SafeNet AT

Bringing Core-Level Data Protection Solutions to the Tactical Field

The views expressed in this presentation are those of the author(s) and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government.

Core-level Security

Extended to the Tactical Field

Trusted, U.S. based source for tactical cyber security solutions…

We **develop**, **manufacture**, **sell** and **support** exclusive, trusted data security solutions in the U.S. that easily integrate into an existing cyber security infrastructure.

…from headquarters to the field…

Our solutions enable agencies to apply the same level of protection deployed at the core to the tactical field.

…extending your data protection ecosystem.

Our solutions extend your data protection ecosystem, where data and cryptographic keys are secured and managed, and access and distribution are controlled, to tactical and mobile environments.

SafeNet AT

© SafeNet AT

Extending Core-Level Data Center Functionality to the Field

- Data Center (Core) functionality is moving to the field
- Core data protection capabilities transitioning with that move
  - » Cryptographic Key Management
    - Key Lifecycle
    - Encryption
      - – Data at Rest
      - – Data in Motion
  - » Authentication
    - Identity Assurance
  - » Information Sharing
    - Transfer Cross Domain Solution (CDS)

SafeNet AT

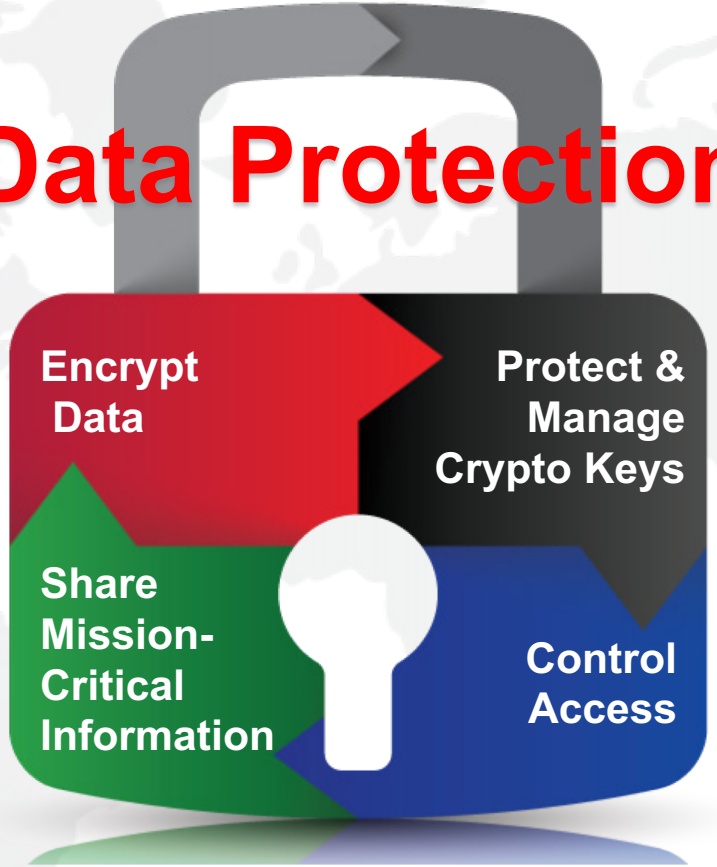
© SafeNet AT

Protecting Active Mission Critical Data

Holistic Data Protection in the Field

At rest and in motion through encryption solutions

While ensuring exchange of correct and authorized data with authorized recipients with cross domain solutions



