



DETAILED BRIEF

Mapping StealthWatch to COBIT Control Objectives

Infrastructure Resource Protection and Availability (AI 3.2)

COBIT states to implement internal control, security and audit-ability measures during configuration, integration and maintenance for hardware and infrastructural software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated.

StealthWatch operates as an internal technical control that provides an added layer of network security and ensures continuous network availability. Additionally, StealthWatch is used during times of change, such as in the case of mergers and acquisitions when disparate networks merge to provide a level of stability and control during unstable and uncertain network transition. StealthWatch does this by monitoring host and traffic activity.

Capacity and Performance of IT resources (DS 3.1 thru 3.5)

COBIT states to:

- Plan, review and model (DS 3.1) the performance and capacity of IT resources
- Review current state (DS 3.2) to determine if service level agreements are deliverable
- Forecast future needs (DS 3.3) to minimize the risk of service disruptions
- Provide what's currently required (DS 3.4) and prioritize tasks for when requirements are not met
- Monitor (DS 3.5) to maintain and tune current performance and to report on service availability

StealthWatch baselines network traffic for historical trending, capacity planning as well as network security purposes. Traffic statistics include interface utilization in general, traffic composition, top 10 statistics, out of profile ports and services, QoS bandwidth utilization to name a few. By alarming on deviations from this baseline, StealthWatch helps organizations retain control of resource consumption and assist with proactive and quantifiable network upgrade decisions as opposed to reactive and potentially unfounded bandwidth upgrades.

Security Testing, Surveillance and Monitoring (DS 5.5)

COBIT states to ensure that IT security implementation is tested and monitored proactively. A logging and monitoring function enables the early detection of unusual or abnormal activities that may need to be addressed.

StealthWatch not only provides network visibility and monitoring but provides a "quick clue" as to what is actually happening on the network and where, expediting incident resolution. Security teams find tremendous value in this immediate contextual awareness because it enables them to focus their research on the log records specific to the problem at hand. Without such a solution to focus resource efforts, personnel become overwhelmed by the innumerable events and find themselves searching for the proverbial needle in a haystack.

Malicious Software Prevention, Detection and Correction (DS 5.9)

COBIT states to ensure that preventive, detective and corrective measure are in place across the organization to protect information systems and technology from malware.

Many customers have deployed StealthWatch for this very purpose and many continue to use StealthWatch to detect malware, when oftentimes signature-based systems cannot. Moreover, some customers have also deployed StealthWatch as a “catch all” for their Data Leakage Prevention (DLP) project to supplement traditional DLP tools.

Network Security (DS 5.10)

COBIT states to ensure that security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation and intrusion detection) are used to authorize access and control information flows from and to networks.

StealthWatch provides value here in several ways:

- **Unauthorized access**

When one host, external or internal, tries to access host that’s off limits, StealthWatch alarms on such violations, providing a level of internal security not available with many other security technologies.

- **Firewall misconfigurations**

StealthWatch provides several capabilities that identify and alarm on traffic not necessary for normal business operations as well as traffic indicative of misconfigured devices, including traffic composition reporting, zone locking and host profiling.

- **Third-party integrations**

StealthWatch integrates with a wide array of third-party devices, including IPSes, DDoS mitigation appliances, pre-admission controls and network management systems, to optionally initiate mitigation or remediation actions.

Cost Modeling and Charging (DS 6.3)

COBIT states that based on the service definition, define a cost model that includes direct, indirect and overhead costs of services and supports the calculation of chargeback rates per service. The cost model should be in line with the enterprise’s cost accounting procedures. The IT cost model should ensure that the charging for services is identifiable, measurable and predictable by users to encourage proper use of resources. User management should be able to verify actual usage and charging of services.

StealthWatch consumes and analyzes flow data, an ideal data source for traffic accounting and chargeback. In fact, the original purpose for NetFlow was traffic accounting and continues to be used as such.

IT Infrastructure Monitoring (DS 13.3)

COBIT states to define and implement procedures to monitor the IT infrastructure and related events. Ensure sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.

StealthWatch’s host-centric view of the network provides broader context around network activity not available with packet-centric technologies. In fact, customers use StealthWatch to quickly focus incident resolution efforts on only those security event logs pertinent to the problem at hand.

For more information, please contact 888.419.1462 (US), +1 770.698.8827 (International), or sales@lancope.com