Cautela Labs

Cloud Agile. Secured.

Threat Management

Security Solutions at Work

Security concerns and dangers come both from internal means as well as external. In order to enhance your security posture work must be done to balance both the internal as well as external security threads to an organization. Cautela Labs addresses this concern by offering a cloud base vulnerability assessment and intrusion detection. With Cautela Labs Threat Management, you cost-effectively defend and protect your network against internal and external threats via Intrusion Detection Service (IDS)/ Intrusion Prevention Service (IPS), Host IDS/IPS, Firewall Management.

IDS/IPS Management

Network Intrusion Detection and Prevention (IDS/IPS) devices can provide a highly effective layer of security designed to protect critical assets from cyber threats. Organizations can detect attempts by attackers to compromise systems, applications and data by deploying network IDS. However, keeping the devices tuned and up-to-date so they are effective is a challenge for many organizations and requires specialized skills. The IDS/IPS devices are only effective if they are well tuned to the current threats and the network in which they are deployed. IDS devices can generate thousands of alerts each day and are very prone to false positives, making it difficult to identify true threats and take timely action to protect assets.

Cautela Labs Security Engineers monitor IDS and IPS to analyze events and identify threats. All event information is analyzed, including full packet payloads. Events are correlated across all available information sources, including other IDS and IPS devices, firewall logs, network devices, host and application logs, vulnerability scan results, and asset information. This intelligence is fed back into our services to enhance Managed Network IDS/IPS monitoring and response capabilities. When a customer is at risk, our security professionals respond to counter the threat.

Cautela Labs's Managed IDS/IPS service offers flexible support in the most complex environments, allowing our Cautela Labs to tailor services to each customer's individual needs. Appliances can be managed in a traditional managed services model, where customer personnel have limited or no administrative privileges for their IDS/IPS devices. Cautela Labs also supports a joint support model, with this approach, our experts alleviate the management, maintenance and monitoring burdens without the customer being locked out of their infrastructure.

Firewall Management

Firewall management is a challenging part of security operations because of the level of resource needed as well as expertise required. Devices must be provisioned, deployed, upgraded and patched to keep up with the latest threats. Security policies and configurations must be updated to ensure appropriate access controls are consistent with changing business environments. Network traffic must be monitored continuously to identify and respond to threats before damage is done. Cautela Labs Firewall Management service provides 24x7x365 firewall administration, log monitoring, and response to security and device health events.

Host IDS/IPS

The Cautela Labs Host IDS/IPS Service serves as an application firewall for your servers to ensure that an application is doing only what it is supposed to be doing. When encrypted traffic is received and decrypted by the operating system on the host machine, the agents intercepts instructions prior to reaching the application to prevent malicious activity. Your servers are even protected from new threats. Host agents are deployed on critical servers with customizable policies providing more precise control over access and usage. A host agent resides between the applications and the operating system, enabling maximum application visibility with minimal impact to the performance of the underlying operating systems. The software's architecture intercepts all operating system calls to file, network and registry sources as well as to dynamic run-time resources such as memory pages, shared library modules and COM objects.

THREAT MANAGER & ACTIVE WATCH FEATURES

Threat Signatures & Rules	• Rule Set Consolidated from Multiple Sources – Cautela Labs Security Research Team – Emerging Threats – Open Source, Third-Party Collaboration • Real-time Signature Updates to Cautela Labs Expert System • Custom Rule Creation and Editing	Integrated Managed Security Services	• GIAC-Certified Security Analysts and Researchers • 24x7 State-of-the-Art Security • Operations Center • Trained Experts in Cautela Labs Solutions • Monitoring, Analysis and Expert Guidance Capabilities • Customized Alerting and Escalation Procedures
Vulnerability Assessment & Intrusion Detection	• Unlimited Internal and External Scans • Broad Scanning and Detection Visibility – Network Infrastructure – Server Infrastructure – Business-Critical Applications – Web Technologies – SSL-Based Intrusion Traffic • Signature and Activity-Based Correlation • Patented 7-Factor Threat Scenario Modeling	Compliance Support	• PCI Approved Scanning Vendor (ASV) • PCI Level 2 Audited Vendor • Support for Multiple Compliance Mandates – PCI DSS 2.0, HIPAA, SOX, GLBA, CoBIT, etc • 6-Month Storage of All Raw IDS Event Data • SSAE 16 Type II Verified Data Centers • Indefinite Storage and Archival of Incident Analysis and Cases
Analysis & Reporting	• Dozens of Dashboards and Reports Available Out-of-the-Box • Custom Reporting Capabilities • Common Vulnerability Scoring System (CVSS) to Assess Risks • Audit-Ready Reports • Single Web-Based Console for Entire Environment – User Management and Administration – Dashboards and Drilldown Analysis – Report Scheduling, Creation and Review – Scan Scheduling and Results Review	Security-as-a- Service Delivery	• Rapidly Deploy and Scale as Needed • Pay-as-You-Go; Minimal Capital Expenditure • Always Utilize Latest Software and Signature Database • No Hidden Costs – Subscription Includes: – Software and Hardware Upgrades, Maintenance and Patches • Architected for Multi-Tenant Support • Easily Deploy in On-Premise, Off-Premise or Hybrid Environments
		Detailed Vulnerability Reports	• Detailed vulnerability and host reports are produced to provide detailed descriptions and lists of impacted hosts, risk levels and remediation tips.

The Cautela Labs Thread Management Services Benefits

- 24x7 security event and log monitoring and analysis.
- Real-time security event response to known and emerging threats.
- Customized escalation procedures.
- Log analysis and compliance reporting.
- Collection from multiple sources, including: network devices, security devices, servers, databases, applications, desktops, to name a few.
- Enables regulatory compliance with automated log data collection and due diligence review as well as immutable, redundant, and secure archival.
- Improves incident response and resolution for security, performance, and availability incidents via quick and easy browser-based access to all historical log data.
- Stores and archives data according to business and security data retention policies in our SSAE16 Type II audited, redundant data centers
- Easy to buy, deploy, use, and own with no software or hardware to purchase or maintain, no upfront investment required, everything included in one convenient monthly fee.

Cautela Labs, Inc.
5080 N. 40th Street, Suite 300
Phoenix, AZ 85018
Phone: 800-997-8132
Fax: 714-862-2177
Email: Support@Cautelalabs.com