**Case Study**

Clearmanage Boosts Cloud Security with CryptoAuditor™

Clearmanage, based in Singapore with operations in Asia and the Middle East, provides cloud services, cloud infrastructure, hosting services, advanced security solutions and services for government agencies and enterprises. Clearmanage also works with its strategic partners to provide additional levels of security for their infrastructure (IaaS), platform (PaaS) and application (SaaS) services to their clients.

CryptoAuditor™ was selected to fulfill stringent audit requirements, provide privileged access management for their own infrastructure and cloud-based security services for their clients.
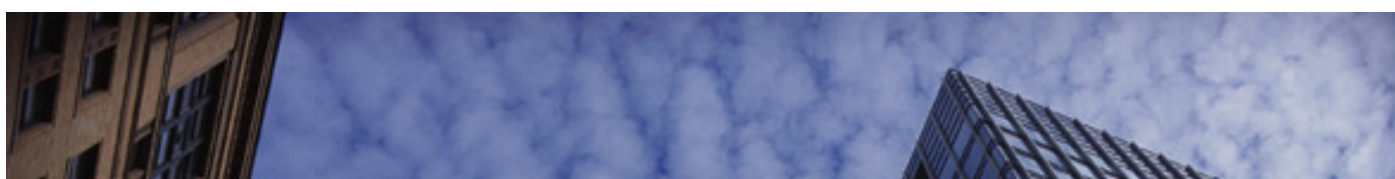
Customer: Clearmanage

clearmanage

Industry: Cloud Service Provider
URL: www.clearmanage.com

Cloud Service Providers need to maintain high standards for data protection and provide reliable cloud services to build trust and credibility with customers. Clearmanage attains a competitive advantage by complying with many security and industry standards. They are one of the first Cloud Service Providers in Singapore achieving the highest Level 3 certification of the Multi-Tier Cloud Security Standard for Singapore (MTCS SS 584:2013), the world's first cloud security standard. Achieving Tier 3 proves the Cloud Service Provider is capable of addressing high impact information systems such as financial and health records as well as highly confidential business data.

Clearmanage was also certified to ISO 27001:2013, requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. Only with these industry recognitions the cloud service providers can put in place the Government Cloud Service Bulk Tenders that are qualified for use by ministries and government agencies in Singapore.

The Challenges

Clearmanage has already implemented security tools and appropriate encryption to protect sensitive information in-transit and in-storage in the cloud environment; however, being able to monitor privileged user activities in the encrypted networks presents an additional layer of complexity.

In order to maintain the stringent certification requirements, Clearmanage is required to provide reliable audit and monitoring capabilities for privileged user activities. Therefore, privileged access management is one of the key compliance requirements needed to certify for industrial standards, in particular MTCS SS 584 and ISO 27001.

Privileged user activities are secured by cryptographic protocols such as SSH, SFTP and RDP. Encryption shields the information from attackers, however it also is a blind spot for security operations and forensics teams. Privileged access can also be the primary threat vector for insider attacks over the encrypted channels. Clearmanage was not able to get the needed visibility into the encrypted channels and privilege identities accessing the cloud, leading to potential security risks and non-compliance. In order to eliminate the risks, Clearmanage needed a Privileged Access Management solution that can decrypt and inspect the traffic in-line and mitigate unwanted access or activity.

clearmanage

Solution Requirements

Clearmanage reviewed a number of Privileged Access Management solutions; and set several criteria for the solution evaluation process. Key evaluation criteria included:

- Agentless, immune to host-based malware
- Non-intrusive to existing cloud service clients
- Real-time monitoring the privileged user activities in encrypted traffic
- Session recording, search and replay
- Audit the encrypted traffic on a need-to-know basis
- Rapid, straightforward deployment
- Scalability and high-availability

After a lengthy review process, Clearmanage selected SSH Communications Security's CryptoAuditor not only because of above features, but also because of the strong and flexible services support SSH Communications Security offered in conjunction with its local distributor.

The Solution

By deploying CryptoAuditor in the infrastructure of its two datacenters located in Singapore, Clearmanage is able to accomplish the following:

- Meet and in some cases surpass the stringent certification requirements and compliance mandates
- Strengthen and demonstrate cloud security controls in its cloud infrastructure
- Provide an additional security service that can be offered to a larger audience
- Give clients more confidence in the security of their confidential data

Value-Added Security Service for Cloud Customers:

In addition to its internal deployment, Clearmanage is able to offer a comprehensive Privileged Access Management service utilizing CryptoAuditor's integration into its cloud service platform. This additional service option will be available for its cloud-hosting clients as part of its offering for government or enterprise cloud services. The offering enables clients self-service provisioning and management of privileged users no matter how the clients are hosted with Clearmanage, in-house or via other service providers.

Customer's Administrator

CryptoAuditor Administrator

CryptoAuditor

Windows Hosts in Datacenter