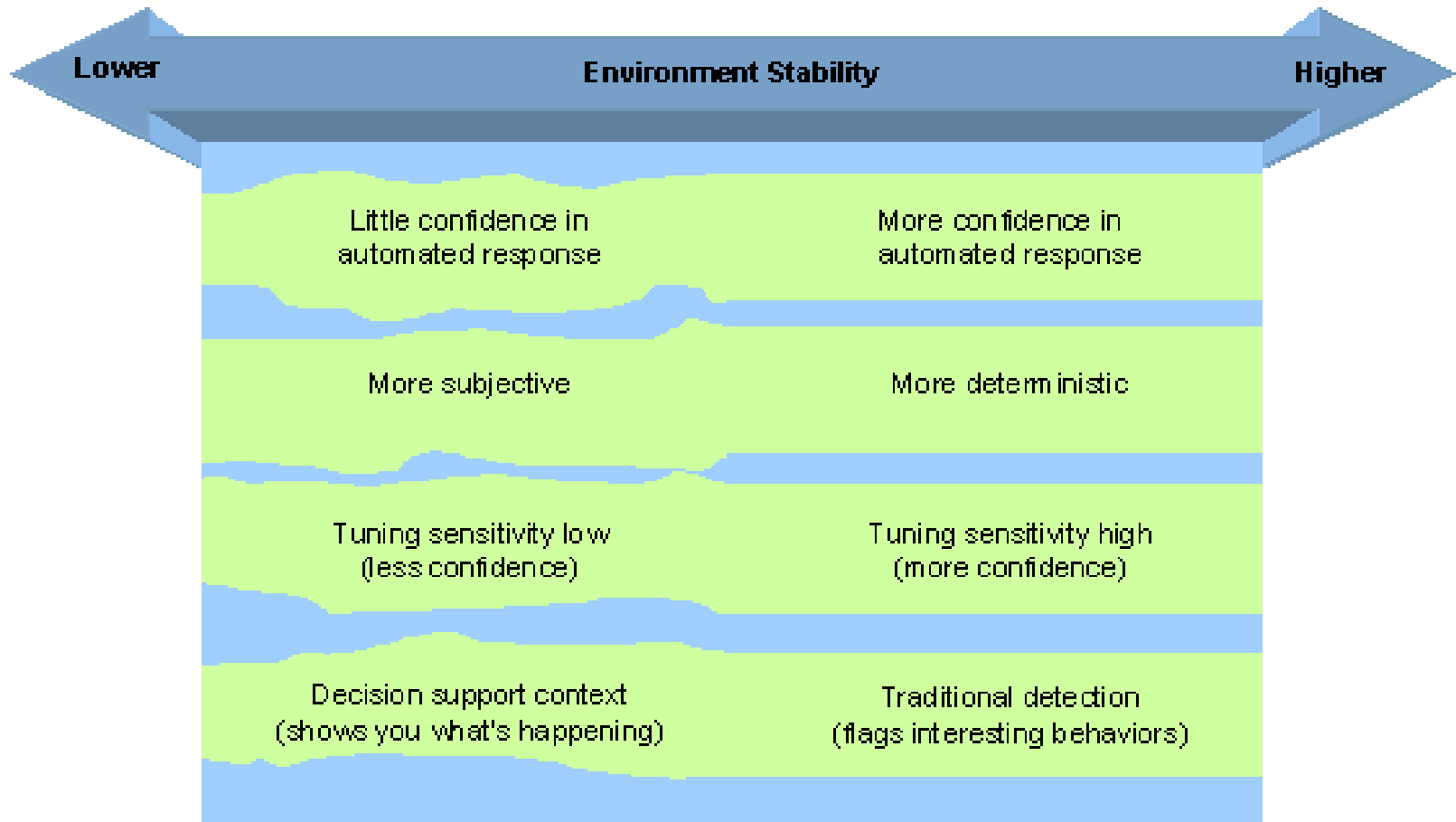


***Managed Security
Services Provider (MSSP)***

Network Behavior Analysis

connet

network stability effects



13+030-1

detection technology

Myth	Reality
Anomaly-detection-automated profiling/modeling/training eliminates tuning.	Anomaly detection doesn't eliminate tuning, but it changes the nature of how the system should be tuned, including which signatures should be enabled and which anomalies should be highlighted and addressed.
Automated response capabilities to enable containment, such as pushing ACLs to network infrastructure, can protect against threats.	Automated response features are present, but most operators are reluctant to turn on the automated response because of the high potential for false positives, and ACL pushing has never proved to be a successful long-term strategy. While NBA produces interesting intelligence, its data is better-suited for investigative rather than automated responses.
NBA catches hard-to-detect insider misuse that cannot be addressed by firewalls and IPSs.	Technically yes, but it is subject to the limitations of determining which anomalies are really important. NBA doesn't substantially affect the difficulty of detecting and addressing malicious insiders.
NBA detects zero-day exploits.	NBA detects infections and helps an organization contain them before they spread, which could be said is the only effective way to deal with zero-day exploits. There's a misperception that NBA can detect zero-day exploits better than other technologies.
NBA is the last line of defense.	This may be true. As decision-support systems, NBA helps organizations address the impacts of various attacks and behaviors on their network.

network behavior analysis vendor

	Arbor Networks	Cisco Systems	CounterStorm	GraniteEdge Networks	Intrusic	Internet Security Systems	Lancope	Mazu Networks	NefFort Technologies	Q1 Labs	Security	Sourcefire
Security												
Operations												
Identity												
Flow Data												
Custom Flow												
DPI												
Less Than 100,000												
100,000 to 300,000												
More Than 300,000												
Carrier												
SIEM												
IDS/IPS												
Vulnerability Management												
DDOS												

Key:

- Gartner does not recommend if you have this requirement
- May meet requirement
- Gartner recommends
- Gartner strongly recommends

Source: Gartner (November 2006)