Major Financial Services Company Gains Visibility & Control Over External Contractors

CryptoAuditor®

Servicing customers in 90 countries including 45 of the top 50 banks, this Financial Services company needed to ensure that external, third-party contractors operating in their data centers were monitored and controlled in order to meet both security and compliance requirements.

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

While ubiquitous encryption protects sensitive information from common attack vectors - such as man-in-the-middle and sniffer attacks - it can also be exploited by malicious insiders to conceal attempts to access systems and steal information.

Privileged users utilize encryption, including SSH, SFTP and RDP to access, manage and support servers. Although encryption protects sensitive data, it also blinds layered defenses and audit tools, including SIEM, IDS and DLP, from monitoring the activities of privileged identities.

As enterprise environments extend and the traditional perimeter erodes, organizations face a new imperative: to monitor remote administrators and external contractors accessing critical systems via encrypted protocols at the same security levels on-site employees are subject to.

The Challenge

For this Financial Services company, controlling access to confidential data is not only crucial to the security of the business, but also mandated by national and international regulation. With over 400,000 financial transactions in excess of several billion USD conducted every day, this enterprise sees a high volume of encrypted communications.

The business's administrators use shared high-privilege accounts (such as Windows *administrator* and Unix *root*) to access and manage servers via encrypted protocols -- a common practice among IT professionals.

The organization needed a solution that gave them visibility and control over these accounts, allowing them to monitor the encrypted traffic between high-privilege accounts and specific human identities.

Additionally, the organization had a requirement to enforce security policy and enable monitoring over encrypted access to high value assets.

Solution Requirements

- **Full recording** of privileged users' RDP and SSH sessions for later forensics
- **Integration with Active Directory** to authenticate privileged users and functionality to map shared privileged accounts on the server to specific human users
- **Granular control and auditing** of RDP and SSH sessions, specifically control over clipboard and drive redirect channels and control over SSH tunnels and SFTP file transfer
- **Regular reporting** on privileged connections
- Easy deployment with **zero impact on end-user workflow**
- **High-availability** and pass-through fail-over to maintain business continuity

*Crypto*Auditor® Monitors & Controls Encrypted Channels

The Solution

The customer selected *Crypto*Auditor because of its extensive auditing and protocol-level control capabilities, simple deployment and without impact to end-users. *Crypto*Auditor also provided a solution for shared account management, without the need to deploy cumbersome password vaults.

*Crypto*Auditor's installation and deployment occurred over a matter of days. Gateway or agent based solutions can take weeks to deploy

The customer elected to use the hardware-based *Crypto*Auditor Vault and Hound appliances, deploying the Hounds in bridge mode in a 1+1 high-availability configuration. The Hounds are connected to Active Directory, and the vault component is deployed in a separate management network.

Benefits

Primary benefits *Crypto*Auditor delivered include:

- Extensive session **recording, vaulting, search and session replay** capabilities.
- **Turn-key integration with Active Directory** and company authorization database
- **Shared account mapping** for high privilege accounts
- Capability to **monitor all privileged identities** transacting the network via SSH & RDP, not just users who log into a gateway or jump host
- **Extensibility into AV, IPS, DLP** and other layered security solutions
- **Improved security** by eliminating back doors and firewall workarounds such as port forwarding

With *Crypto*Auditor the customer gained the ability to comply with regulations, protect against insider threats and prevent and detect the misuse of critical systems.