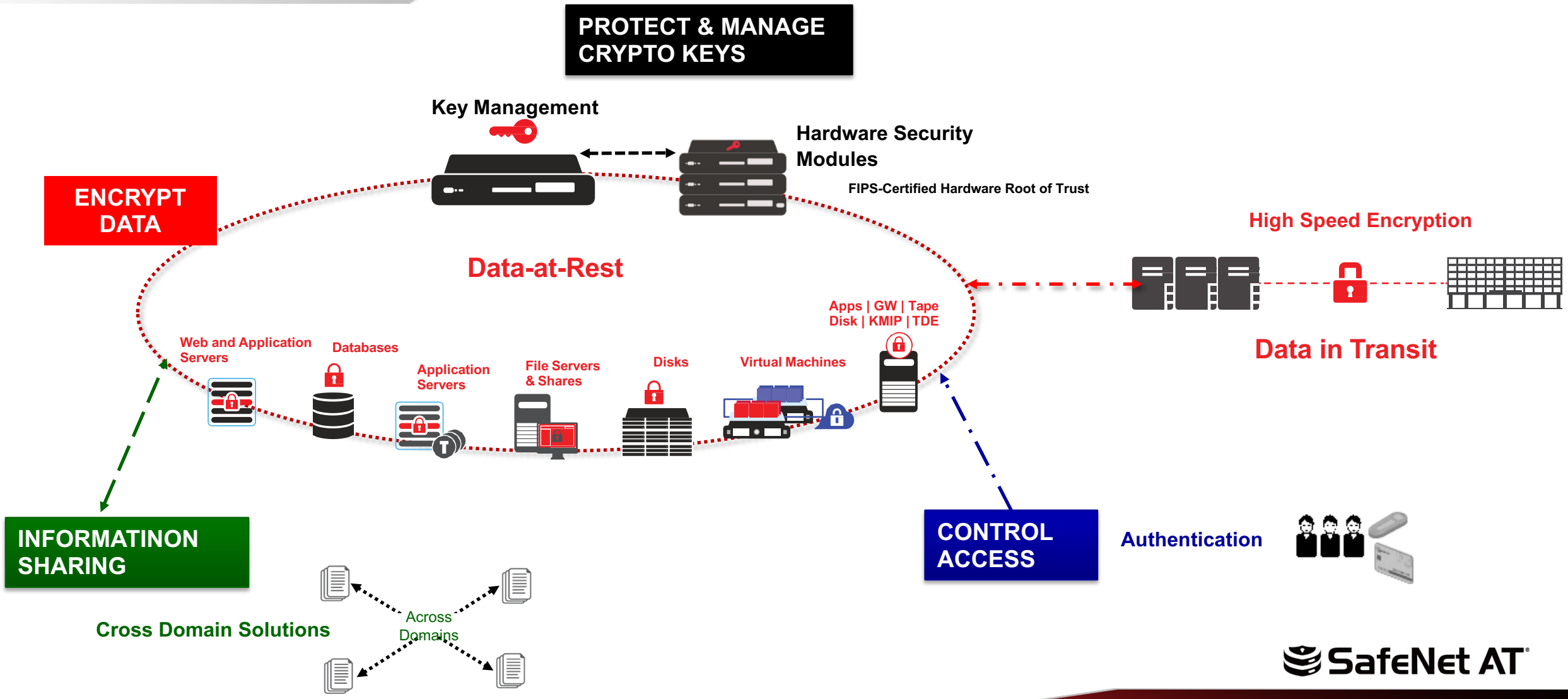
Used to encrypt data with hardware and virtualized cryptographic key management solutions

