

BUYER'S GUIDE

3-D Secure Server

How to evaluate 3DSS providers for authorization performance, transaction intelligence, resilience and growth

The new evaluation standard

Transform EMV 3DS into an authorization intelligence advantage



At a glance

Contents

A practical framework for first-time selection, replacement and optimization decisions.

- 01.** The category has changed
- 02.** What a modern 3DSS should enable
- 03.** How to evaluate performance
- 04.** Continuity, visibility and resilience
- 05.** Integration, testing and future readiness
- 06.** Vendor scorecard
- 07.** Evaluating Entersekt

Why the 3DSS decision matters

The 3DS Server sits at a commercially important point between digital checkout and issuer decisioning.

For years, many organizations evaluated a 3DS Server primarily as protocol infrastructure: certification, scheme connectivity and reliable message processing. Those remain essential. But they no longer describe the full value—or the full cost—of a poor decision.

A modern 3DSS influences the quality of transaction context made available through EMV 3DS, the continuity of authentication journeys, the operating visibility available to payment teams and the organization's ability to improve performance over time.



The buyer's question

Not simply: Can the provider process EMV 3DS? Ask: Can it help us improve decision quality, transaction continuity and measurable business performance?

This guide is for

- Merchants and digital-commerce platforms
- PSPs and payment gateways
- Acquirers and multi-merchant operators
- Payments, fraud, authentication and product leaders

Use it when

- Selecting a first 3DSS provider
- Replacing a legacy or bundled provider
- Expanding into new regions or schemes
- Improving an underperforming 3DS program

The hidden cost of treating 3DS as compliance infrastructure

Compliance and fraud prevention are foundational. The opportunity goes further.

What teams experience

- Good customers challenged or declined
- Checkout abandonment and timeouts
- Incomplete out-of-band result paths
- Fragmented visibility across merchants and regions
- Manual troubleshooting and reconciliation

What the business feels

- Lower approval confidence
- Lost legitimate revenue
- Higher operational expense
- Inconsistent customer experience
- Slow, evidence-poor optimization

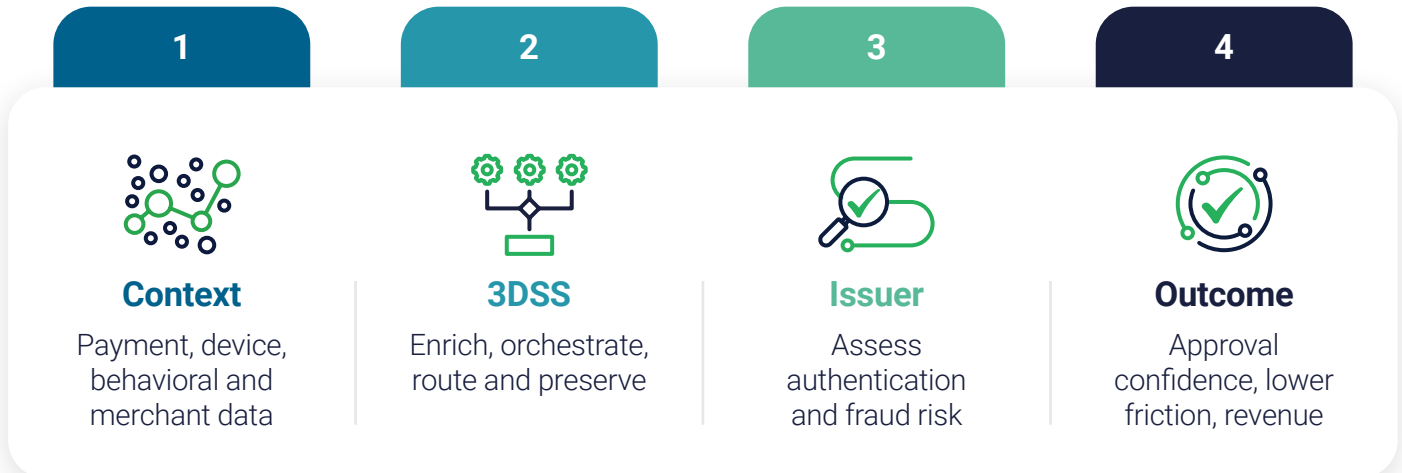
Traditional authorization infrastructure may give issuers limited context about a card-not-present transaction. When uncertainty is high, conservative decisions follow. At the same time, a brittle authentication journey can turn a valid result into an incomplete checkout.

