ssh communications security

DATA SHEET

CRYPTOAUDITOR: Extend the Reach of Your Firewall

Don't be blinded by encryption. Make the unseen visible.

Monitor, audit and control encrypted privileged access as a simple extension to your advanced firewall without disrupting existing process flows or network topology.

Regardless of whether you are monitoring privileged remote access or want to inspect incoming file transfers, running CryptoAuditor in tandem with your firewall will let you gain real-time intelligence to potential threats and immediate response capabilities with your SSH, SFTP, and RDP encrypted traffic.

The security intelligence gap in encrypted channels is a challenge most organizations are aware of but have not been able to get a handle on.

Real-time intelligence, proactive data loss prevention and forensics have been enabled throughout the estate but visibility and control of the encrypted privileged access and file transfers running through SSH, SFTP and RDP remains elusive.

CryptoAuditor can now take a feed from your advanced firewall with policy or application based routing, so that all protocol specific traffic regardless of the port can be filtered through CryptoAuditor and inspected before being sent to the destination server, all simply based on firewall rules. This will now permit your firewall to be able to look into encrypted sessions over SSH, SFTP, and RDP. When integrated with an existing ICAP supporting solutions, such as DLP, IPS, and/or Anti-virus solution you now have the possibility to inspect for malicious data entering the environment and sensitive data leaving. In tandem with your advanced firewall it is now easy to enable two-factor authentication for your organization, and give security engineers the ability to view user sessions in real time with a full video replay available for download.

THE SOLUTION

CryptoAuditor is a network-based, inline traffic monitor that decrypts and records the activities of privileged users without interfering with their normal workflow. There are no agents to deploy; it works regardless of what devices users connect with and what they connect to.

CryptoAuditor is more than a passive monitor; it provides identity-based policy controls that specify where privileged users can go in your network and what they can do. CryptoAuditor also integrates with your DLP, IPS and SIEM systems, enabling real-time detection and prevention of data loss. Here is how CryptoAuditor protects your critical assets:

- **Accountability:** You know exactly who the users are and what they did.
- **Control:** Privileged access on a "need to know, need to do" basis.
- **Audit:** Encrypted database of privileged audit trails, including video replay of graphical sessions.
- **Reporting:** Real-time indexing of sessions for content-based searches, and reportings, also for graphical sessions.
- **Real-time defense:** Your SIEM, DLP and IDS gain real-time visibility into encrypted sessions.
- **Easy deployment:** Transparency and distributed architecture enable efficient, low-cost deployment.

awsmarketplace

Certified for Amazon Web Services Marketplace and available for 1-click deployment

McAfee COMPATIBLE

Certified integration with McAfee WebGateway for powerful DLP and McAfee ESM enterprise-grade incident management

TECHNOLOGY RSA READY PARTNER

Ceritified integration with RSA Security Analytics for powerful enterprise-grade incident management

VBLOCK READY

Certified to work with VCE Vblock System converged infrastructure

Business Partner IBM Ready for Security Intelligence

Certified integration with IBM QRadar SIEM for improved enterprise incident management

