CAT Security Overview

Safeguarding Data Reported to CAT

Agenda

1. CAT Overview
2. Security Program Organization
3. Security Framework
4. Secure Architecture
5. Security Controls

CAT Overview

Introduction to CAT

CAT NMS Plan

The Securities and Exchange Commission (SEC) approved Rule 613 under the Securities Exchange Act of 1934, which requires national securities exchanges and national securities associations (collectively, **the Participants**) to submit a national market system plan to create, implement, and maintain a consolidated audit trail (CAT NMS Plan) that would capture customer and order event information for orders in NMS Securities and OTC Equity Securities (Eligible Securities), across all markets, from the time of order inception through routing, cancellation, modification, execution, and allocation.

CAT Overview

CAT Organizations, Roles & Governance

CATNMS LLC

- Consortium of National Securities Exchanges and National Securities Associations (SROs)

Operating Committee (OpCo)

- Serves as the governing body for CAT and provides review, guidance, and oversight for the overall operations of the CAT
- Industry Advisory Committee provides OpCo with industry perspective and guidance

Leadership Team (LT)

- OpCo designated Participant staff to manage delivery and operations of the CAT pursuant to the CAT NMS Plan

Plan Processor

- Selected by the OpCo to implement and operate the CAT
- FINRA CAT is the Plan Processor. FINRA (parent) provides supporting services pursuant to a shared services agreement.

CISO and CCO

- Fiduciaries of the CAT NMS LLC, to ensure compliance with all Plan requirements, including security.
- Continuously monitor releases and operations
- Recommend and implement improvements

Security Working Group (SWG)

- Working group comprised of CAT CISO as well as CISOs and security experts from each Participant.

CAT Overview

CAT Data

- **Definition of CAT Data**
  - Data derived from Participant Data, Industry Member Data, SIP Data, and such other data as the OpCo may designate:
    - Transaction Data
    - Customer Account Information
    - Customer Identifying Information
- **Efforts to minimize sensitive data collected**
  - OpCo intends to file request for exemptive relief with the SEC to modify Plan
    - SSNs, DOBs, and Account Numbers of individual investors would no longer be required.
  - OpCo believes this will significantly reduce risk profile
    - Substantially reduces potential to facilitate identify theft.

CAT Overview
CAT Users

CAT Reporters

- Plan Participants
  - Transmit transaction data, review and repair errors
- Industry Members
  - Transmit transaction and customer data, review and repair errors
- Authorized Reporting Agents may report on behalf of a CAT Reporter

Regulatory Users

- Includes query tool access for SRO and SEC Regulatory Users
- Separate access and entitlements required for Regulatory Users from the CAT Reporters

CAT Overview

Plan Security Requirements

Architectural Level Controls

1. **Secure connectivity to CAT**
2. **Role Based Access Controls (RBAC)**
3. **CAT Data not accessible via public internet and deployed within the network infrastructure**
4. **Segregation of CAT compute and network infrastructure from other cloud tenants**
5. **Customer data segregated from transaction data**
6. **All data encrypted in flight and at rest including archival data storage**
7. **Separate Customer query system**

Program-Level Controls

1. **CISO and CCO Responsibilities**
2. **CAT Data Access and Confidentiality**
3. **Datacenter Standards**
4. **Industry Standards**
5. **Key Management**
6. **Penetration Testing (Independent third-party)**
7. **Breach detection and management policies**
8. **Review of Participant Security Policies**

Security Program Organization

Strong Security Team / Independent Validation

- Plan Processor security capabilities:
  - Dedicated CAT CISO and Security Analysts
    - CAT CISO (and CCO) has fiduciary obligation to Participants (CAT NMS LLC)
  - Secure Systems Architecture
  - Software Security Engineering
  - Threat Hunting, Detection, Response
  - Identity and Access Management
  - Security Policy, Governance & Operational Oversight
  - Security Monitoring, Analysis, & Reporting
- Experience & Certifications
  - CISSPs, CSSLPs, CTPRPs, ISSAPs, IACRB Pen Testers, Certified Ethical Hackers, A+/Net+/Sec+, and more

