

Don't Let a Trusted Insider Become an Exploit

As the inventors of the SSH protocol, SSH Communications Security is focused on helping organizations secure their information assets. CryptoAuditor is a network based monitor that records and controls the activities of privileged users. It reduces the risk of data breaches and enables compliance.

The Problem

Privileged users such as system and application administrators have broad access to critical business information and systems. These trusted insiders often have more access to sensitive information than even C-level executives. While the vast majority of trusted insiders are trustworthy, just one bad actor can cause irreparable damage. Furthermore, malware that makes its way into the enterprise will leverage insider privileges in order to steal vital information.

In most enterprises, confidentiality and integrity of privileged access is ensured by the Secure Shell protocol (SSH), Remote Desktop Protocol (RDP) and Secure Sockets Layer/Transport Layer Security (SSL/TLS). While these protocols protect privileged sessions from eavesdropping, the activities of privileged users are rarely monitored or controlled. This exposes your organization to data breaches, denial of service and compliance failures.

The Solution

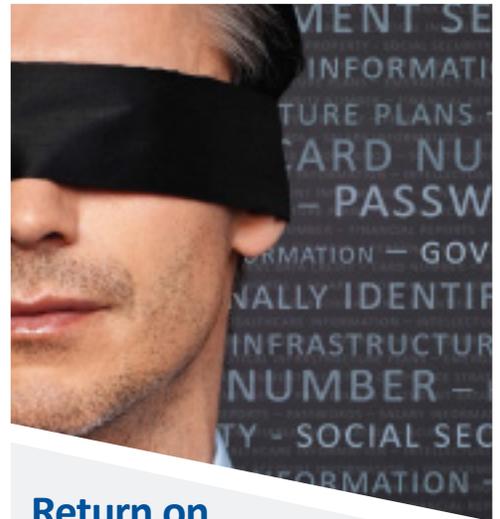
CryptoAuditor is a network based, inline traffic monitor that records the activities of privileged users without interfering with their normal workflow. There are no agents to deploy and it works with all types of end points. Text based and graphical sessions are recorded and indexed into the CryptoAuditor database. You can easily find and investigate sessions of interest with search and video replays.

CryptoAuditor is more than just a passive monitor. It provides identity based policy controls so you can control where privileged users can go in your network and what they can do. It also works with your layered defenses. CryptoAuditor sends session traffic to your DLP, IDS and SIEM systems enabling real time detection and prevention of data loss.

How It Works

CryptoAuditor works as a man-in-the-middle. It decrypts, inspects, records and re-encrypts privileged user sessions in real time. The system consists of central Vault and one or more Hound appliances. Hounds capture the traffic and enforce auditing policies. They are deployed at key locations in the network - in front of server farms, databases and network entry points. They can be deployed in a fully transparent mode so you don't need to change end user access and login procedures. A centralized Vault provides unified system management and all captured sessions are indexed and stored in its encrypted database.

Encrypted Channel Monitoring

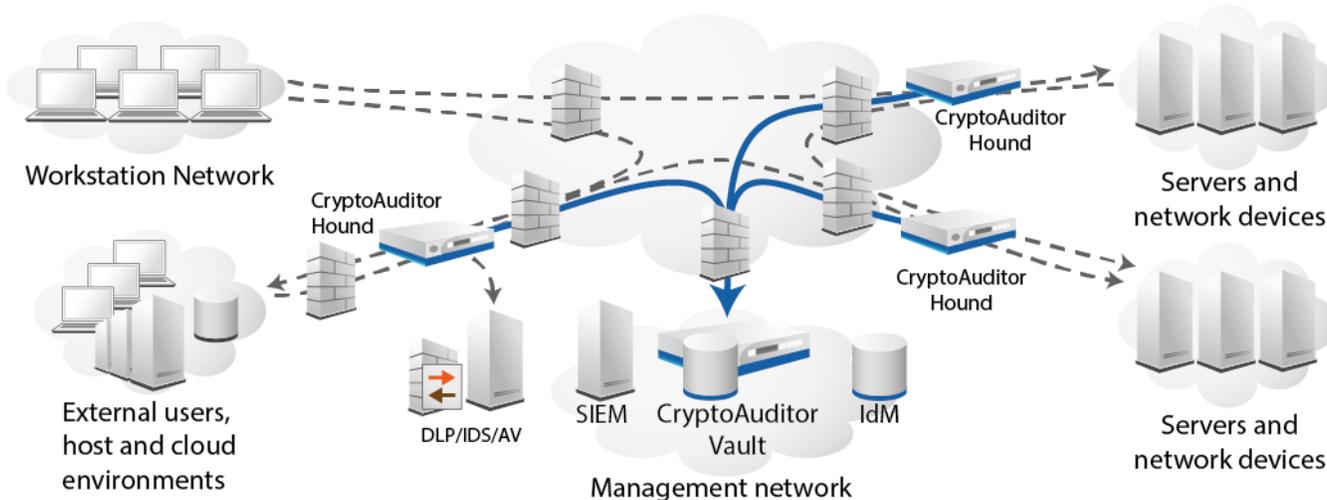


Return on Investment

Reduce the Risks from Trusted Insiders: CryptoAuditor delivers immediate control and accountability over your privileged access users, closing a significant security gap in your information security architecture.

