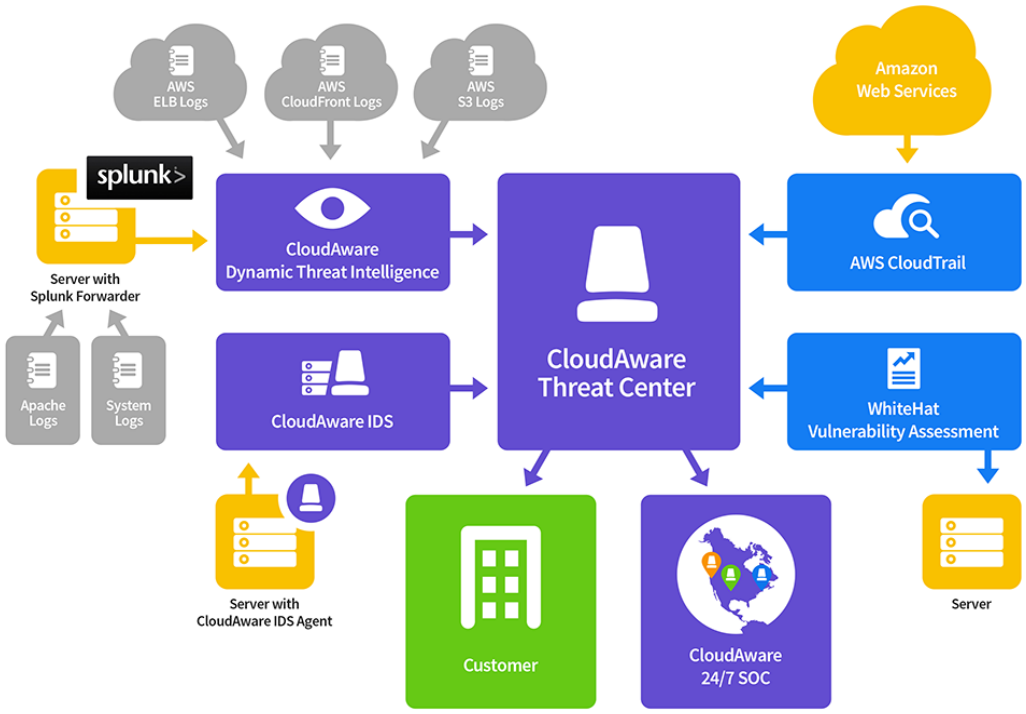
amazon web services | Partner Network
TECHNOLOGY PARTNER

Threat Center

Real-time multi-level threat detection, analysis, and automated remediation

Description

Advanced targeted and persistent threats can easily evade standard security, software vulnerabilities are rampant, insider threats are a constant, and now cloud computing and consumerization are opening the network even further to exploitation.



To minimize your exposure and risk of data breach, analysts recommend a proactive strategy using not only network and host analysis tools but also cloud change detection and management to continually monitor your network and logs for malicious activity.

Threat Center Key Features

Advanced Threat Deterrence and Detection Capabilities

- Inspect AWS Changes through the change detection layer with comprehensive vulnerability analysis
- Cloud Threat Intelligence, and continually updated threat detection rule sets
- Detect zero-day threats while minimizing false positives using multi-level correlation
- Detect malware command and control communication with web reputation
- Inspect AWS environment for unauthorized applications and malicious hosts
- Isolate suspicious endpoints pending mitigation

Automated Threat Remediation

- Performs real-time automated mitigation triggered by AWS Discovery Appliance
- Uses advanced forensic techniques to locate and eliminate malware without signatures
- Identifies and rolls back any system changes made by malware[1]
- Uses built in workflow engine to route violations and incident management

Threat Analysis and Reporting

- Provides end-to-end visibility of threat activity and status
- Offers automated drill down forensic analysis of non-compliant changes, behavior, communication, source, and channel of entry
- Delivers customizable event alarms
- Supports multi-level reporting for network managers and security executives

Risk Management Services Offerings

- Proactive monitoring and alerting
- Threat analysis and advisory
- Threat remediation assistance
- Risk posture review and analysis
- Strategic security planning

[1] Available with DevOps module only

Detect and Protect Against

- Non-compliant cloud changes
- Advanced Persistent Threats
- Targeted network exploits
- Web-based threats
  (web exploits, cross-site scripting)
- Sensitive data loss or transfer
- Bots, Trojans, and Worms
- Key Loggers and Crimeware
- Disruptive applications

Key Benefits

- Cloud Transparency and Control
- Real-time network-wide protection from advanced attacks
- Automated Threat Remediation
- Stop evasive intrusions without manual intervention and endpoint downtime
- Threat Behavior Analysis
- Forensic analysis provides insight needed to optimize risk posture
- Reduced Cost & Complexity

Host-Based IDS

CloudAware Threat Center includes host-based intrusion detection. Cloudasware IDS is a full platform to monitor and control systems. It mixes together all the aspects of HIDS (host-based intrusion detection), log monitoring and SIM/SIEM together in a simple, powerful solution.

