INFOSIGHT SIEM

A BETTER WAY TO ADDRESS THREAT MANAGEMENT AND COMPLIANCE.

SECURITY INFORMATION AND EVENT MANAGEMENT - SIEM

Complete Visibility in a Fraction of the Time of Traditional SIEM

Improve how you manage cyber threats by unifying all of your essential security tools in one location and combine them with real-time threat intelligence. Utilizing a Unified Security Management (USM) platform accelerates and simplifies threat detection, incident response and compliance management for IT teams with limited resources, starting on Day One. With essential security controls and integrated threat intelligence built-in, the USM Appliance puts complete security visibility of threats affecting your network - and how to mitigate them – within fast and easy reach.

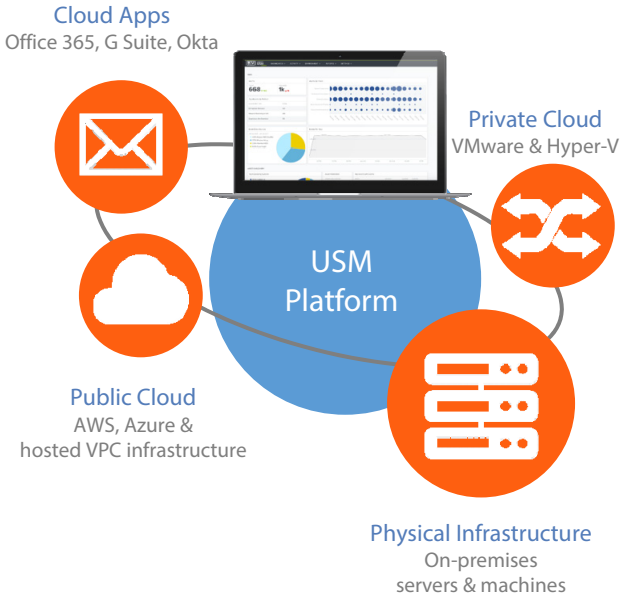
Whether large or small, all organizations need complete visibility to:

- Detect emerging threats across their environments on-premise and in the cloud
- Respond quickly to incidents and conduct thorough investigations to contain and mitigate threats
- Measure, manage, and report on compliance (PCI, HIPAA, FFIEC, etc.)
- Optimize existing security investments and reduce risk

USM Appliance delivers this complete security visibility by providing the five essential security capabilities in a unified platform, controlled by a single management console:

- **SIEM** – log management, event correlation, analysis, and reporting
- **Behavioral Monitoring** – netflow analysis, service availability monitoring
- **Intrusion Detection** – network and host IDS, file integrity monitoring
- **Vulnerability Assessment** – active network scanning, continuous vulnerability monitoring
- **Asset Discovery** – active and passive network discovery

Complete Threat Detection



Integrated Threat Intelligence

A Threat Intelligence subscription maximizes the effective of any security monitoring program by providing regularly updated correlation directives, intrusion detection signatures, response guidance, and much more. These constant updates enable the USM platform to analyze the mountain of event data from all of your data sources, and tell you exactly what are the most important threats facing your network right how, and what to do about them. Threat experts spend countless hours researching the latest exploits, malware strains, attack techniques, and malicious IPs, so you don't have to. We incorporate this expertise into our extensive and growing library of customizable correlation directives that ship with the USM platform, eliminating the need for you to conduct your own research and write your own correlation rules, giving you the ability to detect and respond to threats on day one.

In a partnership with the AlienVault Labs Security Research Team, we leverage the Open Threat Exchange™ (OTX™), the world's first truly open threat intelligence community that enables collaborative defense with open access to collaborative research on emerging threats. OTX integrates with USM Appliance and enables everyone in the OTX community to actively collaborate, strengthening their own defenses while helping others do the same.

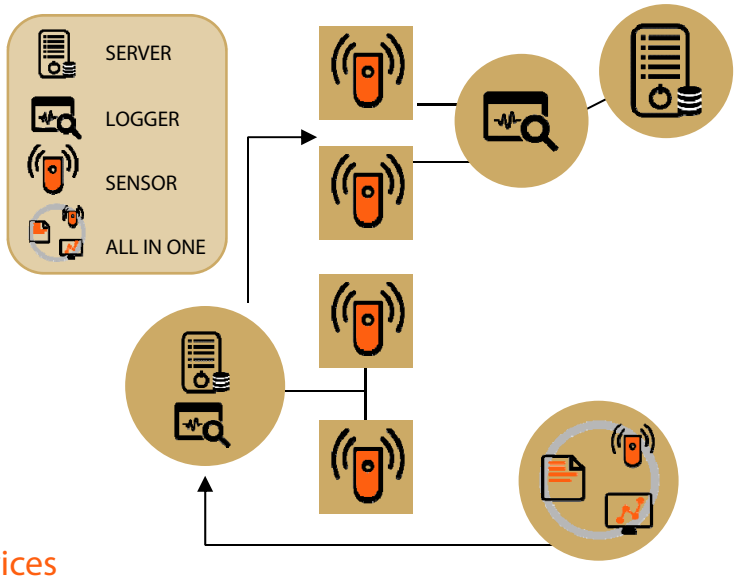
See how quickly you can detect, prioritize and respond to threats. To get started, call or email InfoSight® today.

Detect Threats Across All Your Environments

How it Works

All products include these three core components available as hardware or virtual appliances.

- **USM Appliance Sensor** – deployed throughout your network to collect logs to provide the five essential security capabilities you need for complete visibility.
- **USM Appliance Server** – aggregates and correlates information gathered by the Sensors, and provides single pane-of-glass management, reporting and administration.
- **USM Appliance Logger** – securely archives raw event log data for forensic investigations and compliance mandates.
- **USM Appliance All-in-One** – combines the Server, Sensor, and Logger components onto a single system.



Deployment Options and Professional Services

You can deploy the SIEM/USM in multiple configurations to meet your needs.

- InfoSight private cloud hosted for on-premise assets
- InfoSight Anywhere for both on-premise and cloud assets
- Traditional onsite

By bundling the SIEM/USM platform with InfoSight's professional services, you get 24x7 managed security services. With our **co-managed approach to security monitoring**, we work in collaboration with IT staff. We monitor the most critical devices that require 24x7 attention, and in-house IT staff monitor internal devices and endpoints.

Our MSSP services include:

- 24x7 monitoring & threat analysis
- Alerting and notification
- Reporting
- Incident response and mitigation
- Device management (FW, IPS, NIDS, HIDS, endpoint)
- Threat intelligence and tools

Predefined Event Reports

To give you insights into key events by different data source types and by specific solutions, the following is a sampling of predefined event reports.

EVENT REPORT BY TYPE OF DATA SOURCE		EVENT REPORT BY DATA SOURCE	
Anomaly Detection Events	Intrusion Prevention Events	NIDS	G Suite
Anti-virus Events	Load Balancer Events	AWS	McAfee ePO
Application Events	Mail Security Events	Amazon DynamoDB	Office 365
Application Firewall Events	Mail Server Events	Amazon S3	Okta
Authentication Events	Management Platform	AWS VPC Flow Logs	Palo Alto Networks
Cloud Application Events	Network Access Control	Azure	SonicWall
Endpoint Protection Events	Other Devices Events	Cylance	VMware

INFOSIGHT®
www.InfoSightInc.com