To sensitive data and protect user identities with authentication solutions

SafeNet AT

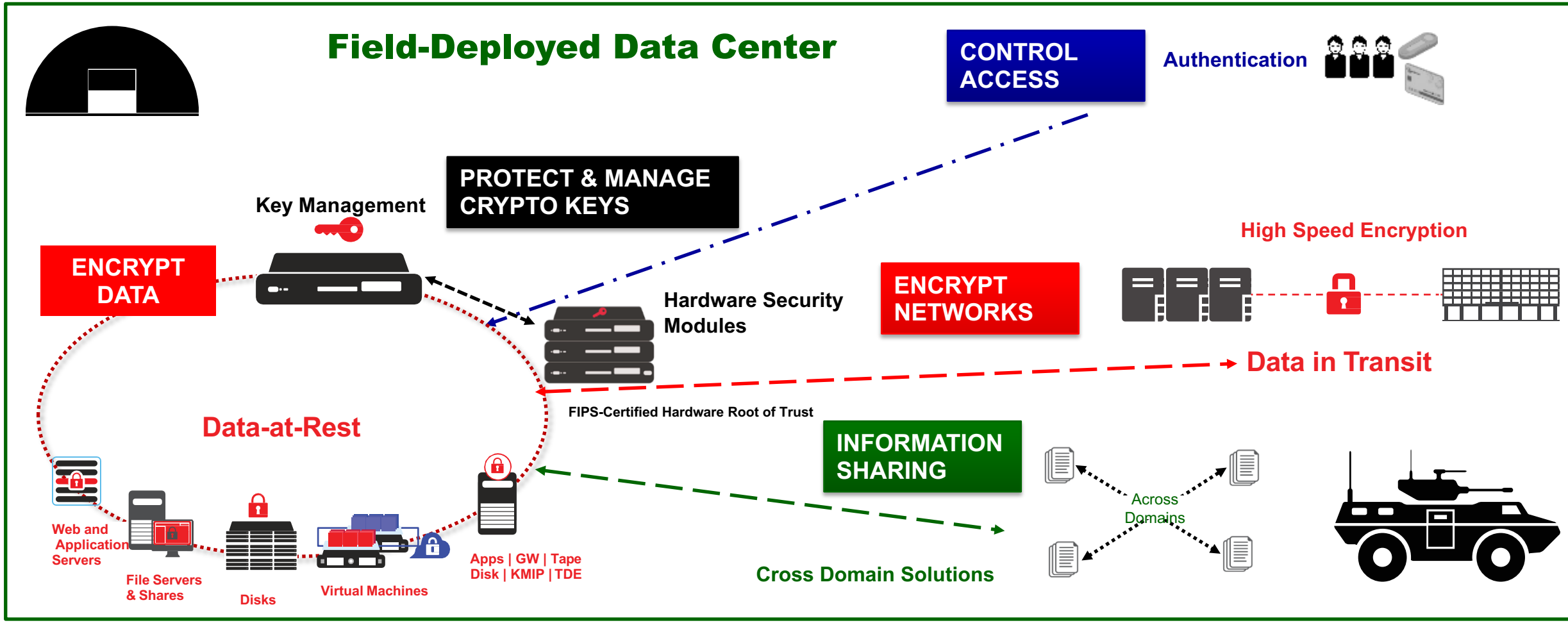
© SafeNet AT

Holistic Data Protection at the Core



© SafeNet AT

Core-Level Solutions Extended to the Cyber Edge



SafeNet AT

© SafeNet AT

Tactical Impacts on Core Data Protection Capabilities

Adapt core-level data protection capabilities to address tactical challenges in the field

Category	Issue	Adaptation
Physical Environment	Robustness	• MIL-STD 810G
	Footprint	• Small Form Factor, Lightweight, Portable
	Loss of Control	• Crypto Erase (CE), Memory processing
Operational Environment	Personnel Constraints	• Limited SME
	Security Domains, Information Domains, Coalitions	• Cross Domain, Virtual Domain, Cryptographic Partitions
Manageability	Logging, Auditing, Monitoring	• Active Export, Non-Retention, Delayed Availability
	Configuration	• Enterprise or Local
	Policies	• Enterprise or Local
Acquisition	Supply Chain Integrity	• Controlled Configurations, U.S. Manufactured
	Technology Refresh	• COTS product lifecycle

© SafeNet AT

Tactical Cryptographic Key Management and Encryption

Protect and **manage** the cryptographic keys used to encrypt data in remote environments in a hardware appliance

Encrypt mission critical data stored remote environments and exchanged between network infrastructures

© SafeNet AT

Cryptographic Key Management for the Field

Enterprise/Local Management

Type 1 HSM Token

Crypto Erase (CE)

Cryptographic keys are best protected when they are secured and managed in a hardware device.

