FUNCTIONS GENERALLY DESIRED:

· Integrates with SMTP email server.	Yes – configured via Threat Management Center (TMC)
· Centralizes policy management.	Yes – within the TMC
· Monitors the health of connected devices.	Yes – CPU/DISK usage etc.
· Operates in inline active mode.	Yes - CounterSnipe Systems may be deployed Inline Active mode.
· Operates in inline simulation mode.	Yes: CounterSnipe Systems operate on a drop and configure bases. There are four modes of operation see fig 3. below
· Operates in passive mode.	Yes – May be configured at Group level or each individual device
· Supports Suricata rules.	Yes – CounterSnipe Systems use suricata as an IDS/IPS engine with the complete Suricata rule set.
· Identifies attacks using pattern matching.	We detect all attacks using industry-leading Suricata engine. In terms of identification we identify vulnerabilities using Common Vulnerability Exposures (CVE) identifiers.
· Identifies attacks using stateful analysis.	Yes
· Identifies attacks using port assignment.	Yes
· Identifies attacks using heuristics.	Yes
· Identifies attacks using protocol tunneling.	Yes
· Identifies attacks using port following.	Yes
· Detects attacks using stateful signature.	Yes
· Detects attacks using protocol detection.	Yes
· Detects attacks using pattern matching.	Yes
· Analyzes traffic using protocol analysis.	Yes all of the analysis is carried out using Suricata
· Analyzes traffic using RFC compliance.	Yes
· Analyzes traffic using pattern matching.	Yes
· Analyzes traffic using TCP reassembly.	Yes
· Analyzes traffic using flow reassembly.	Yes
· Analyzes traffic using signature analysis.	Yes
· Analyzes traffic using Denial of Service attack.	As DOS is an attack and not an analytical technique we

	block most kinds of DOS attacks.
· Responds to attack with drop packet.	Yes – may be configured at device level, group level or globally.
· Responds to attack with silent drop.	Yes – may be configured at device level, group level or globally.
· Responds to attack with drop session.	Yes – In IDS mode by sending a TCP reset to the device being protected. IN IPS mode the CounterSnipe Systems will just drop the bad data.
· Responds to attack with TCP reset	Yes
· Mitigates attacks using content.	CounterSnipe Systems do not change the content in flight. If confident the CounterSnipe SystemsS SYSTEM drops the bad traffic if not confident we avoid the false positive using SAK alerting.
· Mitigates attacks using adaptive behavior	Yes – all mitigation uses adaptive behavior.

CounterSnipe ADDITIONAL FUNCTIONS:

Following are some of the additional functions that the CounterSnipe software has grown to offer. One of the key advantages of using CounterSnipe is our willingness to listen to your requirements for specific features and the speed with which we can deliver those requirements. Our solution is versatile and its application to your networks will provide the most comprehensive network security that is possible today.

Upto 80% of the security breaches occur due to lack of configuration and change management and adapting the security to match that change. With CounterSnipe's offer of install, configure and on going management, you not only selecting IDS security but a whole organization and the knowledge base.

MAC based asset blocking	Once enabled will block any access by a MAC address that is not already known to the system. This is in addition to the IP based blocking.
Quick Location Links	Every system that accesses your network is logged. Quick link provides you ability to check the location and IP history of any system you like in assets page.
Asset Grouping, Scanning, Scheduled Scanning	Create asset groups, eg server

	group. Set up regular scanning for HIPPA. Real time assets awareness by detecting missing assets or by rescanning reappeared assets.
Threshold based alerting	Monitor for DOS attacks or Change in the network usage.
Data Loss Prevention by file detection and storage for forensics.	Files transfers can be detected and blocked based on filenames, MD5s or file types, eg "Microsoft Windows File"
Alerts on discovery of Alien Hosts	Yes – CounterSnipe Systems can be enabled to email you on discovering alien hosts once you are satisfied with the current network status
Actively Scans Newly Discovered hosts	Yes – CounterSnipe Systems can be configured to operate in always-on state for detecting the actual state of all ports on an alien host and emailing the results instantly to security managers.
On-Demand Active Port Scanning of Assets	Priviledged users can be given asset scanning rights in order to build a critical asset profile or assess current state of a host on the network
Detects applications per host	Yes - Drill down facility for each of the hosts allows further information about the applications.
Detects vulnerabilities per host	Yes – TMC presents a list of vulnerabilities associated with each host with a click through option to the MITRE and NIST CVE descriptions for more information.
Identifies vulnerabilities	Yes – CounterSnipe Systems maintain an extensive database of application finger prints and known vulnerabilities thus identifying clearly any detected vulnerabilities.
Prioritizes vulnerabilities	Yes – by comparing detected with the database and associated CVEs
Prioritizes IDS/IPS attack data	Yes – by comparing the attack data with its criticality value

Matches vulnerabilities with attacks	Yes – TMC matches/compares all attack data with the known vulnerabilities before issuing alerts.
Prioritizes alerts	Yes – TMC identifies the source, the destination, type of attack, the presence of a vulnerability, the CVEs and prioritizes alerting accordingly.
Drop and Configure deployment	Yes – In IPS mode the CounterSnipe Systems can be ‘dropped’ in line without effecting the traffic and then configured to suit individual requirements.
Learning operation	Yes – logging the existing network traffic the CounterSnipe Systems can be implemented in a Zero false positive mode. Fine tuning is then possible to include any excluded signatures/rules
Global or group level configuration	Yes – There is no need to configure each CounterSnipe Systems. Configure group settings and add all devices to the group speeds up the installation/configuration process.
Remote addition/deletion of devices	Yes – simply add to/delete from the Managed group.
Hierarchical user management	Yes – Different levels of user access. Including local time zone settings via the TMC
Easy maintenance and support	Yes – TMC offers the facility to automatically (every hour) poll our extensive RISK databases. No human intervention is required for this process.