- AWS brings additional breadth/depth
  - Built on industry leading secure cloud platform.
  - Senior Solutions Architect specializing in security committed via Premium Support agreement.
- Mature and effective policies, tools and processes
- 3rd Party Tested and Evaluated
  - CAT undergoes annual NIST SP800-53 IV&V
  - Third-party pen test and code review
  - FINRA Parent SOC 2 audits, info sec program assessments. Assessed as outperforming peer organizations and employing industry leading practices.
- Relationships & memberships provide early access to threat info & analysis

Security Program Organization

Standards, Policies, Oversight

Robust Controls Framework

- NIST SP800-53, in accordance with Plan.
  - Further informed by ISO 27002, NIST Cybersecurity Framework.
  - System Security Plan established.
  - Third-party Independent Verification and Validation; annually as well as with major changes.
- Continuous Monitoring
  - In accordance with NIST SP800-137
- CAT is an SCI System of the Participants. Plan Processor is an SCI entity and operates in compliance with Reg SCI.

OpCo / Security Working Group (SWG)

- SWG established by OpCo. SWG makes recommendations to Operating Committee.
- Comprised of FINRA CAT CISO as well as CISOs and security experts from each Participant. SEC also an observer to the SWG.
  - Substantial breadth/depth of infosec expertise; hundreds of years combined experience

Security Policies

- Full suite of cybersecurity policies, including:
  - Data Security
  - Insider Risk
  - Incident Management
  - Logging and Monitoring
  - Account Management

