



Business Security Assurance

Solution Brief

Although organizations have made major investments in network security, a significant gap still exists between the actual security state of enterprise networks and what is known to IT.

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, unknown to its own managers.

This uncertainty severely undermines the security state of the network as security measures are only partially applied. One cannot defend against or manage devices whose existence is unknown.

Security and compliance cannot be achieved. At any given moment:

- Not all of the devices are accounted for
- Security measures are not applied against all devices
- Not all of the devices are aligned with the organization's standards and policies

The actual risk an organization is exposed to is unknown, and there is no control over the security status of the enterprise networks. This is the "black hole" of network security. It threatens your business's reputation, revenue, and ability to comply with regulations.

The Insightix Business Security Assurance (BSA) product suite is designed to detect, identify, profile, audit and control ALL devices connected to your network, in real-time.



Control & Enforcement

Safeguarding the network's security integrity by preventing network access from unauthorized and/or non-compliant elements.



Discovery

Comprehensive collection of data from ALL network assets, gathering complete, accurate and detailed continuous network intelligence. This unique approach provides always on, real-time network visibility acting as the foundation for the BSA solution.

Bridging the Network Security Gap.



Remediation

Identification of the corrective measures that must be put in place and fix inconsistencies with the security posture of assets attached to the network. Aligning the security configuration of assets with security best practices considerably reduces the enterprise networks' risk of exposure.



Audit, Compliance & Risk Analysis:

Automated security configuration auditing, simplifying the process of conducting network-wide configuration audits. This provides efficient security compliance tracking and auditing procedures.



User Identity Profiling

Establishment and maintenance of user intelligence by correlating between user identities and specific IP addresses. This improves audit controls, and enhances regulatory compliance. It also significantly enhances incident response by enabling locating vulnerable and/or exploited hosts, and eliminating the manual efforts to track users.

