CryptoAuditor®

Monitor and Control Privileged Access to Encrypted Data

You depend on your firewall to protect your company, yet there is a gap in its security: it does not monitor or inspect privileged access in encrypted channels.

CryptoAuditor does. It reinforces firewall defenses with comprehensive privileged-user access control and data security for SSH environments.

CryptoAuditor is a network-based, inline traffic inspector that provides a trusted audit point to examine and manage privileged user sessions. It terminates and re-opens each session, inspecting and recording the activity of privileged users. Then it re-encrypts the session and moves it forward.

Running CryptoAuditor concurrently with your existing firewall lets you find and respond **in real time** to potential threats in SSH, SFTP, and RDP sessions.

Using your existing firewall rules, CryptoAuditor monitors and audits protocol-specific traffic from any port, regardless of the user's device or data destination and without disrupting workflow or network architecture.

Based on user identity, CryptoAuditor controls where the user is allowed on the network and which activities are permitted. Security personnel can view user sessions in real time and replay video of activity.

When integrated with an existing ICAP-supporting solution such as DLP, IPS, or SIEM, malicious data can be found before it enters the environment and sensitive data can be prevented from leaving. CryptoAuditor also easily enables two-factor authentication to protect critical data.

Boost Your Firewall Defenses

Real-time intelligence, complete forensics,
and proactive data loss prevention.

CONTROL

Define privileged access based on user identity.

REAL-TIME DEFENSE

Enable DLP, IDS, and SIEM to investigate encrypted sessions.

ACCOUNTABILITY

Trace privileged users' access and activities: who, where, what.

AUDITING

Retain encrypted database of activity history including video of graphical sessions.

REPORTING

Real-time indexing of data and graphical sessions for content searches.

EASY DEPLOYMENT

No agents to deploy; efficient, low-cost installation on distributed architecture.

SDS
DO MORE WITH LESS

CryptoAuditor solves an array of security challenges in traditional and cloud data environments.

Virtual appliances are deployed at key locations in the network, such as in front of server farms, databases, network entry points or in outgoing data gateways. Sessions are indexed and stored in an encrypted database for reporting, review, and forensic investigation.

The software is run from a centralized console to increase efficiency and oversight. It can be run in a fully transparent mode so that login procedures and user access remain unchanged.

Who Uses CryptoAuditor?

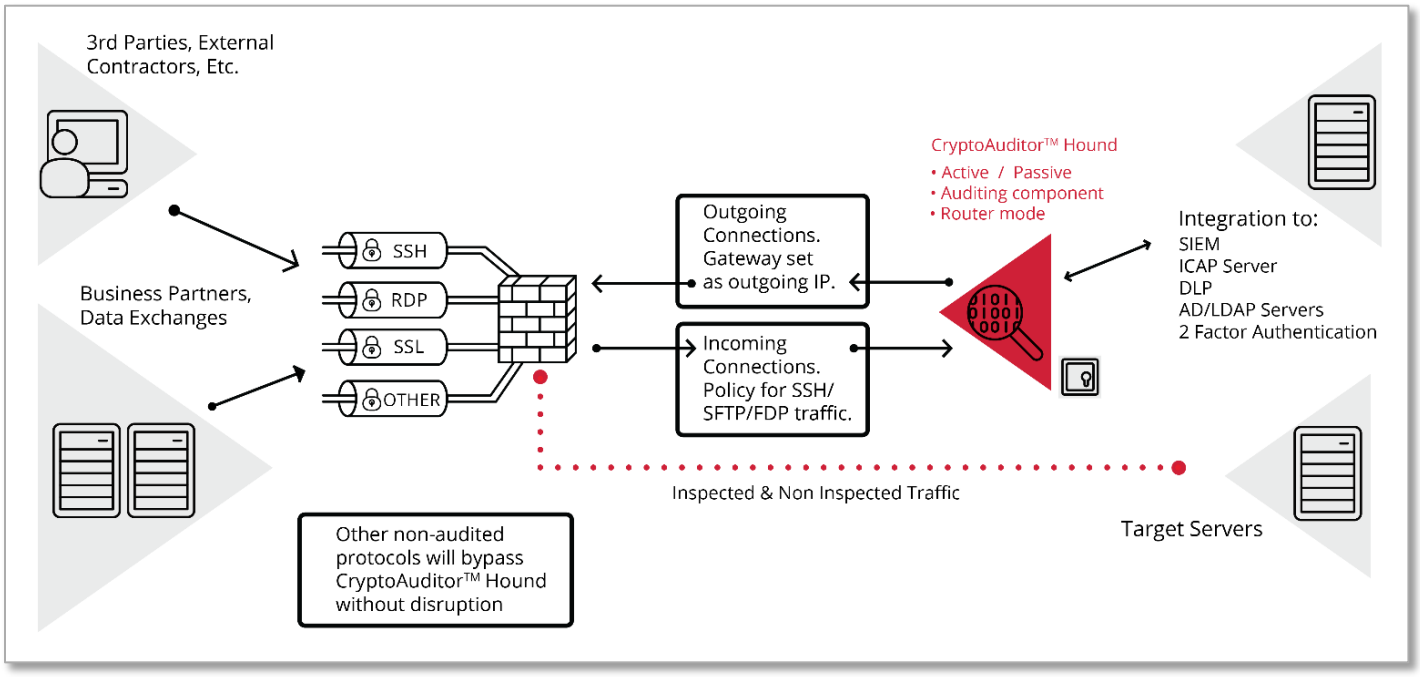
Cloud and Hosting Provider
Improves operation efficiency; meets security SLAs that customers demand.

Technology Company
Prevents contractors from removing source code and designs.

Global Financial Services
Protects multi-trillion-dollar financial settlement services.

Gaming Operator
Monitors Windows and Unix administrators.

Firewall-Based Policy / Application Routing



About SDS

Founded in 1982, SDS supports over 25 products for z/OS, MVS, VSE, VM, AIX, Linux, and Windows. SDS has licensed more than 1,000 enterprise clients worldwide with quality mainframe software and offers award-winning technical support. Comprehensive solutions focus on security, encryption, data compression, and network monitoring. To learn more, please visit our web site.