Important distinction

The 3DSS does not approve or decline the authorization. It can improve the richness, reliability and observability of the information available around that decision.

From authentication processing to authorization intelligence

From transaction data to business outcomes



The 3DSS does not make the issuer's authorization decision. It improves the quality and continuity of the information surrounding it.

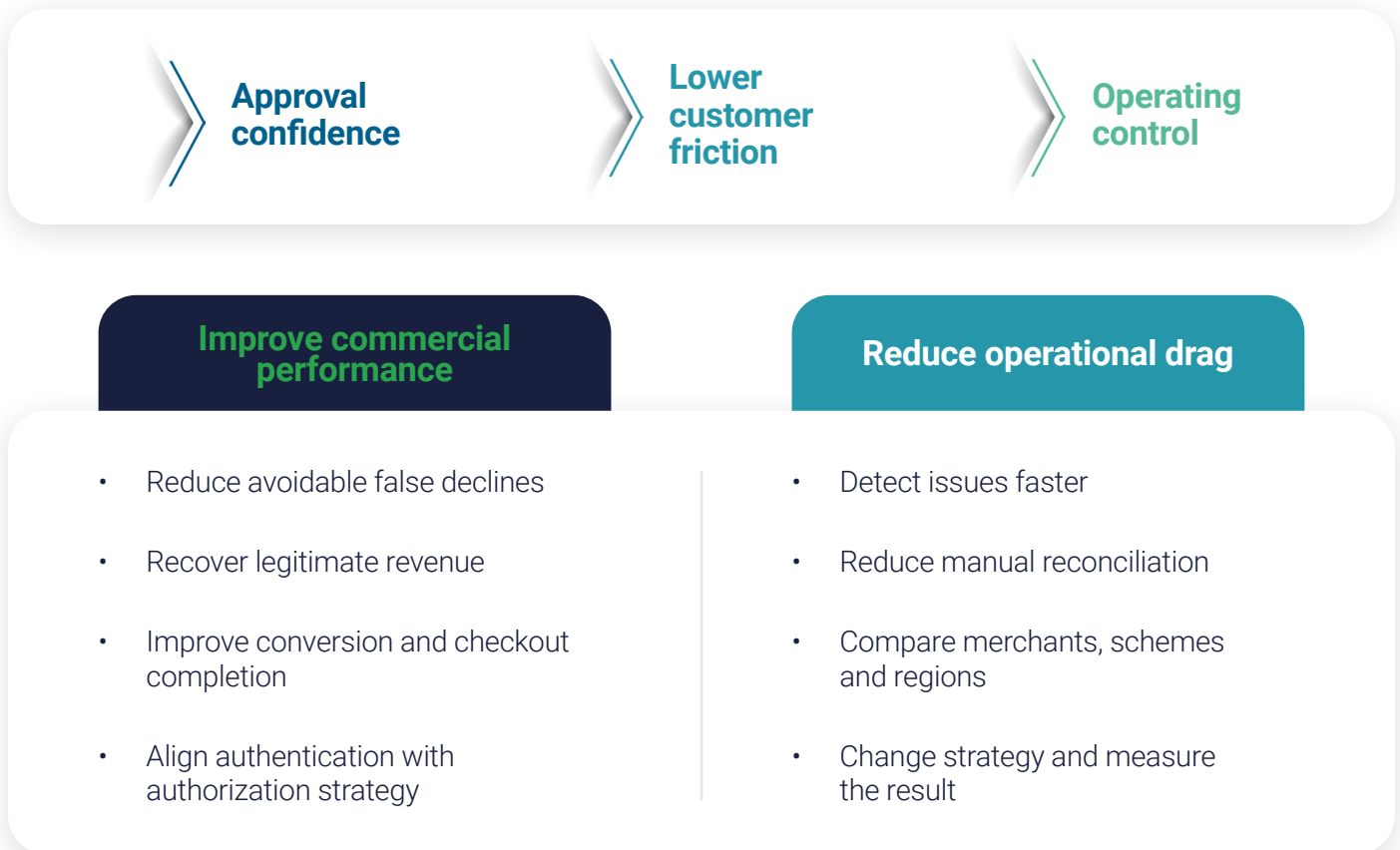
Authorization intelligence is not a replacement for compliance or fraud prevention. It is the strategic value created when richer transaction context, dependable execution and usable performance insight strengthen authentication and authorization decisioning.