IDS Features and Benefits

- File Integrity Checking
- Log monitoring
- Rootkit and Malware Detection
- Detect unmonitored servers
- Trending attacks and hosts
- Geo-IP Enabled
- Custom Policy
- Integrated Incident Management

amazon web services | Partner Network
TECHNOLOGY PARTNER

Compliance Requirements

Cloudaware IDS helps customers meet specific compliance requirements such as PCI, HIPAA etc. It lets customers detect and alert on unauthorized file system modifications and malicious behavior embedded in the log files of COTS products as well as custom applications. For PCI, it covers the sections of file integrity monitoring (PCI 11.5, 10.5), log inspection and monitoring (section 10) and policy enforcement/checking.

Multi Platform

Cloudaware IDS lets customers implement a comprehensive host based intrusion detection system with fine grained application/server specific policies across multiple platforms such as Linux, Solaris, AIX, HP-UX, BSD, Windows, Mac and Vmware ESX.

Real-time and Configurable Alerts

Cloudaware IDS lets customers configure incidents they want to be alerted on which lets them focus on raising the priority of critical incidents over the regular noise on any system. Integration with smtp, sms and syslog allows customers to be on top of alerts by sending these on to e-mail and handheld devices such as cell phones and pagers. Active response options to block an attack immediately is also available.

Integration with Current Infrastructure

Cloudaware IDS will integrate with current investments from customers such as SIM/SEM (Security Incident Management/Security Events Management) products for centralized reporting and correlation of events.

Centralized Management

Cloudaware IDS provides a simplified centralized management server to manage policies across multiple operating systems. Additionally, it also lets customers define server specific overrides for finer grained policies.

Agent and Agentless Monitoring

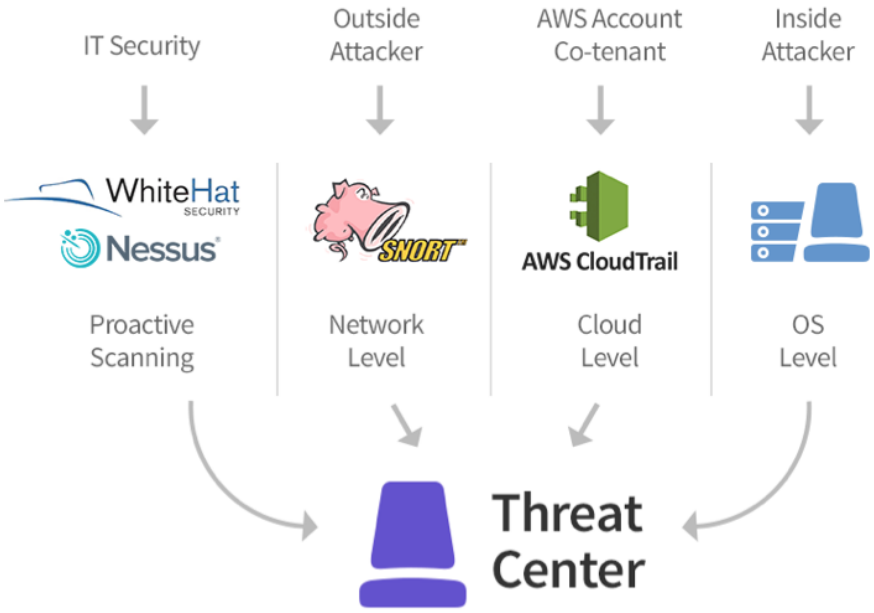
Cloudaware IDS offers the flexibility of agent based and agentless monitoring of systems and networking components such as routers and firewalls. It lets customers who have restrictions on software being installed on systems (such as FDA approved systems or appliances) meet security and compliance needs.

amazon web services | Partner Network
TECHNOLOGY PARTNER

Features

Multilevel Threat Management

CloudAware Threat Center continuously processes security events from multiple sources. Events are correlated across inputs by source IP address, vulnerability type, username and host of other common attributes. Threat center detects coordinated attacks and suspicious activity regardless whether it is coming from inside or outside.



