Bluefin®

CyberSource®

CALL CENTER SOLUTION

PCI-validated P2PE for Call Centers

Securely accept payments, reduce PCI scope, and protect your brand

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 provide our PCI-validated Point-to-Point Encryption (P2PE) solution for encryption of all 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.

Key Features

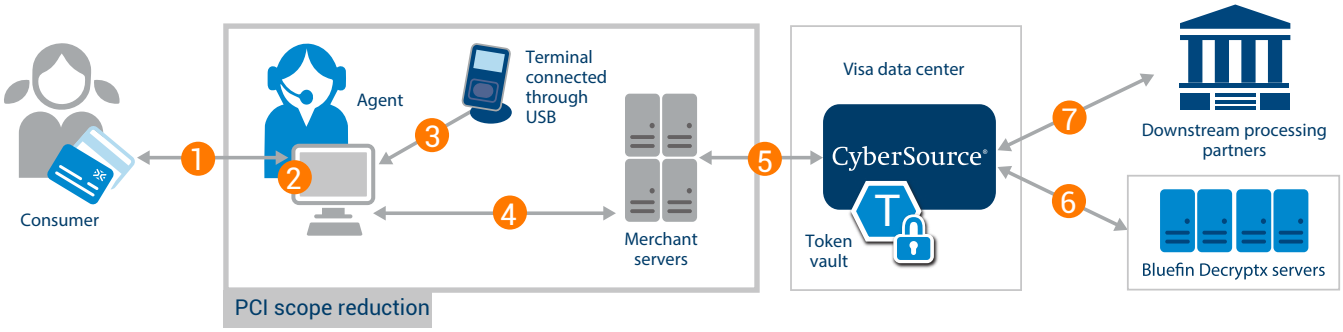
+ ID Tech SREDKey2 keypad and swipe device enabling agents to enter credit card data.
+ Easily deployable PCI-validated P2PE Solution The Bluefin P2PE Manager for managing users, deploying devices, and PCI attestation.

Key Benefits

+ Reduced PCI DSS scope to the 33-question P2PE SAQ.
+ Improved payment security: clear-text card-holder data within the call center and helps lessen the risk posed by hackers and malware.

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.

How It Works



1. Customer calls in to place an order and provides payment card data
2. Agent creates an order in the CRM/ERO system
3. Agent enters the payment card number into the ID Tech SREDKey terminal; the terminal encrypts the card number and return the 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 proessing

01

Device Security

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

02

Strict Controls

All PCI P2E solution providers must abide by strict controls for the encryption and decryption processes. Device key injection is done through certified Key Injection Facilities (KIFs).

03

Cost Savings

The reduced scope of the SAQ to 33 questions enables significant cost savings across security environments, with reductions seen in firewalls, penetration testing, system administration and more.

Bluefin®
bd@bluefin.com
800-675-6573