Eight capabilities define a modern 3DSS

Criterion	What good looks like	Evidence to request
Transaction intelligence	Preserves and enriches high-quality context across flows.	Supported fields, validation process, mapping documentation.
Performance optimization	Supports frictionless, challenge, Data Only and exemption strategies.	Production metrics by flow, region and scheme.
Transaction continuity	Returns completed results reliably when browser journeys fail.	Callback design, retry, acknowledgement and reconciliation behavior.
Operational visibility	Makes performance issues visible and actionable.	Live demonstration using realistic dimensions and filters.
Resilience and scale	Maintains service through peaks, failures and geographic events.	SLA, latency, failover tests and incident history.
Integration and control	Fits merchant, PSP, gateway and acquirer operating models.	API docs, tenancy model, routing and configuration options.
Testing confidence	Supports realistic end-to-end and exception-path validation.	Test components, certifications and migration methodology.
Future readiness	Adapts to new protocols, schemes, use cases and signals.	Delivered roadmap record, architecture and standards participation.

Three outcomes should govern the buying decision



A provider should demonstrate how its capabilities contribute to these outcomes, while separating what the product directly controls from what also depends on issuer behavior, merchant configuration, traffic mix and regional regulation.

Optimize the balance—not a single headline metric

The performance balance



The highest frictionless rate is not automatically the best result. The right target balances fraud control, approval confidence, regulatory obligations and customer experience for the buyer's portfolio.

Ask for comparable evidence

Require metrics for a defined production period, transaction population, market, scheme, device/channel mix and flow type. A portfolio-wide average can hide the behavior that matters.



Evaluate the quality of transaction context

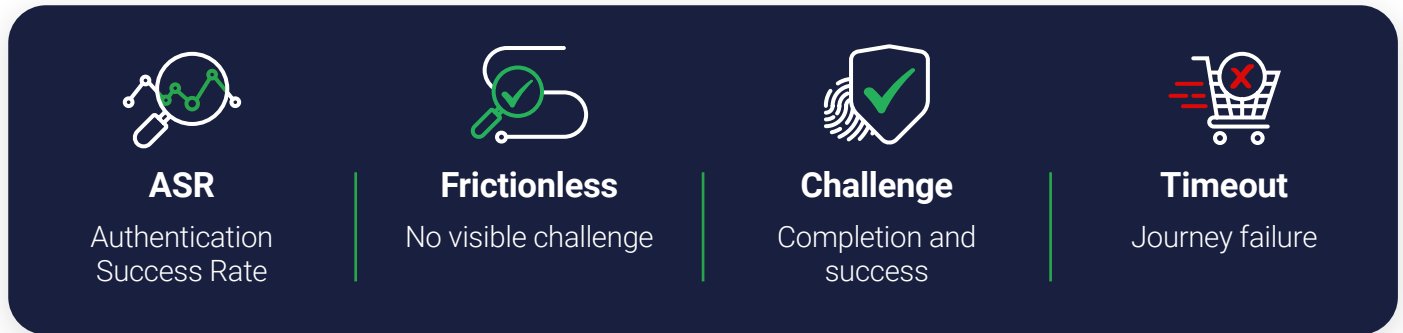
More data is useful only when it is accurate, consistently mapped and relevant to decisioning.

Criterion	What good looks like	Evidence to request
Data coverage	Supports the required EMV 3DS fields and relevant contextual signals.	Field inventory by version, scheme and channel.
Data quality	Validates completeness, format and consistency before routing.	Validation rules, rejection handling and quality reporting.
Enrichment	Adds useful merchant, device, behavioral or contextual information where supported.	Architecture and examples of enriched transactions.
Interoperability	Preserves meaning across DS, ACS, scheme and protocol differences.	Field-mapping approach and exception handling.
Decision relevance	Shows which data contributes to better authentication or authorization confidence.	Controlled analysis or comparable production evidence.

RED FLAG

A large advertised number of data points is not evidence of value. Ask which signals are populated, accurate and demonstrably useful for your traffic.

Interrogate the complete performance story



Performance must be examined across the entire journey. A provider may show a strong aggregate success rate while particular merchants, issuers, schemes, devices or challenge flows underperform.

