

EdgeShield from OpenEdge



A proprietary bundle of complementary, EMV-ready security solutions to deliver one of the industry's most secure payment platforms

Cardholder data breaches have become a serious issue among big-box retailers and small businesses, alike. Since 2004 – despite complex PCI requirements – more than 1 billion records have been compromised, raising concerns about the health of digital commerce. A data breach can be a significant liability for a developer offering payments functionality, not to mention the impact on merchant operations.

OpenEdge maintains that the most effective method for keeping cardholder data safe is a multi-pronged approach, combining EMV, encryption and tokenization. **EdgeShield** is the OpenEdge answer – an advanced security services bundle intended to protect credit card data, prevent counterfeit fraud, and enhance payment processing security. Through a unique collection of complementary security solutions, EdgeShield delivers one of the industry's most secure payments platforms while preparing point-of-sale developers and merchants for upcoming EMV mandates. When integrated into systems that accept payments, the bundle protects credit card data while at rest and in transit.

**Protect card data.
Reduce fraud.**

 855.443.8377

 developers@openedgepay.com

 openedgepay.com





Included with EdgeShield

EDGE EMV

This fraud-reduction technology protects card issuers, merchants and consumers from losses due to the use of counterfeit and stolen payment cards at the point-of-sale. EMV Smart Cards are embedded with a chip that interacts with a merchant's point-of-sale device, ensuring the card is valid and belongs to the user. This chip technology is virtually impossible to duplicate. The technology helps insulate developers from complex device driving and card brand certifications.

P2P ENCRYPTION

OpenEdge's proprietary encryption is designed to render cardholder data unreadable, encrypted at the device. Merchants are unable to view card numbers after the swipe or hand-key.

TOKEN VAULT

Cardholder data is replaced by digital "tokens" based on this technology. Sensitive data is stored in the secure OpenEdge vault rather than in the merchant environment.

PCI 3.0 OUT-OF-SCOPE

Payment applications are rendered out-of scope with EdgeShield, eliminating cumbersome PCI validation requirements.

PCI ASSURE

EdgeShield includes the PCI ASSURE program to help merchants simplify PCI compliance with online access to security self-assessment questionnaires, regular system scans, breach insurance and custom security profiles generated from the business' processing activity.

BREACH REIMBURSEMENT GUARANTEE FOR DEVELOPERS

OpenEdge can cover up to \$150,000 in legal costs associated with a developer's defense against a customer in the unlikely case of a card data breach while using EdgeShield.

Merchant Breach Example

There is no "typical" data breach scenario. Cyber-thieves access merchant credit card processing systems in sophisticated, unexpected ways, often skimming sensitive cardholder data for months. Here's an example of how one business was affected by a recent data breach:

Industry: Self Storage

Breach method: Network sniffer planted on server

Time until discovery: 7 weeks

Records compromised: 450

Associated costs:

- Lost business
- Detection
- Escalation
- Customer notification
- Remediation
- Fines
- Legal fees

Total price tag for breach: \$46,000

Data Breach Statistics