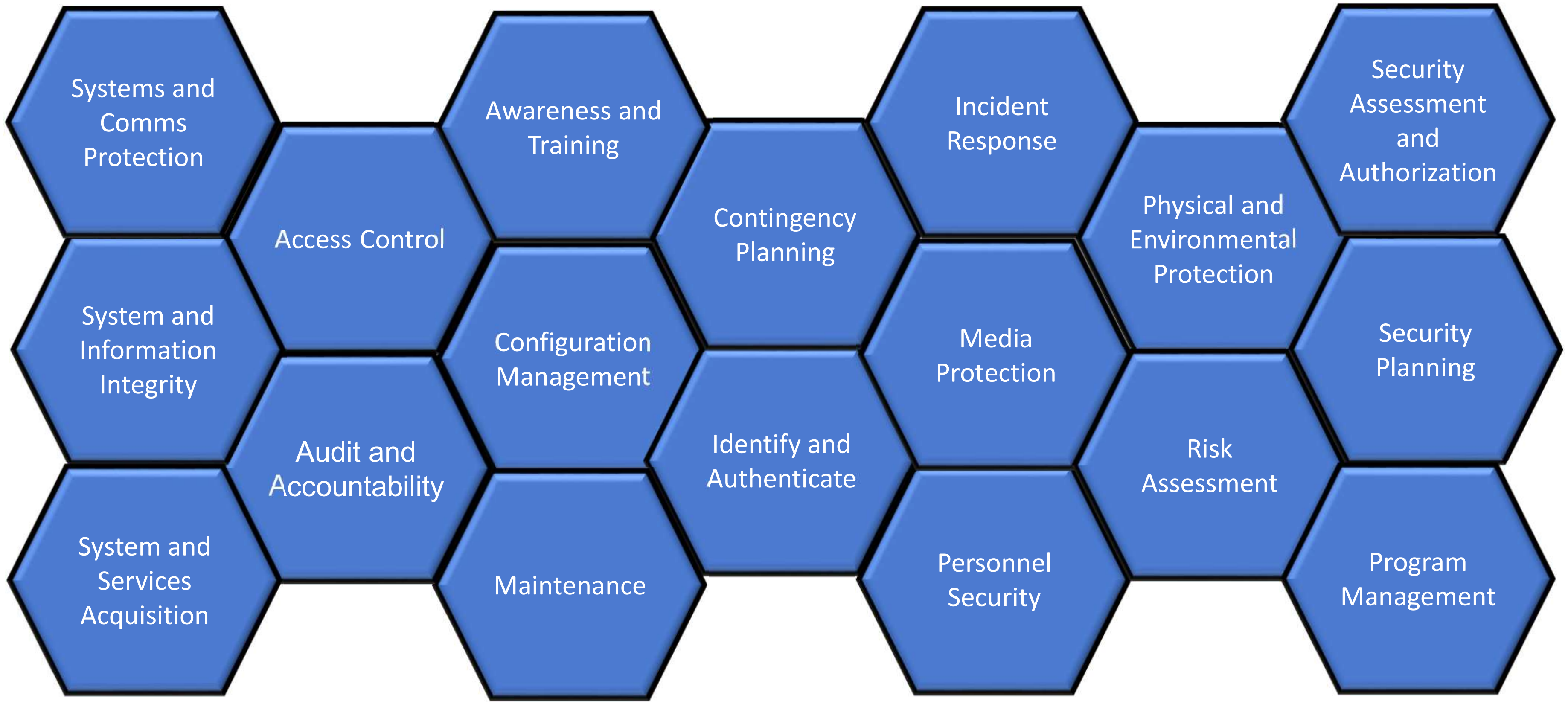
Security Program Organization

AWS is Secure, Well-governed Foundation

- **AWS complies with broad array of industry and international security standards; maintains relevant independent certifications**
  - PCI DSS Level 1 (Payment Card Industry Data Security Standard)
  - ISO 27001 (International Standard for Information Security Management)
  - DIACAP (DoD Information Assurance Certification and Accreditation Process)
  - FISMA (Federal Information Security Management Act) / NIST SP800-53
  - FedRAMP (Federal Risk and Authorization Management Program)
  - ITAR (International Traffic in Arms Regulation)
  - FIPS 140-2 (Federal Information Processing Standards for Cryptographic Modules)
  - SEC Rule 17a-4(f)
  - CSA (Cloud Security Alliance)
  - MPAA (Motion Picture Association of America Security Best Practices)
  - HIPAA (Health Insurance Portability and Accountability Act)
  - AICPA SOC1, Type II report (SSAE 16/ISAE 3402; formerly known as SAS70)
  - AICPA SOC2, Type II report (Security Trust Principles)
  - AICPA SOC3 (SysTrust Certification)

Security Program Framework

NIST SP800-53


Systems and Comms Protection

System and Information Integrity

System and Services Acquisition

Access Control

Audit and Accountability

Awareness and Training

Configuration Management

Maintenance

Contingency Planning

Identify and Authenticate

Incident Response

Media Protection

Personnel Security

Physical and Environmental Protection

Risk Assessment

Security Assessment and Authorization

Security Planning

Program Management

Security Program Framework

Security-integrated Development Lifecycle

Cloud Security

Web Application Firewalls

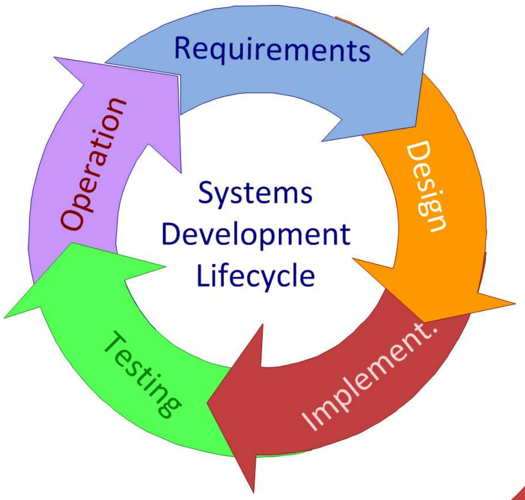
Data At-rest Encryption

Penetration Testing

System Risk Categorization

Security Requirements

Threat Modeling



Security Architecture

Security Configuration Standards

Source Code Analysis

Access Control Validation

Dynamic Vulnerability Testing

Continuous Scanning

Foundational Elements	
Education/Outreach: Maintain Plan Processor staff security knowledge and skills	**Vendor Security**: Assess/Monitor third-party risk
Governance/Compliance: Robust suite of policies and standards. Managed compliance with industry standards (e.g. NIST SP800-53)	**Separation of Duties:** Lower environments sanitized; entitlements apply ‘policy of least privilege’