Metrics to request	Segments to require
• Authentication Success Rate (ASR) • Frictionless and challenge rates • Challenge completion and success • Timeout and technical failure rates • Authorization approval and false-decline indicators	• Merchant and tenant • Scheme and region • Issuer / ACS • Browser, app and device • Data Only, frictionless and challenge flow

Evidence standard

Ask the provider to explain the metric definition, denominator, exclusions, time period and relationship between authentication and downstream authorization outcomes.

Treat Data Only and exemptions as strategies—not checkboxes

Data Only—also referred to here as Data Share Only (DSO)—can improve the context available to issuers without initiating a conventional authentication challenge. Exemptions can reduce unnecessary friction where scheme rules and regulation permit.

The commercial value depends on market rules, scheme support, issuer behavior, data quality and how the merchant integrates Data Only and exemptions into a broader fraud, authentication and authorization strategy.

Criterion	What good looks like	Evidence to request
Coverage	Which schemes, regions, transaction types and versions are supported?	Current support matrix and restrictions.
Routing control	Can Data Only be configured by merchant, transaction, scheme or geography?	Configuration demonstration and rule hierarchy.
Visibility	Can teams distinguish DSO performance from authenticated flows?	Reporting filters, outcomes and export/API support.
Evidence	What measurable results exist for comparable traffic?	Defined production cohort, downstream outcomes and net chargeback impact.
Governance	How are regulatory and scheme-rule changes managed?	Ownership, update process and customer communication.

Buyer discipline

Do not accept a universal approval-uplift claim. Require evidence from a comparable market, scheme, issuer mix and merchant category.

