Unified Security Management

Most businesses outside of the Fortune 500 cannot afford a Chief Information Security Officer plus an IT Security Team plus the cost of buying IT security tools. Therefore, businesses are left vulnerable and confused on how to protect and monitor their network; especially small and medium size businesses.

Protecting a network is very similar to protecting a physical building. You need locks, gates, cameras, security guards, etc. In the network world, it is very similar. There are multiple tools that you need; however, unless they are all working together, you are only getting a fraction of the real picture.

Our solution unifies the key parts of security no organization should go without. USM is designed to assess risk, create awareness, and inspect the effectiveness of existing controls for identification and reaction to a problem. This security operation system utilizes five important pillars to prevent, uncover, and respond to threats that have breached your protection.

1. SIEM (Security Incident & Event Management) – Uses Log Management, Event Correlation and Remediation Support Services to correlate and analyze security event data from across your network.
2. Asset Control – Network scanning and monitoring helps USM identify and categorize network and service assets.
3. Vulnerability Management – Vulnerability testing and continuous monitoring helps to identify systems on your network that are vulnerable to exploits.
4. Threat Detection – Network IDS, Host IDS, and File Integrity Monitoring are all key to detect malicious traffic on your network.
5. Behavioral Monitoring – Netflow Analysis and Service Availability Monitoring makes it easy to identify suspicious behavior and potentially compromised systems.

Service Features

▪ Allows you to leverage existing investment in security assets.

▪ Continuous compliance and security surveillance to reduce risk.

▪ Unified Security Mgmt approach:
   1. Asset Control
   2. Vulnerability Management
   3. Behavior Management
   4. Security Intelligence
   5. Threat Management

▪ Customer Web Portal produces reports, tracks events, and creates tickets and more all in one central location.

Business

▪ Cross Customer event correlation

▪ More efficient use of security staff

▪ Better and timely intelligence

▪ Quality analysis

▪ Closes the gap on vulnerabilities

▪ Continuous and comprehensive scanning and review for emerging threats and vulnerabilities