Most hardware cryptographic key management platforms are not conducive to mobile and/or tactical environments due to their size

COTS

SFF

Portable

Agencies need the ability to provide secure means for key management and protection in remote and tactical environments

Log Exports

U.S. Manufactured

Lightweight

SafeNet AT

© SafeNet AT

Rightsizing Cryptographic Key Management for the Field

Supports leading storage platforms

Storage Encryption

Provides encryption solutions for structured/ unstructured data & SEDs

Data Encryption

Supports application level encryption and cloud application partners

Applications

Provides a “Keys in Hardware” solution for VM encryption

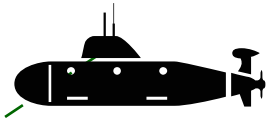
VM Encryption

Supports link level encryption and traffic flow security

Network Encryption

Store → Generate → Distribute → Rotate → Terminate → Recover

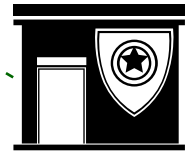
Forward Deployed Environments



Disconnected Environments

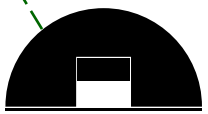
Forward Operating Base

Mobile Command Center

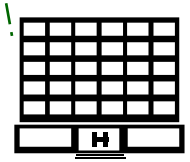


Forward Mission Operations

Off-line Data Protection



Crypto-Erase



Disaster Recovery

SafeNet AT

Authentication in the Field

Provide simplified access to sensitive networks and workstations through a single authentication device

© SafeNet AT

Identity Assurance Authentication for the Field

MIL-STD 810G

Portable

COTS

Multi-Domains (Partitions)

SFF

Widespread data breaches and rampant insider threats mean agencies are looking to deploy strong authentication solutions to:

- Secure access to multiple independent networks
- Protect user identities

Agencies want to bring the **same level of authentication** used to access DoD enterprise infrastructures to their own tactical environments