CRYPTOAUDITOR: Extend the Reach of Your Firewall

HOW IT WORKS

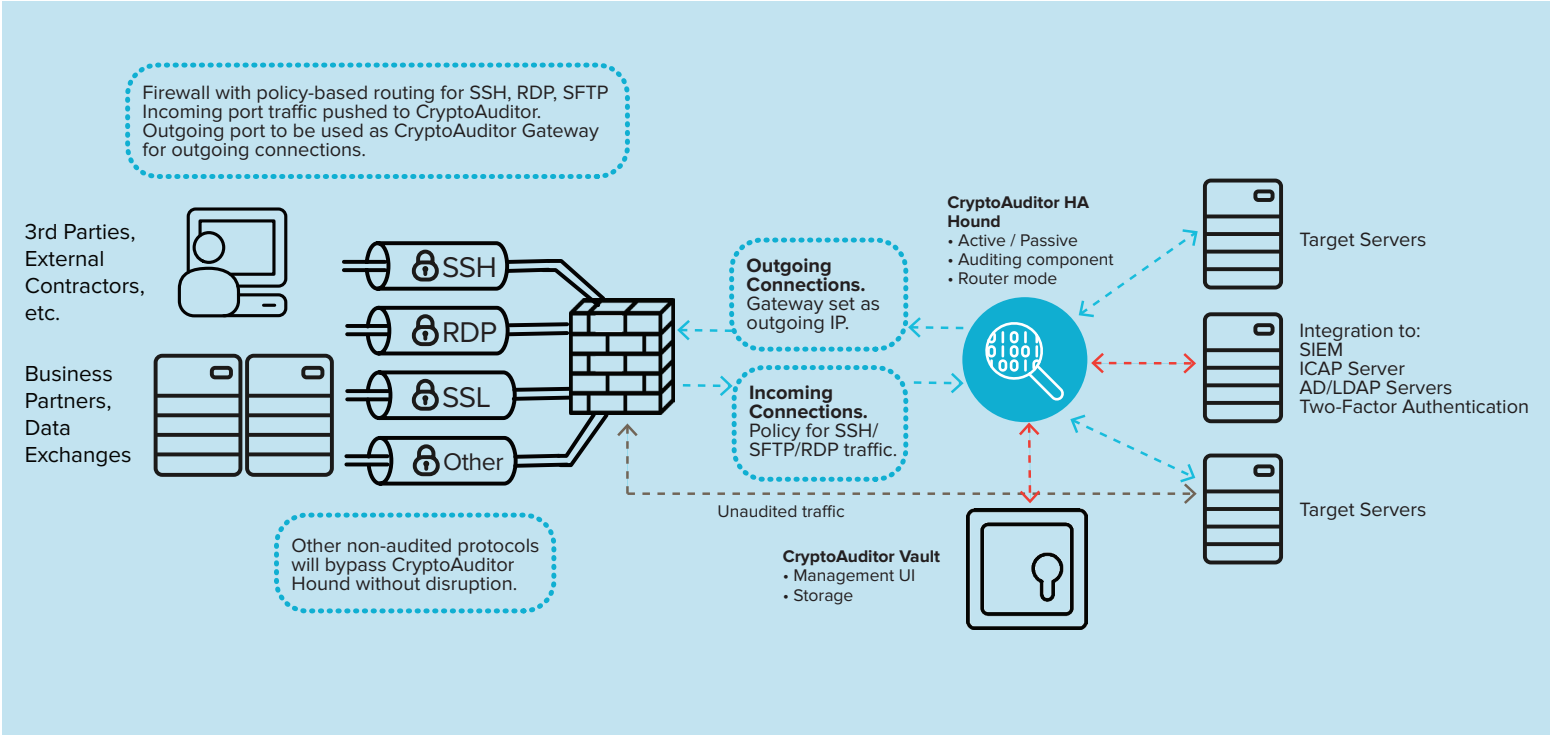
CryptoAuditor works as a trusted audit point. It terminates and re-opens privileged user sessions, and inspects and records those sessions in real time before re-encrypting and pushing the session forward. Virtual appliances are deployed at key locations in the network - in front of server farms, databases, network entry points, or for example, in outgoing data gateways. It can be deployed in a fully transparent mode so you don't need to change end-user access and login procedures. A centralized console provides unified management. Sessions are indexed and stored in an encrypted database for reporting, replay and forensic investigation.

SOME OF OUR CUSTOMERS

CryptoAuditor solves diverse security challenges in the cloud and traditional data centers:

- **Cloud and Hosting Provider:** Improves operational efficiency and meets the security SLAs customers demand.
- **Global Financial Services:** Protects multi-trillion dollar financial settlement services.
- **Gaming Operator:** Monitors Windows and Unix administrators.
- **Technology Company:** Prevents contractors from removing source code and designs.

