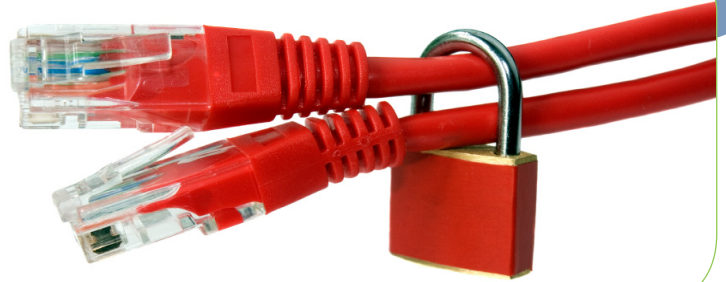


Contact Centers today are being asked to interact with customers via more mediums such as audio, fax, web and email. This gives their companies competitive advantages in the marketplace, while increasing the complexity of managing performance, efficiency, validation of information and the protection of company's assets.

Cacti Encryption PCI/DSS Data Security Standard



PCI Data Security Standard

The PCI Data Security Standard (DSS) is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. When evaluating a new recording solution, organizations should not only consider how the product can help achieve PCI DSS compliance, but also whether the product itself is secure and addresses the various aspects of the Standard.

Secure Your Data

Cacti solutions offer multi-level security control of your recordings, suited to the requirements of your enterprise. Starting with a finely detailed list of user rights and privileges, system administrators can define the criteria for each user's ability to access certain types of recordings, evaluations, agents, agent groups, etc. A separate secure, password based auditor application is required to review recordings, further preventing general personnel from accessing critical data. In addition to these security measures, Cacti solutions also offer both general **Level One** encryption (Basic) as well as **Level Two** 128-bit AES encryption to ensure that your recordings are safe from malicious intent. Data cannot be compromised, accessed, or retrieved without access to the system or the encryption keys, which are limited to certain system administrators.

Mask Sensitive Information

For contact centers that handle sensitive data, multiple options exist for masking those segments, both voice and screen, from being saved or viewed in the call recording. Cacti solutions can use various methods including custom software development, agent/user triggers, event or application triggers, and speech analytics to replace sensitive data with "white noise". This not only provides enhanced PCI DSS compliance, but allows recordings to be used on a broader scale for training and other quality assurance purposes.

Ensure PCI-DSS Compliance

Our server-based solutions allow all storage of recordings to reside within your internal network, enabling compliance to company requirements for physical and network security. All system access events are logged within Cacti's audit trail, which can be visible or hidden based on user permissions. All Cacti server software components are thoroughly tested for security and integrity in Cacti's labs before deployment.

BENEFITS

- Multi-level Security
- Provides up to 128-bit Advanced Encryption Standards (AES)
- Secure Server Level Storage
- Protect critical customer information (i.e., credit card information)
- Restrict user access to recordings by business need-to-know
- Track and monitor all access to recording resources and customer information
- Masking of Sensitive customer data

PCI Compliance

128 AES Encryption

Protect Customer Information

AVAYA

DEVELOPERCONNECTION
GOLD

