ENCLAVE FEATURES

Host-based Intrusion Detection (HIDS) and Incident Response

Your cloud infrastructure is protected at the host level with both intrusion detection monitoring and incident response. The Aptible Security Team investigates, responds to, and resolves any security incidents that are discovered via the HIDS.

How Enclave Host-based Intrusion Detection Works

Event Collection & Monitoring

Security events are collected using OSSEC, a leading open source intrusion detection system. The Aptible Security Team monitors these events.

ISO 27001 Certified Investigation & Response Process

The Aptible Security Team actively reviews each security event using our ISO 27001 certified security review process. The Security Team classifies each as either legitimate or indicative of potential attack.

ISO **Learn more about Aptible's ISO 27001 certified Incident Response Process**

Enclave Security Team Resolution

The Aptible Security Team immediately resolves any underlying issues related to detected anomalous activity on your behalf and notifies you of the actions taken.

The Enclave HIDS Compliance Report

Provide your customers and auditors with evidence that your host-based intrusion detection system is monitoring activity and potential threats are resolved.

Subscribe to the available Enclave HIDS Compliance Report, containing a digest of security events and Aptible Security Team review and remediation activities. This report satisfies compliance requirements related to HIDS.

DOWNLOAD SAMPLE REPORT

The Aptible Security Team Monitors, Investigates, Responds to, and Resolves Security Events

Your host-based intrusion detection system (HIDS) is an important tool to manage your stack's security.

Your infrastructure generates a constant stream of events relevant to the security of your data. Aptible Enclave® HIDS is installed on each host that runs your containers by default and will detect potential intrusions and other anomalous activities.

The Aptible Security Team monitors and investigates each event to determine the legitimacy of all activity. Crucially, the Aptible Security Team immediately responds to and resolves any issues that are discovered through investigation of anomalous activity and will notify you of any remediation steps taken.

You can optionally subscribe to the Enclave HIDS Compliance Report to provide your customers and auditors evidence that you are using HIDS to monitor, analyze, and remediate security events.

List of Security Events Collected

- File integrity change
- Rootkit check
- Malware scanning
- System integrity check
- Privilege escalation
- SSH login
- User or group modification

ENCLAVE AUTOMATES SECURITY CONTROLS

Deploy Your First App Now

Enclave empowers you to deploy and scale Dockerized apps and databases–all without speaking to sales or support

Enter your email SIGN UP

Deploy your app ● **$500 free credit** ● **Pay as you go** ● or **Request a Demo**

Other Enclave Security Controls

Meet regulatory compliance and customer audit requirements–automatically–as you deploy and scale

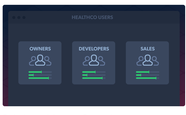
Data Encryption

Enclave provides everything you need to meet encryption requirements. Databases are encrypted at rest using AES-256 and eCryptfs. App and database traffic is encrypted in transit using SSL/TLS.

Enclave handles SSL/TLS termination on your behalf and, optionally, provisions and renews certificates using Let's Encrypt.

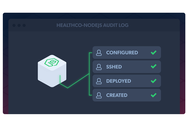
Business Continuity Procedures

Your data is backed up automatically every 24 hours and whenever you trigger a manual backup. Restoring your data from a backup is simple.



Role-based Access Controls

Define as many roles as needed to ensure logical separation of apps, databases, and environments across functions and teams. Additional roles and environments are free.

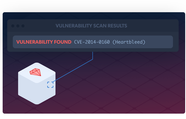


Audit Reports for Every Operation and Resource

Every deploy, config change, database tunnel, and console operation and session can be traced back to an individual user.

Log Collection and Backup

Route your logs in one click. Deliver logs to integration partners including Papertrail and Logentries, or send them to a self-hosted ELK stack. If things go wrong, Enclave has your back with an archived cold copy of your logs.



Vulnerability Scanning

Vulnerability scanning is enabled by default on all your containers, with automated scanning and real-time notifications via integration with Appcanary.

1644 Platte St, Denver, CO 80202
(866) 296-5003