

Securing modern commerce: How omnichannel payment security protects every interaction



Why modern payment security matters

- Real-time transactions allow for improved fraud detection.
- Multiple payment channels create more access points for fraud.
- Quantum computing could compromise current encryption and authentication.
- Point-in-time compliance isn't enough — security must be continuous, omnichannel, and multilayered.

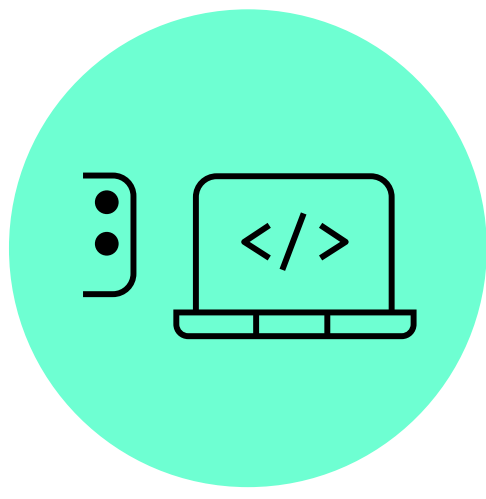
Verifone's multidimensional security approach

A three-legged stool approach ensures robust protection across:



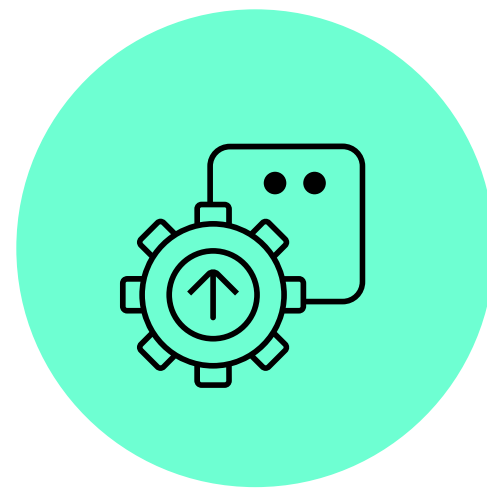
1. Hardware

- Tamper-evident terminals, anti-skimming devices, and case-open switches
- Security meshes and bunkers protect sensitive components
- Embedded security features to prevent tampering and data theft



2. Software

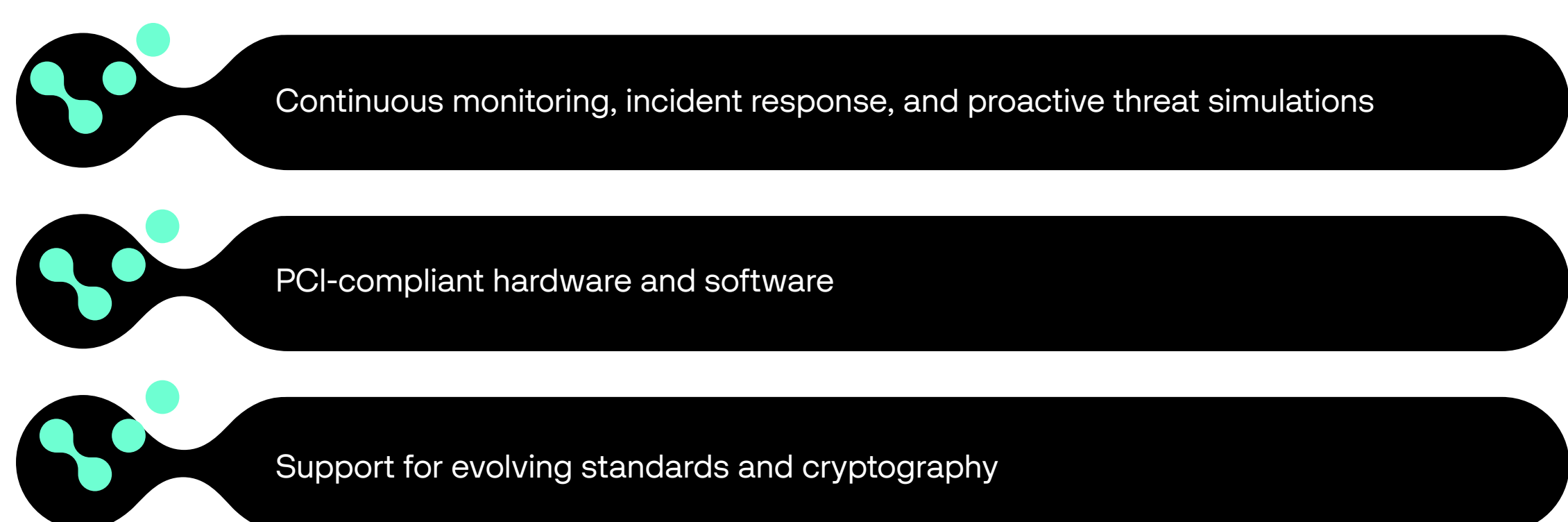
- End-to-end encryption (E2E) & PCI-validated point-to-point encryption (P2PE)
- Advanced AES DUKPT encryption protocol
- Tokenization safeguards and eliminates exposure of sensitive card data
- Biometric authentication (palm, face)
- Remote skimming detection (RSD) for multilane terminals