Firewall-Based Policy / Application Routing



TECHNICAL SPECIFICATIONS

FEATURES AND BENEFITS

Features	Benefits
Multiple deployment modes: Bridge, Router, Bastion	Fits into diverse network topologies including VLAN-based audit and policy control.
High-availability clustering for Hounds, and configurable failure-tolerance policy	Minimal downtime in event of a single Hound node failure. If a single Hound node fails, the system can recover and continue relaying new connections.
Transparent network appliance	No need to retrain users to have them use another SSH client or portal, 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, HTTPS	Audit high value, privileged access. Comply with security mandates.
Customizable auditing policies	Focus on high value targets, activities.
Real-time 4-eyes authorization. HTTP REST API for requesting connection authorization from third-party solutions.	Extra security layer for accessing critical servers.
Identity-based policy control with integration to directory services	Control which users can access which servers and what activities they can perform.
Distributed architecture with multiple freely-distributable Hound audit-points, and shared Vault storage.	Adapts easily to changes in network topologies and business processes, enabling fast deployment and low Total Cost of Ownership.
Integrates with SIEM, IDS, DLP, Network AV	Certified compatibility with major vendors such as McAfee, RSA, IBM and VCE vBlock.

Public and Private Cloud Instance	Virtual Appliance
• Amazon Machine Image (AMI) available in AWS Marketplace • OpenStack (on KVM hypervisor)	• Supported platforms: VMware ESXi and MS Hyper-V • For evaluation purposes Oracle VirtualBox and VMware Workstation (no production use support)

PERFORMANCE

Throughput	• 930 Mbit/s (unaudited passthrough) • 400 Mbit/s (single encrypted SFTP connection)
Connections	• Simultaneous connections: 3000 SSH or 300 RDP or 300 SSL/TLS • New connections per second: 3 SSH or 3 RDP or 10 SSL/TLS

* Setup used in the performance test: HP DL320e Gen8 server running VMware ESXi 5.5, CryptoAuditor VM (4 CPUs, 12 GB RAM)

DEPLOYMENT AND SYSTEM ADMINISTRATION

High Availability	• Active-Passive redundancy (Hound) * VMware (and hardware appliance) in production use
Operation	• Transparent bridge and router modes • Non-transparent bastion mode • SOCKS proxy functionality for HTTP/HTTPS auditing
VLAN	• Supported in bridge mode
Management	• Web-based admin UI (current version of Mozilla Firefox for optimal experience) • Dedicated management interface • CLI
Administration	• On device management accounts • AD/LDAP-based management accounts • Customizable role-based administration and audit rights
HTTP REST-based API	• Managing users and credentials

CRYPTOAUDITOR TECHNICAL SPECIFICATIONS

AUDITING, END-USER AUTHENTICATION & AUTHORIZATION

Inspected Protocols	• SSH (v2), SCP, SFTP, RDP, SSL/TLS-protected TCP, HTTP/HTTPS • Supported protocols can be audited also recursively in SSH tunnels
Audit Levels	• Options between “Metadata only”, and “Full channels”
Monitoring and Policy Control	• Rules by protocol, address, port, VLAN, or user group • Easy-to-use rule verification tool • Flexible user credential management (through HTTP REST-based API)
End-User Authentication & Authorization	• On device password or SSH public key • Passthrough password or keyboard-interactive • AD/LDAP-compliant directories • RADIUS • RSA SecurID/OTP • X.509 certificate (SSH only), with PIV/CAC smart card support • HTTP REST API for user authorization • 4-eyes authorization. Alerts via e-mail; connection accept/reject in the web-based admin UI
Shared account management	• Secure password and SSH-key safe
Other	• OCR-based content recognition for RDP (Latin and Cyrillic) • Indexing-enabled free-text content searching

SECURITY

Encryption	• Key Exchange: Diffie-Hellman, RSA • Host Key: RSA, DSA • 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)
Compliancy	• FIPS 140-2 compliant operation through certified OpenSSL library
System Security	• All communication between Hound and Vault secured by TLS • All information stored in the Vault is encrypted with 128-bit AES • No user passwords captured and stored
Alerts and Reports	• System and connection-based alerts to SIEM and syslog • Customizable e-mail reports

THIRD-PARTY APPLICATION SUPPORT

SIEM & Syslog	• IBM Security QRadar SIEM • McAfee Enterprise Security Manager • Splunk Enterprise • RSA Security Analytics • HP ArcSight Logger • Rsyslog • Syslog-ng
IDS	• RSA Security Analytics • Bro
DLP and Network AV	• RSA Data Loss Prevention Suite • Symantec Cloud Protection Engine • McAfee Web Gateway • F-Secure Internet GateKeeper * DLP and network AV integration support through the standard ICAP protocol