A successful authentication should not become an incomplete checkout

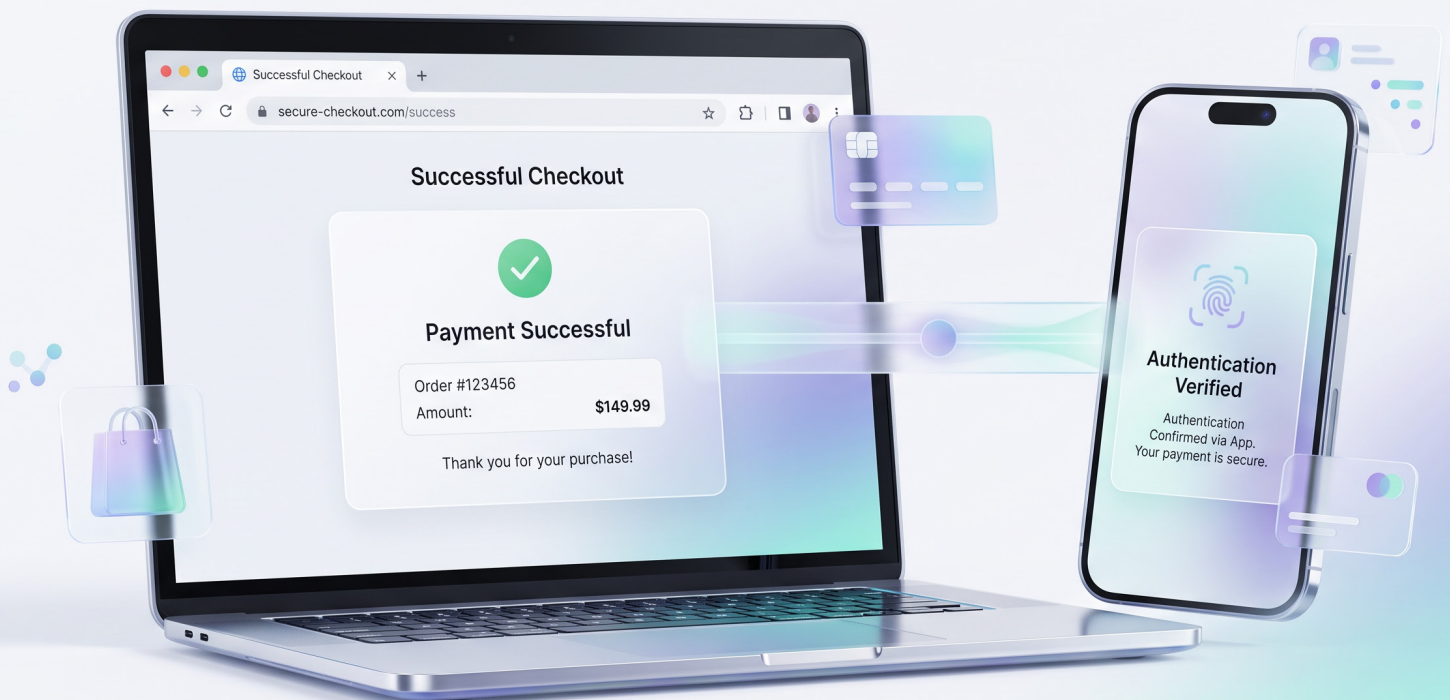
Merchant callback: close the result gap



Why it matters

The browser may fail to return even after successful authentication. A secure callback gives the merchant the result it needs continue the payment, even when the browser stalls.

Authentication and checkout data is distributed across the merchant, 3DSS, Directory Server, ACS and issuer; no single participant sees the entire journey. Merchant Callback is especially valuable in browser-channel out-of-band flows, where the cardholder may approve in a banking app but an interrupted browser return leaves checkout status uncertain. A secure server-to-server callback can deliver the final result without relying solely on redirection. Evaluate endpoint security, acknowledgements, retries, idempotency and reconciliation.





04 | Continuity, visibility and resilience

Operational visibility must support continuous optimization

Visibility should lead to action



A dashboard is not the end state. The test is whether teams can diagnose performance, change strategy and demonstrate improvement.

Questions the data should answer

- Where are failures increasing?
- Which merchants or issuers differ?
- Are challenges, timeouts or abandonment changing?
- How do schemes, devices and regions compare?

Operating questions

- Who owns optimization?
- How quickly can a team isolate a problem?
- Can data be exported or integrated?
- How is improvement measured and governed?

Resilience is more than an uptime percentage

Criterion	What good looks like	Evidence to request
Availability	Architecture removes single points of failure.	Contractual SLA and historical attainment.
Geographic continuity	Service can recover from regional disruption.	Hosting topology, RTO/RPO and failover evidence.
Peak performance	Latency and throughput remain predictable under load.	P95/P99 latency, peak TPS and volume-test results.
Recovery behavior	Retries, queues and idempotency prevent loss or duplication.	Failure-path design and test evidence.
Monitoring	Teams receive actionable alerts and status information.	Monitoring coverage, notification policy and status history.
Support	Incidents have clear ownership and escalation.	24/7 coverage, severity model and response commitments.
Feature release control	Supports controlled activation and rapid rollback of new capabilities.	Release documentation, feature-control demonstration and rollback test.
Maintenance continuity	Maintains service during planned maintenance and component failure.	High-availability design and controlled maintenance/failover test results.

Contractual test

Ask which metrics are contractual, which are merely observed and which exclude planned maintenance, downstream scheme latency or customer-side dependencies.

Choose the operating model—not just the API

Integration flexibility

- Redirection and server-to-server models
- Synchronous and asynchronous APIs
- Version compatibility and field mapping
- API documentation, security and key management
- Migration and certification support
- Connection reuse and keep-alive options that reduce latency and improve throughput

Control at scale

- Multi-tenant and PSP modes
- Tenant-, merchant- and scheme-level configuration
- Transaction routing logic
- Role-based administration
- Regional and local scheme support

For PSPs, gateways and acquirers, tenancy, hierarchy and merchant-level controls can be as important as base protocol support. Buyers should test whether the provider's operating model matches their commercial model and support responsibilities.

Demonstration request

Ask the provider to configure a representative merchant hierarchy, route two different transaction types, expose the results in reporting and demonstrate how an operational change is governed.

Test the journeys that fail—not only the happy path

Criterion	What good looks like	Evidence to request
End-to-end coverage	Merchant, 3DSS, DS, ACS and SDK paths can be exercised.	Available certified components and supported scenarios.
Exception paths	Timeouts, retries, duplicate messages and unavailable components are testable.	Negative-test catalogue and expected outcomes.
Realistic data	Testing reflects production versions, schemes and routing.	Environment parity and test-data controls.
Performance	Scale, latency and concurrency are validated before launch.	Load-test plan and acceptance criteria.
Migration confidence	Cutover, rollback and parallel-running risks are managed.	Detailed implementation plan, owners and gates.