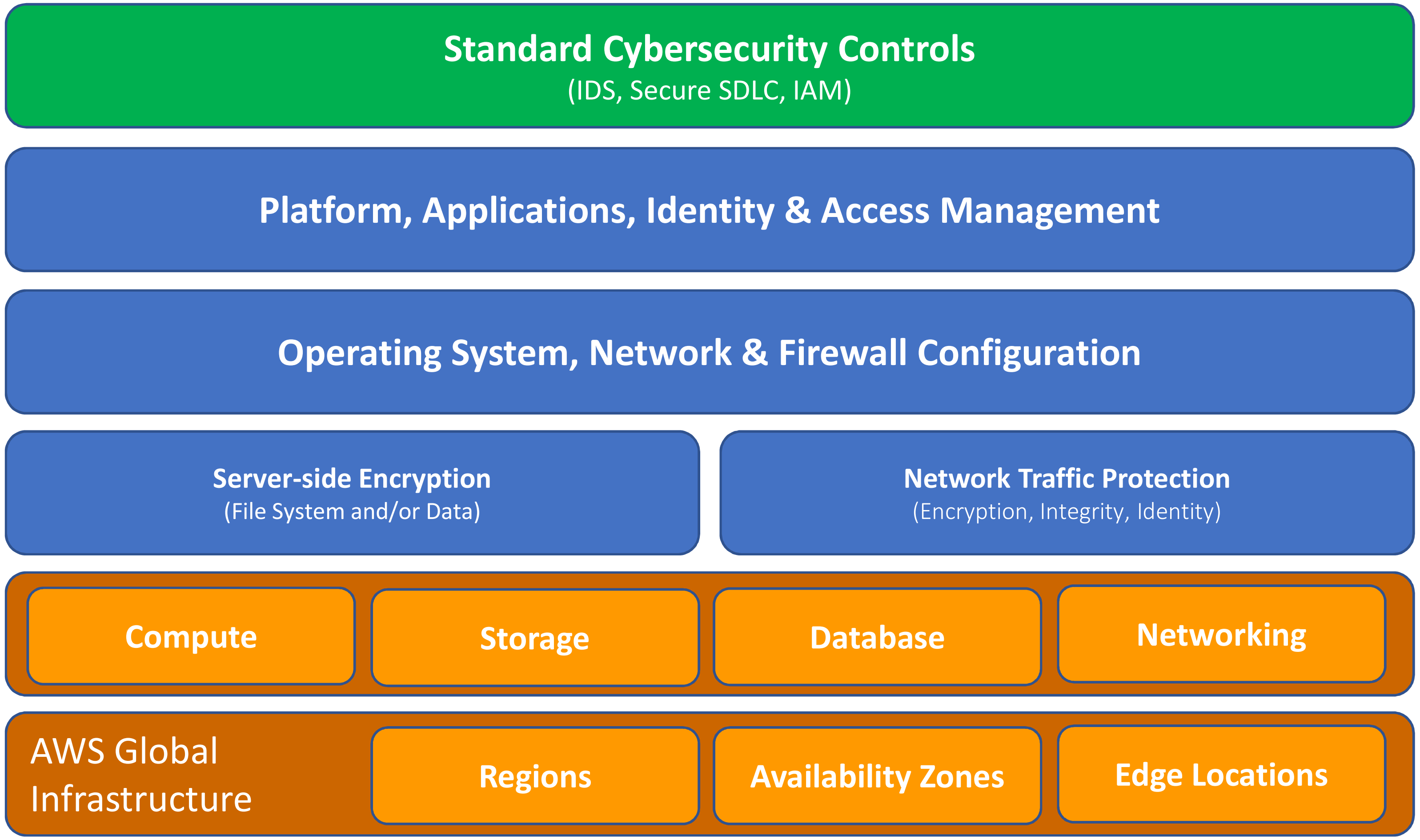
Security Program Framework

Cloud–Powered Security

Security **“ABOVE”** the cloud
Secure software design, assurance
Access Management
Monitoring, threat management

Security **“IN”** the cloud
Hardened configs, monitoring
Microsegmentation
Operational Separation of Duties, Monitoring

Security **“OF”** the cloud
AWS native controls.
FINRA CAT validates and monitors through its mature third-party risk management program.



