Case Study: Monitor, Audit & Control Privileged Users in the Cloud

A major IT services company providing a full range of services from cloud hosting to product development had both a compliance issue and customer SLA requirement mandating they audit their system administrators' access to customer data across their three datacenters, including approximately 20,000 Windows and 10,000 Unix/Linux hosts.

The customer has 16,000+ employees and operates in 20+ countries globally with net sales of about EUR 1.7 billion (USD 2.3 billion) in 2013.

***Crypto*Auditor® was selected to provide transparent, inline privileged access management, demonstrate compliance and protect customer data.**

IT security & cloud providers need to provide reliable audit and monitoring capabilities for privileged user activity but find it difficult to deploy and scale with traditional privileged access management solutions in highly elastic cloud environments.

Privileged users utilize encryption, including SSH, SFTP and RDP, to access, manage and support customer systems. While encryption protects customer information, including personally identifiable information, intellectual property and credit card data, it also blinds layered defenses and audit tools such as SIEM, IDS and DLP from what privileged identities are doing while performing tasks.

Without proper management and controls, a rogue administrator can easily steal customer information and conceal their actions by erasing the end point's sys log and exfiltrating the data through encrypted channels. In addition, advanced persistent threats (APT's) and advanced malware target encrypted channels because it provides both a means to access highly prized data and exfiltrate that data.

Privileged access is expanding to entities outside the enterprise through outsourcing, business partnerships, supply chain integration and cloud services, making trust, audit, forensics, data loss prevention and real time security intelligence a challenge for many IT service and cloud providers.

Additionally, a need has emerged to have more granular control over role-based permissions such that IT Security professionals can tie user actions to human end-users, rather than narrowing the potential actor down to one of a group of system administrators.

The Challenge:

The customer serves thousands of customers worldwide and is a leading provider of application development, consulting services, product development and cloud hosting. Their customer base consists a number of verticals including government, financial, energy, healthcare, manufacturing, retail and media.

The customer needed to solve two challenges:

- Meet a compliance requirement mandating that the company's **privileged administrator access be controlled, monitored and audited** and demonstrate that administrators were not accessing customer data

*Crypto*Auditor™ for the cloud

- Meet an SLA requirement that the company could document that **system administrator's had not accessed customer data and provide a defensible audit trail** for compliance and liability purposes

Solution Requirements:

In evaluating potential solutions, the customer considered the following elements:

- **Rapid, straightforward** deployment
- Impact on **user workflow**
- **Scalability** (hundreds of simultaneous RDP and SSH connections)
- Ability to provide **full recording of privileged user's sessions** for forensic purposes
- **Integration with multiple company Active Directories** to authenticate privileged users
- **Integration with company authorization database** containing continuously updated lists of hosts each user is permitted to access
- **Integration with SIEM** system for collating log information on audited connections
- **High-availability** and, in case of failure, default to passing traffic through instead of blocking it

The customer looked at a number of alternatives including traditional, gateway-based Privileged Access Management solutions or building a homegrown solution.

The Solution:

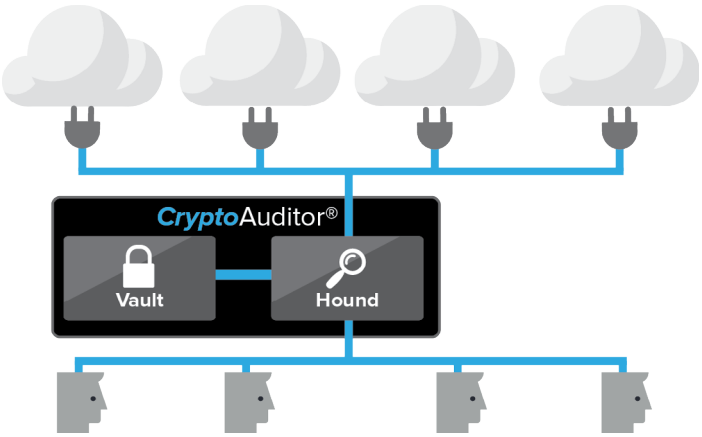
The customer decided to deploy ***Crypto***Auditor because of its next-generation capabilities including:

- **Plug-and-play** deployment
- **Transparent & inline**, requiring little or no change to user workflows
- The **ability to scale** to hundreds or thousands of simultaneous RDP and SSH connections in an elastic environment
- Extensive session **recording, vaulting, search and session replay** capabilities.
- **Turn-key integration** with Active Directory and company authorization database
- **Security intelligence enablement** with the customers existing SIEM system
- **High-availability** and pass-through fail-over to maintain business continuity during peak times

In addition to the customer's requirements ***Crypto***Auditor delivered:

- **Cost savings** by virtually eliminating the need for help desk support and provisioning versus traditional PAM solutions
- The ability to **monitor all privileged identities** transacting the network via SSH & RDP, not just users who log in to a gateway or jump host
- **Extensibility** into AV, IPS, DLP and other layered security solutions
- **Better security** by eliminating back doors and firewall workarounds such as port forwarding

Once fully deployed, the customer was able to comply with regulation mandates, meet customer SLA agreements and strengthen their security posture against both malicious insiders and advanced external threats.



© SSH Communications Security | www.ssh.com