SOLUTION BRIEF

Don't Be Blinded by Encryption: Enable Compliance and Productivity

Empower Internal and External Administratprs with CryptoAuditor

The CryptoAuditor solution from SSH Communications Security enables Audited Privileged Access Management. This creates the transparency organizations need for compliance purposes while empowering users to access critical resources in a controlled but productive way. This is accomplished using existing tools and workflows. The solution adapts to your organization's ways of working, adds a layer of security and visibility, and enables either two-factor authentication or integrates with enterprise-wide authentication. When coupled with McAfee® Web Gateway—part of the McAfee product offering—CryptoAuditor is capable of stopping both accidental and malicious data loss over encrypted channels in real time.

McAfee Compatible Solution

- CryptoAuditor 1.5 integrates with McAfee Web Gateway and McAfee Enterprise Security Manager.
- This powerful combination enables auditing of SSH and SFTP transfers.
- Prevent data leaks in real time.
- Securely manage auditing and configuration from a centralized management console.

The Business Problem: Enabling Transparency with Security

SSH CryptoAuditor is a network-based, inline traffic monitor that is able to record the activities of privileged users without interfering with their normal workflow. Because there are no available agents to deploy, the solution is device-agnostic and can monitor any user on any connection, even when using encrypted SSH, RDP, or HTTPS protocols.

CryptoAuditor is more than a passive monitor. It provides identity-based policy controls that limit where privileged users can go in your network and what they can do. Integration with McAfee Web Gateway and McAfee Enterprise Security Manager enables real-time detection and prevention of data loss. Benefits of protecting critical assets with CryptoAuditor include the following:

- **Accountability:** Know exactly who the user is and what they did.
- **Control:** Grant privileged access on a "need-to-know, need-to-do" basis.
- **Audit:** Access an indexed database of privileged sessions, including video replays of graphical sessions.
- **Real-time defense:** Get security information and event management (SIEM), data loss prevention (DLP), and intrusion detection system (IDS) integration to gain real-time visibility into encrypted sessions.
- **Easy deployment:** Gain transparency and a distributed architecture.
- **Amazon Web Services (AWS) Cloud:** Enjoy efficient, low-cost deployment.

McAfee and SSH Joint Solution

DLP systems provide the tools for inspecting traffic that is relayed to them and make decisions on what to do with the traffic. These systems can, for example, recognize credit card numbers and act according to policies set by the organization.

However, one of the challenges for DLP systems is that they lack the visibility within encrypted traffic (for example, secure shell), and they cannot protect what they cannot see. Similarly, antivirus engines that are deployed in various network infrastructures can only scan unencrypted data. CryptoAuditor makes it possible for organizations to utilize the powerful DLP functionality of McAfee Web Gateway to inspect the contents of privileged SSH and SFTP sessions, or TLS/SSL-secured TCP traffic to enforce compliancy with an organization's policies. This is done in real time, enabling effective data loss prevention and enhancing centralized reporting to the enterprise SIEM solution with McAfee Enterprise Security Manager.

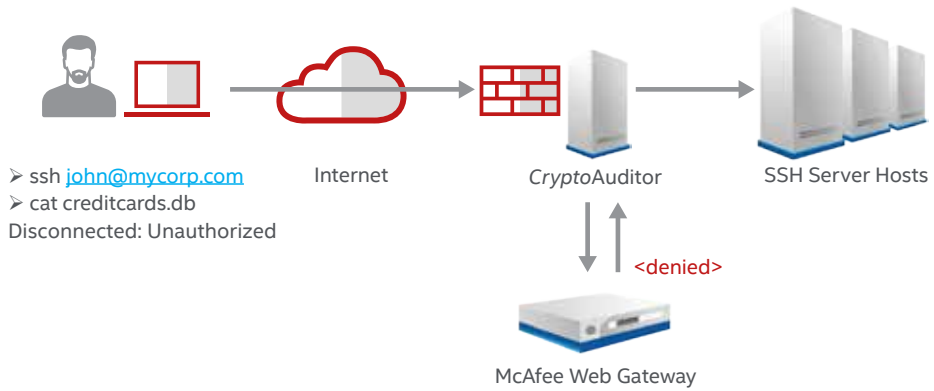

Figure 1. The McAfee and SSH joint solution.

In the example above, a user is accessing the corporate network as a privileged user over an encrypted SSH connection and tries to access a database containing sensitive credit card information. CryptoAuditor analyzes the session content and securely feeds it to McAfee Web Gateway for inspection over the ICAP protocol. This empowers McAfee Web Gateway to determine if this interaction violates a set policy for the organization. At this point, CryptoAuditor can terminate the connection and raise an alert in a central security event management system as per policy.

About SSH

As the inventor of the SSH protocol, SSH Communications Security has a 20-year history of leading the market in delivering advanced security solutions that enable, monitor, and manage encrypted networks. More than 3,000 customers across the globe trust the company's encryption, access control, and encrypted channel monitoring solutions to meet complex compliance requirements, improve their security posture, and save on operational costs.

About McAfee Web Gateway

The McAfee Web Gateway appliance is the first line of defense for any organization to protect against evolving malware threats. It empowers organizations to enable employee access while greatly reducing an organization's risk with an advanced security approach that combines powerful, local intent analysis with cloud-based protection powered by McAfee Labs.

About McAfee Enterprise Security Manager

McAfee Enterprise Security Manager—the foundation for the SIEM solution family from McAfee—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com