Standard Cybersecurity Controls
(IDS, Secure SDLC, IAM)

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

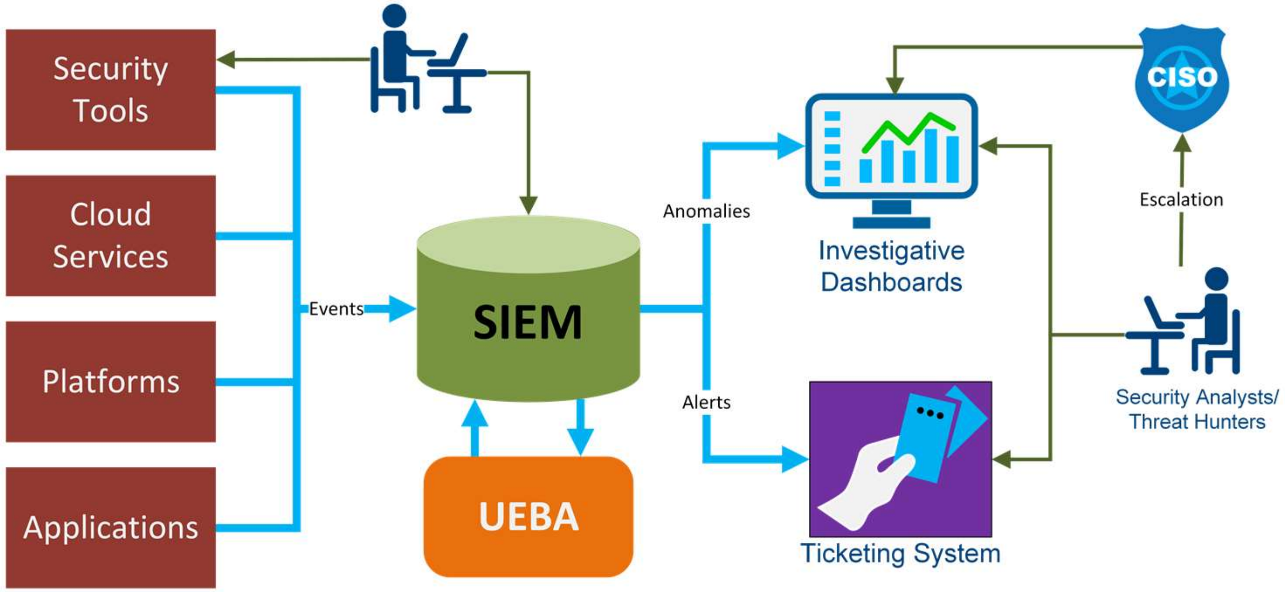
Server-side Encryption
(File System and/or Data)

Network Traffic Protection
(Encryption, Integrity, Identity)

Security Program Framework

Threat Detection, Monitoring, & Alerting

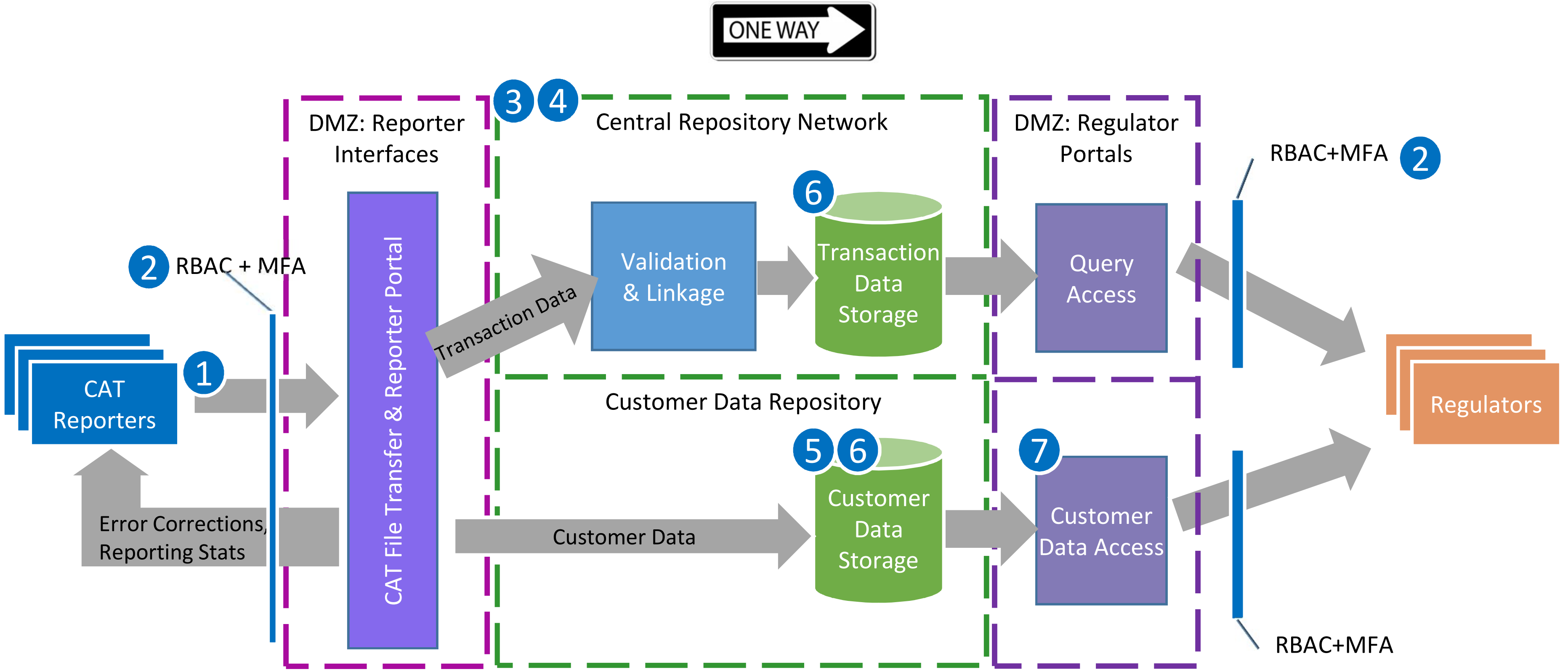
- Multiple automated Threat Intelligence Feeds
- Extensive logging (breadth and depth)
  - Security Tools
  - Cloud services
  - Platforms
  - Applications
- Security Information and Event Management (SIEM)
  - Collection, analysis, and reporting
  - Behavioral Analytics (UEBA)
  - Continuous Monitoring (NIST SP800-137)
  - Dashboard, Alerting
  - Ticketing, triage, resolution.