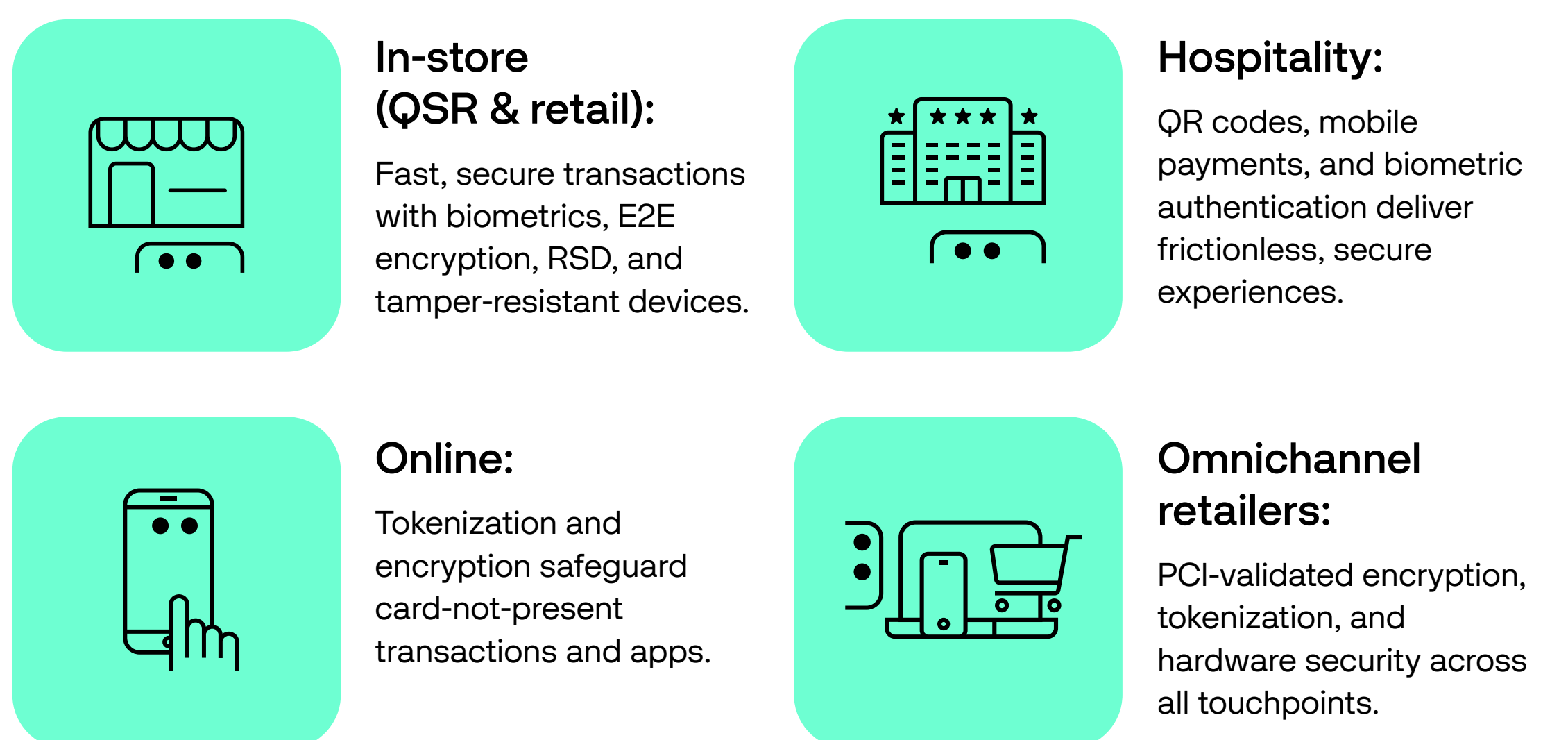
3. Deployment

- PCI-compliant hardware and software
- Continuous monitoring, incident response, and proactive threat simulations
- Support for evolving standards and post-quantum cryptography

Future-ready payment security



Securing every environment



The Verifone advantage



Verifone provides a trusted foundation for driving modern, seamless, and secure commerce experiences.

[Learn more about Verifone omnichannel solutions](#)