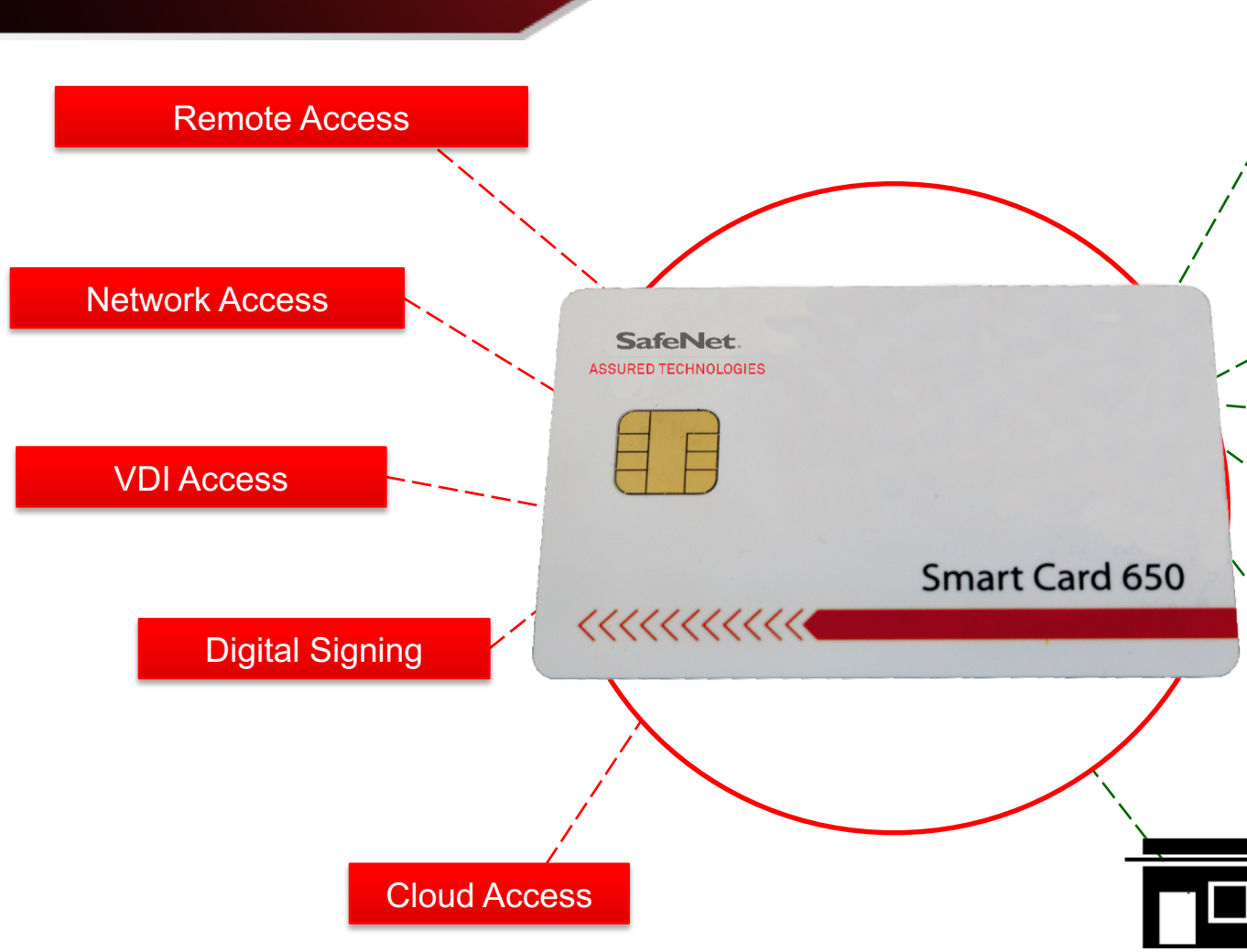
Lightweight

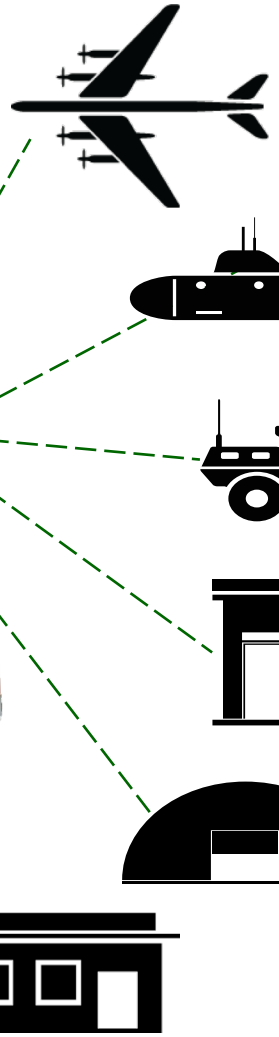
U.S. Manufactured

SafeNet AT

© SafeNet AT

Rightsizing Identity Assurance Authentication for the Field





Forward Deployed Environments

Mobile Command Center

Disconnected Environments

Forward Operating Bases

Disaster Recovery

Forward Mission Operations

Remote/Lights-Out/Non-Managed Facilities

SafeNet AT

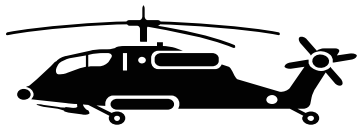
Tactical Cross Domain Solution

Across **classification levels and domains** and across **organizations** and **missions**

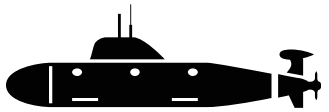
© SafeNet AT

Assured Information Sharing/CDS for the Field

- Situational Awareness
- Defense/Intelligence Coordination
- Disaster Response
- Supply Chain Security
- Cloud Storage and Analytics



