Cautela Labs **Threat Manager**

Protect your network with Threat Management from Cloud based Cautela Labs fully managed solution.

Cautela Labs **Threat Manager** is a cloud based threat management solution that provides a vulnerability and intrusion detection solution with full Integration with **Cautela Labs Enterprise Security Manager,** providing advanced analytics, correlation, alerting, and reporting. All threats are monitored 24x7 under the guidance of our certified analyst and security experts.

Key Advantages

- Intrusion Detection
- Internal and External Vulnerability Scanning
- Dual Scanning engine
- Rule Sets updated daily and weekly
- Multiple sources of Rule Sets
- Cautela Labs Research Team
- Sourcefire VRT
- Emerging Threats
- Third-Party Collaboration
- Custom Rule Creation and Editing
- Robust Dashboard

Features & Capabilities

- Robust dual scanning with 85,000+ multiple IDS signature databases with multiple scanners which is updated daily and/or weekly.
- Rule sets consolidated from multiple sources with real time signature updates to Cautela Labs Enterprise security manager.
- Advanced network traffic and payload visibility with detection of SSL based intrusion traffic and also any web based technologies including anti-virus detection.
- Artificial Intelligence rules engine customized for each client to detect any activity based or signature based threat analysis.
- Defined SLA with a customized escalation process for each client.
- Quickly generates security reports for PCI DSS, GLBA, SOX, NERC CIP, HIPAA, and more.
- Out-of-the-box correlation rules, reports, and responses enable speedy deployment in an hour or less.

CL300

Front

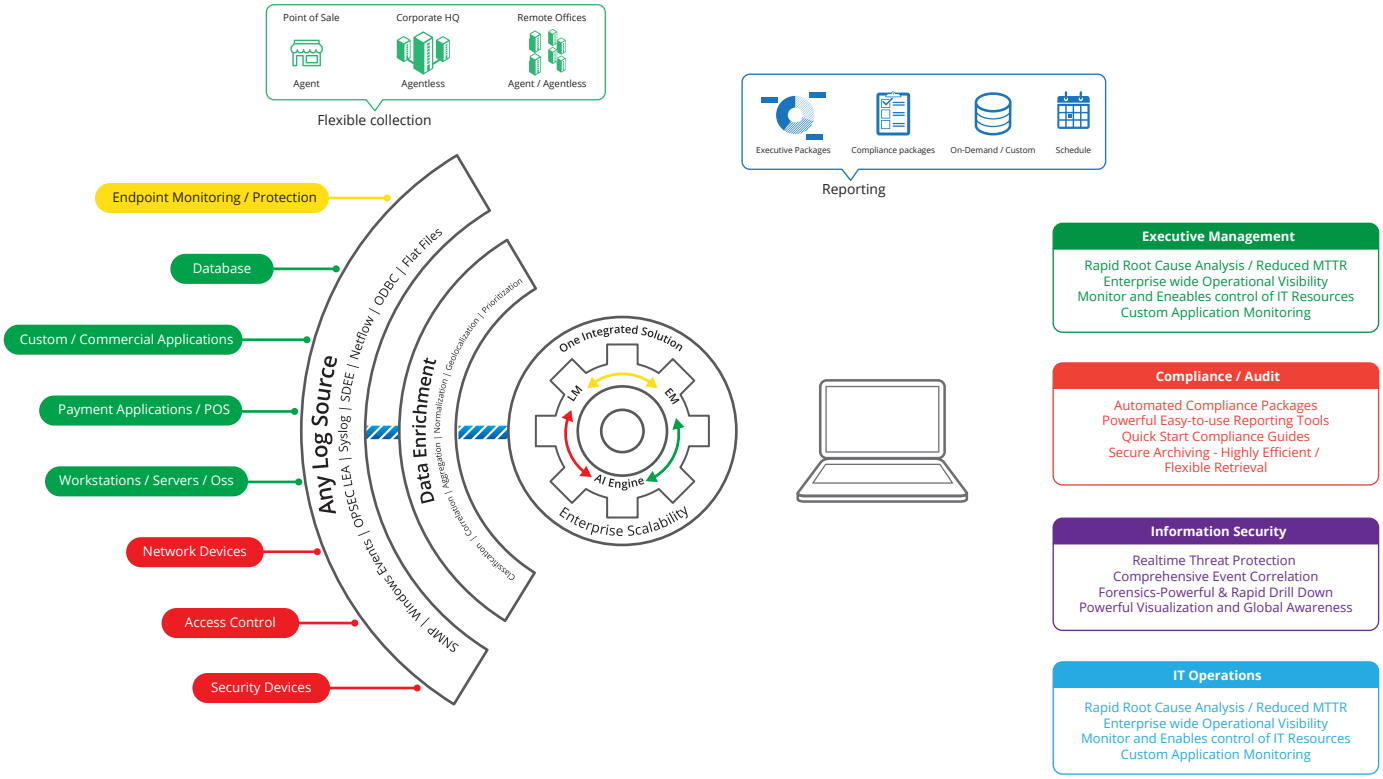
Back

Deployment:

- The Threat Manager Appliance (physical CL300 or virtual) is installed in the customer environment
- The appliance needs to have access to Switched Port Analyzer (SPAN) connections
- The data is collected and transmitted to Cautela Labs Cloud through secure SSL connections
- All threats are analyzed in real time and any suspicious signature or data patterns are analyzed by the Cautela Labs Enterprise Security Manager
- Any threats that require security analyst review are displayed on the console for further investigation
- Based on client escalation procedures, the response from the security operations center are directed accordingly
- The security analyst works with clients to remediate the threat 24x7

Cautela Labs **Threat Manager**

Cautela Labs Security Architecture



Appliance Configuration

Hardware	Configuration	Description
CPU	Intel Xeon	All Intel Xeon processors and above
Memory	4GB / 8GB DDR3	Minimum 4GB RAM and above
Hard Drive	250GB	Minimum 250GB and above with RAID 1
OS	Linux	Hardened Linux
Network	INTEL Pro/1000	Dual Port NIC, other options available
Power	Single Power	Dual Power option available
Chassis	1U	1U Chassis with 2/4 Post Rails included

Virtual Appliance

A virtual appliance can be installed on VMware, XEN Server or a KVM virtualized environment. Recommended configuration per instance: 4GB RAM, 2 Cores, 100-200GB Disk Space with NIC dedicated to the environment.