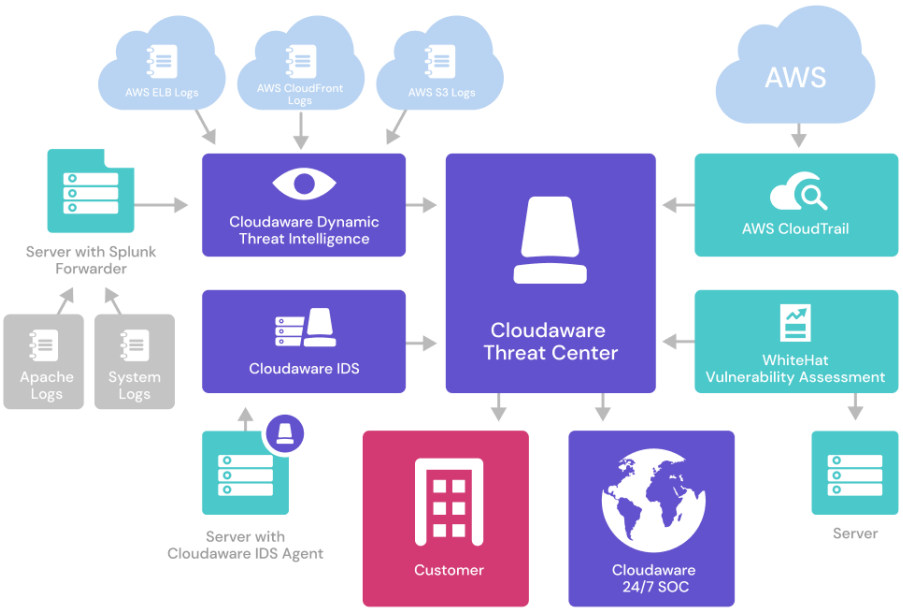
cloudaware

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.

cloudaware.com
info@cloudaware.com
+1 (888) 997 3550
1350 Avenue of the Americas,
2nd Floor, New York, NY 10019

cloudaware

Threat Center Key Features

Advanced Threat Deterrence and Detection Capabilities

- Inspect cloud 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 cloud environment for unauthorized applications and malicious hosts
- Isolate suspicious endpoints pending mitigation

Automated Threat Remediation

- Performs real-time automated mitigation triggered by e.g. 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 the 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

cloudaware

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
- Keyloggers 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 insights needed to optimize risk posture
- Reduced cost and complexity

Host-Based IDS

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

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- or 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 are 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 the software being installed on systems, such as FDA-approved systems or appliances, meet security and compliance needs.

cloudaware

Features

Multi-Level 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 a host of other common attributes. Threat Center detects coordinated attacks and suspicious activity regardless of whether it is coming from inside or outside.

Cloud Change Detection and Risk Assessment	Network Visibility and Control	System Level Protection	Proactive Vulnerability Assessment
Detect Non-Compliant changes in cloud that pose security risk	**Integrate with Snort to provide real-time visibility and insights**	**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 cloud 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 unscanned assets • Workflows for handling new vulnerabilities and resolutions

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
- Keyloggers and crimeware

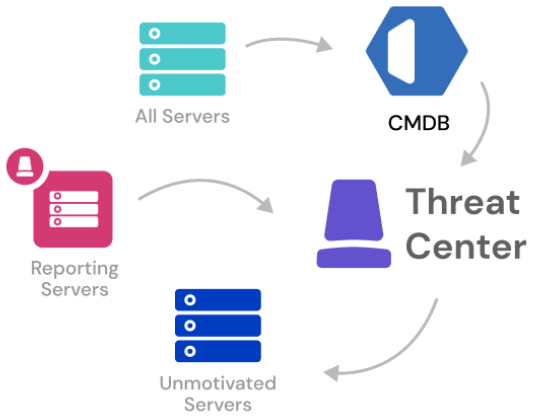
Cloud-Specific Risks

- API and cloud console privileged access
- Rogue hosts (unauthorized AMIs)
- Hosts running outside of secure perimeter, e.g. AWS VPC
- Best practice compliance
- Sensitive data stored on cloud 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 is running on machines but also about relationships between instances and applications. Threat Center uses this data to quickly map emerging threats against applications and environments.



Automated Scan Initiation

Cloudaware has an 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 applications. For example, if a 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

cloudaware

Using the Cloudaware deployment orchestration module, you can deploy IDS agents to thousands 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

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 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.

cloudaware.com
info@cloudaware.com
+1 (888) 997 3550
1350 Avenue of the Americas,
2nd Floor, New York, NY 10019