediated) or automatically for a number of configuration parameters

Post-Admission NAC Module

- Real-time provisioning of the device and users successfully admitted to the network
- Deviations from the device's profile result in blocked network access



Features and Benefits

Know What You Are Defending

As part of the Insightix BSA solution suite, the BSA Network Access Control uses BSA Visibility to build and maintain a complete and accurate inventory of ALL devices operating on the enterprise network in real-time. Utilizing unique profiling technology, BSA Visibility provides meaningful network, device and user intelligence.

The information provided by BSA Visibility enables BSA Network Access Control to operate against ALL devices whether capable or not of user-based authentication, managed or unmanaged, physical or virtual.

Real-Time Operation

BSA Network Access Control detects and applies control measures as soon as a device is attached to the network. For example, rogue devices are detected and blocked in real-time.

Your Network, No Changes

Insightix's patent-pending network access prevention technology, used by BSA Network Access Control, does not require any integration with infrastructure components, such as switches or routers, for quarantine and/or enforcement. This eliminates the added costs typically associated with implementing a NAC solution (i.e., buying more switches). BSA Network Access Control works with your existing network – no changes are needed.

Effortless Configuration & Setup

As implementing BSA Network Access Control does not require any integration with infrastructure components the overhead usually associated with implementing NAC is considerably reduced. With minimal prerequisites, zero physical infrastructure changes, agentless operation, implementing the BSA Network Access Control is easy and fast, requiring almost no configuration effort.

Measuring the Effect of Turning NAC On

BSA Visibility provides vast audit information that can be used to simulate the effect NAC would have on the network and the devices connected to it once turned on. This enables the adjustment of key settings prior to enabling NAC, preventing an overwhelming effect against the devices attached to the network and its users when turning NAC on.

Accurate Pre-Planning

The vast audit information provided by BSA Visibility allows accurate pre-planning of the various NAC verification actions to be applied against devices and users accessing an enterprise network. For example, this information makes it possible to easily distinguish unauthorized devices from legitimate devices based on the accurate and in-depth audit information produced by BSA Visibility – thus supporting the blocking of rogue devices in real-time.

Gradual Implementation of NAC

The different verification stages can be either turned on or off, configured for a hybrid operational mode of alerting and enforcing at the same time against different groups of devices and/or users, allowing operation against subsets of the enterprise network, and so on.

