I AM SOLIDCORE SUITE FOR APTRA™

An NCR Secure™ Solution

Prevent the execution of unauthorized code on your ATM systems

Solidcore Suite for APTRA is focused on two urgent, but historically opposed, challenges facing IT organizations:

- To eliminate the business risk posed by network perimeter breaches or internal security threats
- To reduce growing information security operating costs while facing increasingly restrained IT resources

Solidcore Suite for APTRA addresses both these issues simultaneously by only allowing authorized code to run on a protected ATM.

Maintain protection and compliance of your ATM network:

Protecting the code at runtime and maintaining the integrity and compliance of the ATM means you can reduce the risk and costs related to ATM protection.

No unauthorized code will run. Eliminating the ability for malicious programs or persons to compromise your ATM network.

For more information,
visit www.ncr.com, or email financial@ncr.com.

Why NCR?

NCR Corporation (NYSE: NCR) is the global leader in consumer transaction technologies, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables more than 450 million transactions daily across the retail, financial, travel, hospitality, telecom and technology industries. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Duluth, Georgia with over 26,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.

Key features

External threat defense

- Ensures that only authorized code will run
- Unauthorized code cannot be injected in memory
- Authorized code cannot be tampered with or hijacked

Internal threat defense

- Local administrator lockdown gives the flexibility to disable even local administrators from changing what is authorized on a solidified system, unless authenticated

Deploy and forget

- Easily installed
- Low maintenance following initial configuration

Rules-free, signature-free, and application independent

- Does not depend on signature databases
- Effective across all applications
- Protects against known and zero-day threats

Small footprint, low runtime overhead

- Takes up less than 200MB disk space
- Minimal runtime footprint

No false positives

- Logging can be configured to note all changes at the ATM – authorized and unauthorized

Integration

- Integrates with existing enterprise infrastructure software

Reporting

- Provides a collection framework that consolidates logs across individual end points
- Can provide image deviation, event analysis, and alerting integration with querying and reporting data analysis, linked to global threat intelligence database
- Supports PCI compliance by providing standard interfaces to export/integrate loss of data and reports

Search

- Includes a web-based free form search interface that can quickly provide detailed and actionable information in response to ad-hoc queries

Customizable

- Easy to use standard interfaces to customize protection and behavior on the ATM

 www.ncr.com