Rapid and effective ability to detect and respond to malicious activity.

Secure Architecture

Architectural Features Enhance Security



Network Isolation

- Industry Members: Private Lines, AWS PrivateLink, Secure Reporting Gateway
- Participants: Private Line
- Reporters separated from Regulators
- Reporter Interfaces cannot access the Central Repository
- Separate network segments DMZs, Central Repository, & Customer Data

Encryption

- In Transit
- At Rest

Authentication & Entitlement

- Multi-factor Authentication (MFA)
- Granular Role Based Access Control (RBAC)

Extensive, Granular Logging

- Security Information & Event Management (SIEM)
- User and Entity Behavior Analytics (UEBA)

Key

➡	Encrypted Connection	🟩	Encrypted Storage
– –	Isolated Network	– –	DMZ Network

Security Control Highlights

Connectivity

- Two categories of secure connectivity offered:

	Private Line	CAT Secure Reporter Gateway
Industry Member Reporting	IM machine-interface reporting	Interactive (human) access to IM Reporter Portal for small-scale reporting/corrections; status.
Plan Participant Reporting	All Reporting	N/A
Regulator Use	All Access	N/A

○ **What is the CAT Secure Reporter Gateway (SRG)?**

- Only for ***small scale***, manual reporting/corrections; status.
- IM uses existing Internet connectivity.
- User authenticates (MFA) to SRG; only authenticated traffic routed to Reporter Portal
- Communication occurs over VPN to SRG.

○ **Questions?**

- Connectivity Webinar, Thursday 8/29/19 at 10:30a.

Security Control Highlights

Authentication

- **Multi-factor Authentication (MFA) required**
  - Regulator/Query Tools
  - IM Reporter Portal
  - IM Secure Reporting Gateway
- **Two factors:**
  - Something you know: Username/Password
  - Something you have: Registered mobile device
- **Secure, state-of-the-art MFA approach**
  - E.g. “push authentication”
  - No deprecated technologies used (e.g. SMS codes)
  - Details forthcoming
- **Protects against**
  - Unauthorized access by Regulator insiders
  - Any interaction with the Reporter Portal, other than by authorized individuals.