Cloud Change Detection and Risk Assessment	Network Visibility and Control	System Level Protection	Pro-active Vulnerability Assessment
Detect Non-Compliant changes in AWS that pose security risk.	**Integrate with Snort to provide real-time visibility and insight.**	**PCI and HIPAA endpoint protection**	**Automated risk assessment and handling based on scan results.**
• Identify security changes that weaken security posture • Generate cloud change audit-feed • Mitigate AWS weak access control model	• Signature, protocol, and anomaly based inspection • Buffer overflows, CGI attacks, SMB probes • Real-time alerts and IPS	• File integrity checking • Log monitoring • Rootkit and malware detection • Covers PCI DSS 11.5 and 10.5.5	• Proactive vulnerability discovery • Identify un-scanned assets • Workflows for handling new vulnerabilities and resolutions

amazon web services | Partner Network
TECHNOLOGY PARTNER

Traditional Risks

- Advanced Persistent Threats
- Targeted network exploits
- Web-based threats
  (web exploits, cross-site scripting)
- Email-based threats
  (phishing, spear-phishing)
- Sensitive data loss or transfer
- Bots, Trojans, and Worms
- Key Loggers and Crimeware

Cloud Specific Risks

- AWS API and Console privileged access
- Rogue hosts (unauthorized AMIs)
- Hosts running outside of secure perimeter (VPC)
- AWS best practice compliance
- Sensitive data stored on AWS instances
- Non-Compliant cloud changes
- Inability to detect changes
- Data location
- Data segregation
- Insecure or incomplete data deletion

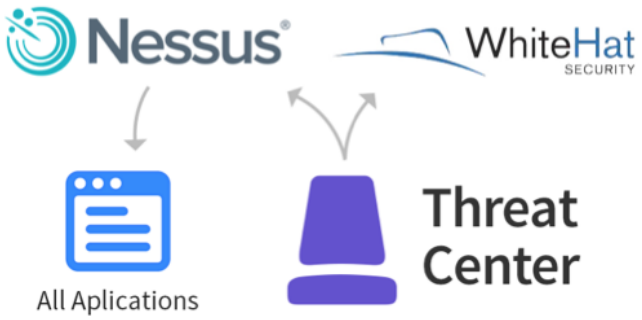
CMDB Integration

Any IDS will show you what hosts it is scanning, but CloudAware Threat Center can actually show you which hosts have not been scanned or are not running IDS agents. This information is available to CloudAware via its highly integrated CMDB module. CMDB contains information not only about what is installed and running on machines but also information about relationships between instances and applications. Threat center uses this relationship data to quickly map emerging threats against applications and environments.

amazon web services | Partner Network
TECHNOLOGY PARTNER

Automated Scan Initiation

CloudAware has API integration with WhiteHat security and Tenable. Either on-demand or automatically when certain conditions have been met, CloudAware can request either provider to scan the application. For example if new application is launched in production, CloudAware user can configure an automatic workflow to kick off a WhiteHat scan as soon as the application is up and running.



Rapid Deployment

Using CloudAware deployment orchestration module, you can deploy IDS agents to 1000s of servers in a single day. CloudAware supports technologies such as Puppet, Chef and Ansible and provides modules for its IDS agents for all of these configuration management tools.

Deployment Orchestration

amazon web services | Partner Network
TECHNOLOGY PARTNER

Continuous Monitoring With 24x7 Security Operations Center

With a focus on managed security services (MSS) and cloud threat intelligence, Cloudaware SOC protects traditional and cloud environments. Clients are able to optimize security programs, make informed decisions, achieve compliance and reduce costs.

Built on the patented, cloud-based MultiThreat® service platform, global threat intelligence from the Security Engineering Research Team (SERT) and certified AWS Engineers, CloudAware services are delivered 24/7 through multiple state-of the art security operations centers (SOCs)

Five Problems We Solve

1. Inability to correlate inside and outside attacks.	**2.** Not knowing where gaps in security are.	**3.** End-to-end threat visibility and status	**4.** Detecting new cloud-level attacks.	**5.** Taking too long to deploy IDS across the board.