CyberSource®

CyberSource Call Center Solution with Bluefin Point-to-Point Encryption

In many businesses, sensitive payment data is still exchanged in the open within the call center. Even security-conscious companies find adequately securing their call center environments challenging, often because the centers are geographically dispersed and the requisite technology solutions are expensive and complex to deploy. As a result, these centers and environments are in Payment Card Industry Data Security Standard (PCI DSS) scope and remain vulnerable to hackers and malware attacks.

CyberSource and Bluefin have partnered to introduce a validated PCI Point-to-Point Encryption (P2PE) standard-based solution[1] for securing call center operations. This solution encrypts cardholder data at the point of interaction (POI) using a PCI-approved P2PE device. Transactions are processed by the CyberSource platform, and decryption is performed off-site in an approved Bluefin Hardware Security Module (HSM). By deploying this solution, you can remove clear-text cardholder data within your call center and reduce the payment security risk posed by hackers and malware. Protecting your systems against such potential threats helps you safeguard your brand reputation in the event of a breach.

Securely accept payments in your call center and reduce PCI scope without overhauling your operations.

KEY FEATURES

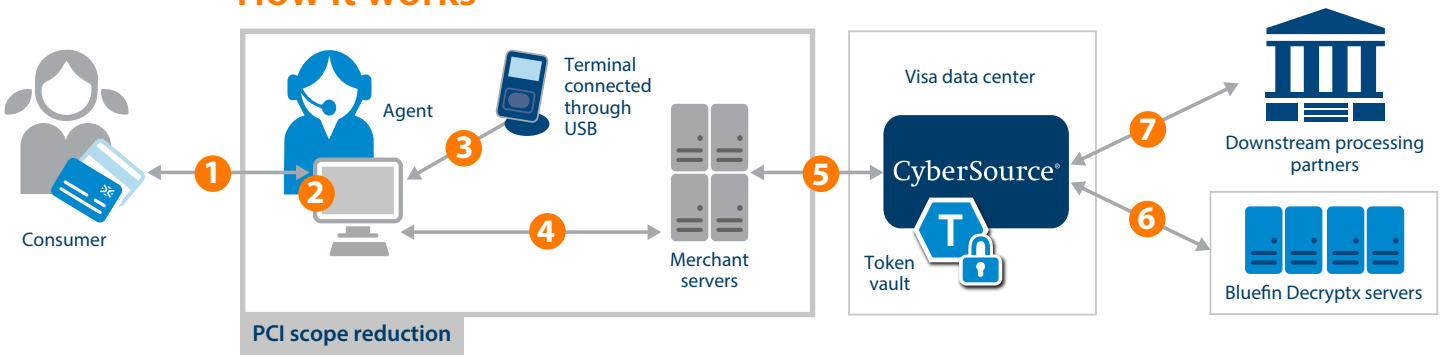
- PCI-validated P2PE
- ID Tech SREDKey keypad and swipe device enabling agents to enter card data
- The Bluefin P2PE Manager for managing users, deploying and terminating devices, tracking device shipping, viewing transactional history, and downloading reports

KEY BENEFITS

- **Improved payment security:** Protecting the call center with a validated PCI P2PE solution removes clear-text cardholder data within the call center and helps lessen the risk posed by hackers and malware
- **Reduced PCI DSS scope:** You may be able to significantly reduce your PCI scope when you implement this solution—check with your Qualified Security Assessor (QSA) for advice

CyberSource®

How it works



1. Customer calls in to place an order and provides payment card data
2. Agent creates an order in the CRM/ERP system
3. Agent enters the payment card number into the ID Tech SREDKey terminal; the terminal encrypts the card number and returns encrypted data to the workstation
4. The workstation sends the encrypted transaction to your servers
5. Your servers send the encrypted transaction to CyberSource
6. CyberSource sends the encrypted data to Bluefin for decryption; Bluefin returns the decrypted values back to CyberSource
7. CyberSource sends the transaction for payment processing

PCI-Validated P2PE

A PCI-validated P2PE solution includes a combination of secure devices, applications, and processes that encrypt data from the POI—for example, at the point of swipe or dip in the terminal—until the data reaches the solution provider's secure decryption environment. The PCI-validated P2PE solution providers such as Bluefin undergo assessment by a highly specialized P2PE Qualified Security Assessor (QSA) before being brought before the PCI Security Standards Council for final acceptance.

PCI-validated P2PE solutions include the following features:

- Secure encryption of payment card data at the POI (the payment terminal)
- P2PE-validated application or applications at the POI
- Secure management of encryption and decryption devices
- Management of the decryption environment and all decrypted account data
- Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading and injection, administration, and usage

Device Security

PCI P2PE-certified devices are designed to detect tampering. If malicious activity is detected, the device is automatically deactivated, preventing a breach at the point of entry or POI device.

Strict Controls

PCI P2PE has a built-in chain-of-custody process for managing PCI P2PE-certified devices. The CyberSource Call Center solution with Bluefin P2PE includes access to the P2PE Manager in which you can automatically track and report on all POI devices for PCI compliance review.

Chain of Custody

All PCI-validated P2PE solution providers must abide by strict controls to protect encryption keys. Device key injection is done directly at a certified Key Injection Facility (KIF), and decryption occurs only in the Bluefin HSM.

The CyberSource Call Center solution with Bluefin P2PE is integrated with the core CyberSource platform and compatible with other CyberSource solutions.

[1] *PCI Security Standards Council, LLC, "Securing Account Data with the PCI Point-to-Point Encryption Standard v2," June 2015, https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf. Information on the PCI-validated P2PE solution in this data sheet is based on this PCI Security Standards Council reference document.*

CONTACT US: t. +1 888-330-2300 e. sales@cybersource.com w. cybersource.com

CyberSource is a Visa solution VISA