

PerformanceEdge® Quality Management Helps Manage Sensitive Customer Data

Keeping your customers' sensitive cardholder data secure is critical for your business to minimize risk and reduce exposure to fraudulent activity. However, adhering to the Payment Card Industry (PCI) Data Security Standard (DSS) across your various contact center technologies can be daunting. PerformanceEdge Quality Management can be a vital element of an overall strategy towards PCI DSS compliance by providing robust recording encryption and security features to help ensure sensitive customer data is securely handled.

With today's ever-increasing threat of identity theft, credit card fraud, and other security breaches, keeping your customers' cardholder data secure is critical for conducting your business and the principal reason for the implementation of PCI DSS compliance standards.

PerformanceEdge Quality Management helps promote compliance with the PCI DSS requirements by securely recording, storing, and replaying customer interactions while at the same time improving the quality of those interactions.

Secure Firewall Configuration Support

PerformanceEdge Quality Management supports your secure firewall configuration as a part of its standard full system operation. All ports required to extend access beyond firewalls are fully documented to address the verification of firewall and router configuration standards for connections to cardholder data.

Customized Password and Security Parameter Controls and Secure Server Configurations

To help keep access to the system secure, all default login credentials for PerformanceEdge Quality Management are fully customizable and include no fixed passwords. In addition, the software's components can be implemented on separate servers. And full documentation of all services, protocols and ports used by PerformanceEdge Quality Management are made available to ensure consistency with industry-accepted system hardening standards.

Automated Tools and Encryption of Recordings to Protect Cardholder Data

To comply with PCI DSS requirements, you need the ability to easily pause recording when sensitive data is being communicated between your agents and customers and resume it at the appropriate time in order to prevent your customers' sensitive account data from being recorded and stored.



Highlights

- Automatic triggers to pause and resume audio and screen recordings.
- AES 256-bit encryption of all stored audio and screen data.
- Secure transmission of recordings over public and private networks.
- Secure firewall configuration support.
- Enables restricted access to audio and screen recordings on a per user basis.
- Provides audit trail of access stored in database.

PerformanceEdge® Quality Management streamlines your ability to meet these requirements using compliance triggers that pause recording whenever sensitive data, such as a Payment Card Number (PCN) is being entered or spoken, and then resume recording once the data has been entered. The software also offers the flexibility to enable your agents to manually pause and resume recording of the call at the appropriate times.

Not only is it important to prevent the recording and storing of sensitive cardholder information, but you also need a way to ensure information is captured properly and securely handled. Therefore, PerformanceEdge Quality Management offers the ability to encrypt all stored audio and screen data using AES 256-bit encryption

Robust Encryption of Recordings for Network Transmission and Secure File Playback

PerformanceEdge Quality Management includes encryption capabilities to ensure cardholder account information is securely handled across open/public networks. The system provides the option to encrypt all audio and screen recordings during the recording process using AES 256-bit encryption prior to transmission over the network. And this secure transmission for recordings is extended at time of playback using Secure Sockets Layer (SSL) communication. Encrypted format is also maintained while the recordings are at rest in their media storage location, thus providing a full end-to-end encryption process throughout the recording's life cycle.

Secure Development and QA Standards Based on Industry-Best Practices

PerformanceEdge Quality Management's development and quality assurance processes (QA) are established based on Microsoft best practices and .net secure code practices throughout its software development life cycle. In addition, the development and QA test environments of the software are maintained separate from the production environment with access controls and a code review process is followed prior to each production release.

Restricted Access to Audio and Screen Recordings

PerformanceEdge Quality Management enables restricted access to all audio and screen recordings that can be configured on a per user basis. This capability allows users to access recordings based on their job responsibilities.

Detailed Tracking and Monitoring of All Access to Recording Files

As part of its standard features, PerformanceEdge Quality Management stores all user access activity within its database to provide an audit trail of all access to your audio and video files. Based on this activity, the software includes an out-of-the-box Web Audit Activity Detail report that gives you visibility into a variety of users' activities, including logon, administrative, playback, and scoring of recordings.

PerformanceEdge Quality Management provides call logging (full-time call recording), sophisticated speech analytics and flexible agent quality coaching capabilities that help you derive value from the knowledge you gather with every customer interaction. It helps drive improvement to people and processes by allowing you to easily evaluate agent quality performance, identify and act on important customer trends and can play a vital role in a company's overall plan to address compliance guidelines (such as PCI DSS).

Aspect cautions that nothing contained in this document is meant to provide legal advice, a guarantee of compliance with any laws, or to create any warranties, expressed or implied, including any warranties of merchantability or fitness for a particular purpose. Compliance with regulatory and other legal requirements is the sole responsibility of each customer. In this document, Aspect is simply illustrating product features that, when used properly, and at each customer's sole determination, may assist with compliance. It is the responsibility of each customer to fully identify and understand current regulatory and legal requirements that are applicable to each customer's unique business circumstances, particularly as such requirements may be revised from time to time. Please note that the information contained in this document is relevant as of the publication date noted herein and does not reflect future revisions to the applicable regulations or other legal requirements.

About Aspect

Aspect provides software and consulting services that turn the potential of unified communications into real business results across the enterprise and in the contact center. Applying 35 years of insight and experience, Aspect helps more than two-thirds of the FORTUNE Global 100, as well as small and medium enterprises, power their business processes with communications. For more information, visit www.aspect.com.

PerformanceEdge™ Group

The PerformanceEdge Group is a dedicated resource within the Aspect organization that is comprised of contact center performance professionals with technical, process and application subject matter expertise.

Corporate Headquarters

300 Apollo Drive
Chelmsford, MA 01824
978 250 7900 office
978 244 7410 fax

Europe & Africa Headquarters

2 The Square, Stockley Park
Uxbridge
Middlesex UB11 1AD
+(44) 20 8589 1000 office
+(44) 20 8589 1001 fax

Asia Pacific & Middle East Headquarters

138 Robinson Road
#13-00 The Corporate Office
Singapore 068906
+(65) 6590 0388 office
+(65) 6324 1003 fax
[aspect.com](http://www.aspect.com)