Forward Deployed Environments

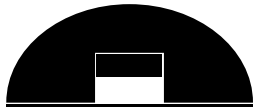


Disconnected Environments

Forward Mission Operations

Mobile Command Center

Forward Operating Base

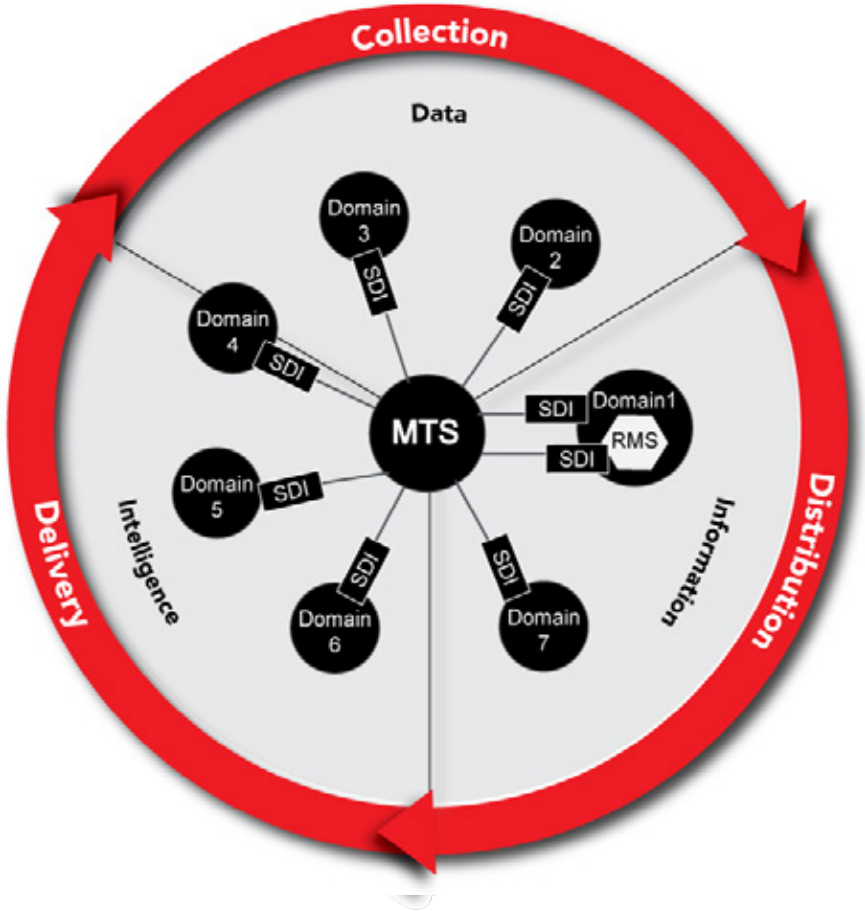


Disaster Recovery

SafeNet AT

© SafeNet AT

Rightsizing CDS Capabilities for the Field



MDeX Transfer System (MTS)

Security core appliance that orchestrates the flow and filtering of information according to customer policies and rule sets

Remote Management Station (RMS)

Enterprise management appliance for policy and security management, command and control, and monitoring of MTSs

Security Domain Intermediary (SDI)

Protocol and queuing software agent that is the edge interface between domain applications and MTS

SafeNet AT

© SafeNet AT

Summary

- Taking Capabilities to the Field
  - » No loss of Capabilities
- Rightsizing Capabilities for the Field
  - » Mitigating Tactical Impacts
- Future Directions for the Field
  - » Integrating with other Data Protection Capabilities

SafeNet AT

© SafeNet AT

Questions?

Contact Information:

Barry Lotenberg
Director of Sales Engineering
SafeNet Assured Technologies
info@safenetat.com

SafeNet AT

© SafeNet AT