Why it matters

A realistic test environment reduces integration surprises, but it does not replace production monitoring. Require both preproduction confidence and post-launch observability.

Future readiness should be observable today

Future-ready by design



Evaluate architecture, standards participation, investment history and delivered capabilities - not roadmap language alone.

A future-ready provider should show a repeatable ability to interpret standards, deliver scheme changes, support new transaction patterns and help customers adopt them without major architectural disruption.

Weight the criteria around your operating model

Suggested evaluation weighting

Authorization intelligence & data quality

20%

Authentication, approvals & customer experience

20%

Resilience & transaction continuity

15%

Visibility & optimization

15%

Integration & control

10%

Security & compliance

10%

Implementation & support

5%

Future readiness

5%

Merchants may increase the weight on approvals, checkout continuity and conversion. PSPs and gateways may emphasize tenancy, integration, routing and operational visibility. Acquirers may place additional weight on scale, scheme coverage and portfolio reporting.

Evidence-based evaluation scorecard

Score each provider only after reviewing the requested evidence.

Category	Decision standard	Provider score
Authorization intelligence	Quality, enrichment and relevance of context.	1 2 3 4 5
Performance optimization	Balanced fraud, approvals and CX outcomes.	1 2 3 4 5
Data Only and exemptions	Flexible, visible and compliant strategy support.	1 2 3 4 5
Merchant Callback	Secure, reliable and actionable result delivery.	1 2 3 4 5
Operational visibility	Fast diagnosis and measurable optimization.	1 2 3 4 5
Resilience and scale	Contractual, tested and geographically robust.	1 2 3 4 5
Integration and control	Fits the required operating model.	1 2 3 4 5
Testing and migration	Realistic coverage and controlled transition.	1 2 3 4 5
Future readiness	Delivered innovation and adaptable architecture.	1 2 3 4 5

Scoring guide: 1 = unsupported or assertion only; 3 = supported with partial evidence; 5 = proven with comparable production evidence and contractual clarity.

How Entersekt addresses the modern 3DSS standard

Entersekt 3DSS builds on compliance and fraud prevention to create an authorization-intelligence advantage.

Criterion	What good looks like	Evidence to request
Richer transaction intelligence	Enriches, orchestrates and routes EMV 3DS context before authorization.	Validate field support and enrichment for the target use case.
Frictionless and Data Only	Supports low-friction, DSO and exemption strategies.	Validate scheme, region and flow coverage.
Merchant Callback	Securely pushes completed authentication results to a defined merchant or processor endpoint.	Review endpoint security, retries, acknowledgements and reconciliation.
Insights	Provides near-real-time visibility across transaction and authentication performance.	Demonstrate required merchant, scheme, status and time filters.
End-to-end testing	Provides test capabilities using EMVCo-certified components for realistic journey validation.	Confirm supported versions, scenarios and implementation plan.
Flexible operation	Supports browser and server-to-server models, multi-tenancy, routing and configuration controls.	Map architecture to the buyer's exact operating model.
Smart Authentication (emerging)	Extends pre-authentication decisioning with Advice and Intelligence capabilities.	Confirm current availability, supported use cases and production-readiness for the target deployment.

Commercial principle

Entersekt should be evaluated using the same evidence standard as every other provider: comparable production data, explicit metric definitions, technical validation and contractual clarity.

Next step: run a performance and architecture assessment

Turn the guide into a working evaluation using your transaction mix, operating model and measurable objectives.



Entersekt can help payment, fraud, authentication and product teams assess current-state performance, map high-priority journeys and define an evidence-based provider evaluation.

Bottom line

Richer EMV 3DS intelligence >> stronger authorization confidence >> better business outcomes

Selected sources and terminology

- EMVCo, EMV 3-D Secure: emvco.com/emv-technologies/3-d-secure.
- EMVCo, EMV 3-D Secure white paper and public protocol educational materials.
- Entersekt 3-D Secure Server: entersekt.com/platform/3-d-secure/server.
- ASR = Authentication Success Rate.
- DSO = Data Share Only.
- ACS = Access Control Server.
- DS = Directory Server.
- Availability and terminology may vary by scheme and market.

Results vary by transaction mix, issuer behavior, scheme, market, integration and customer configuration. Buyers should validate capabilities and outcomes for their own environment.