Transparent Footprint: With its minimally invasive approach, CryptoAuditor captures a broad array of traffic across all of your needed audit points while remaining transparent to administrators.

Easily Deployed in Your Existing Architecture: CryptoAuditor is designed to easily deploy across your distributed architecture and makes management easy through a one-console approach.



Popular Use Cases

- You want to prevent users from leveraging SSH to create tunnels for other applications.
- You want to prevent contractors from removing files containing intellectual property.
- You have a jump host or proxy solution in place, but need better control over what hosts the users can get to without changing their login procedures.
- You want administrators to login using their personal credentials to systems provisioned with a common, shared credential.
- You want to record the activities of the privileged insiders who administer Windows servers, UNIX servers and network devices.
- You want to block outgoing encrypted file transfers if they contain credit card numbers.

Features	Benefits
Multiple deployment modes: Bridge, Router, Bastion	Fits into diverse network topologies including VLAN based audit and policy control
Hardware and Software bypass	In the event of device failure traffic will continue to pass through.
Transparent “man-in-the-middle”	No need to retrain users or provide them with new SSH keys.
Session replay, including video sessions	Straightforward audit of privileged activity
Searchable database	Quick and easy access to recorded session information.
Encrypted storage with audit zones	Audited activity is secured from unauthorized access. Separate audit zones enable access on a need to know basis.
Monitors and records SSH, SFTP, RDP, SSL/TLS	Audit high value, privileged access. Comply with security mandates.
Customizable monitoring recording	Focus on high value targets, activities.
Identity based policy control with integration to directory services.	Control which users can access which servers and what activities they can perform
Integrates with SIEM, IPS, DLP, Network AV. Supports ICAP.	Leverage existing security infrastructure.

Hardware Appliance Specifications

Platform	HP ProLiant DL 320 Gen8
Dimensions	1U rack-mountable, 4.32 x 43.46 x 75 cm (1.7 x 17.11 x 29.5 in); Large Form Factor
Weight	13.5 kg (29.76 lb)
Electrical	100 - 240 V AC ; 3 A (at 200 V AC) to 6A (at 100 V AC); Idle 115 W, 100% utilization 174 W (230 V supply voltage)
Network Interfaces	4 x RJ45 GbE
Storage	Default: 2 x 1 TB in RAID1, Extended: 4 x 3 TB in RAID1
Throughput	930 Mbit/s (unaudited SFTP); 400 Mbit/s for single encrypted SFTP connection
High Availability	Active-Passive redundancy (Hound)
Simultaneous Connections	3000 SSH, 300 RDP

Virtual Appliance Specifications

Supported Platforms	VMware ESX/ESXi 5.0 or later
---------------------	------------------------------

Software Specifications

Inspected Protocols	SSH, SCP, SFTP, RDP, SSL/TLS protected TCP
Version Support	SSHv2, RDPv5
Management Interface	Web based admin UI (Mozilla Firefox 28.0 or higher), CLI
Administration	On device or AD/LDAP based password authentication, Customizable role based administration
Alerts	Email, remote syslog, SIEM
Security Features	All communication between Hound and Vault secured by TLS. All information stored in Vault encrypted with 128-bit AES. No user passwords captured and stored.
Monitoring Control	By source or destination address range, by protocol, by port, by user, by VLAN
End User Authentication & Authorization	On device, AD/LDAP, RADIUS. Password, SecurID/OTP, Certificate, SSH Key. HTTP REST API support for authorization.
Audit Levels & Policy Control	Metadata only, full audit. Notify only, deny action, deny session.
Encryption Support	Key exchange: Diffie-Hellman, RSA Host Key: RSA, DSS Connection: AES-CTR/CBC (128-, 192-, 256-bit), 3DES-CBC, Blowfish, RC4
Data Integrity	HMAC SHA-1 (160-bit, 96-bit), HMAC MD5 (128-bit, 96-bit)

Copyright ©2014, SSH Communications Security, Inc. All specifications are subject to change without notice. SSH Communications Security Inc. assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. SSH Communications Security Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice. SSH 05082014