Something You Know

+

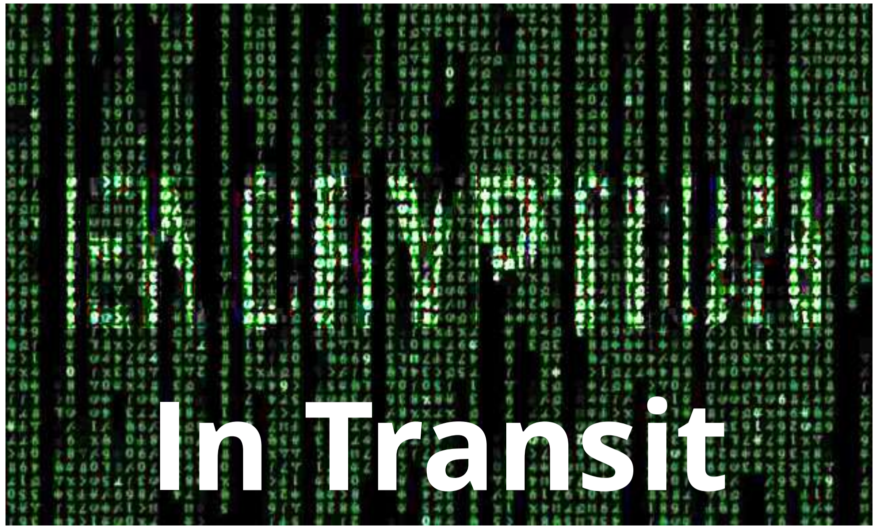
CAT Login App
Are you attempting to access CAT?
YES
NO

Something You Have

Security Control Highlights

Data Protection

At Rest



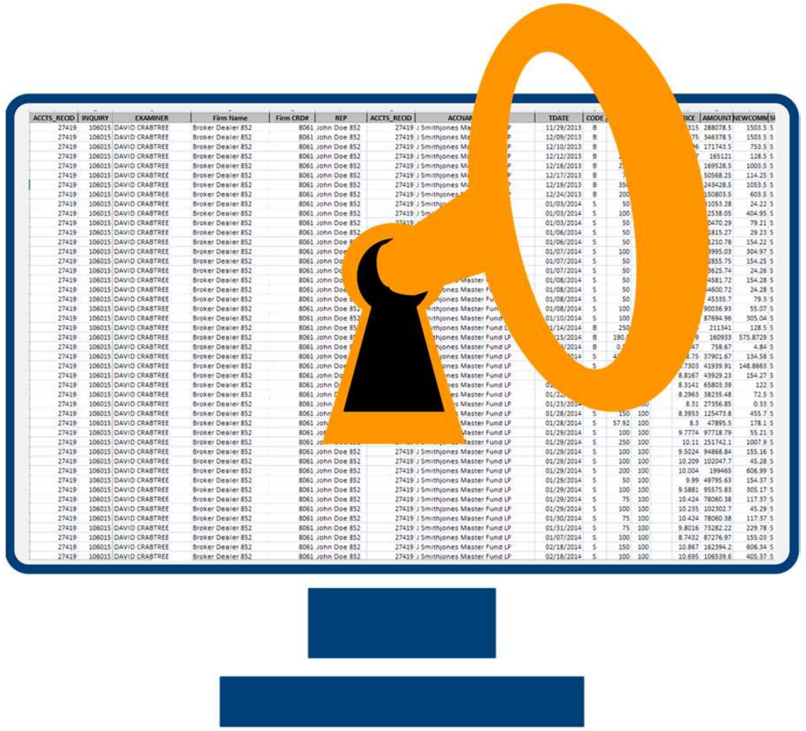
Pervasive Use of Encryption

Security Control Highlights

Targeted Monitoring

- **CAT-specialized Security Monitoring**
  - Explicit Plan requirements
  - Threat-determined requirements
- **Enabled by Threat, Detection, Monitoring, and Alerting Framework**
  - Extensive Component-level Logging
  - Security Tooling
  - Behavioral Analytics
- **Plan Requirements: Regulatory User Access and Monitoring**
  - Every instance of access to the Central Repository is logged
  - Full audit trail of Customer Data access is maintained
  - A list of authorized users and their most recent access is made available to the Operating Committee, the SEC, and Plan Participants
  - Each user organization will periodically verify their list of users is accurate, including the roles assigned to each user.

Closing



- **This presentation will be recorded and available on catnmsplan.com**
- **E-mail questions to FINRA CAT helpdesk: help@finracat.com**