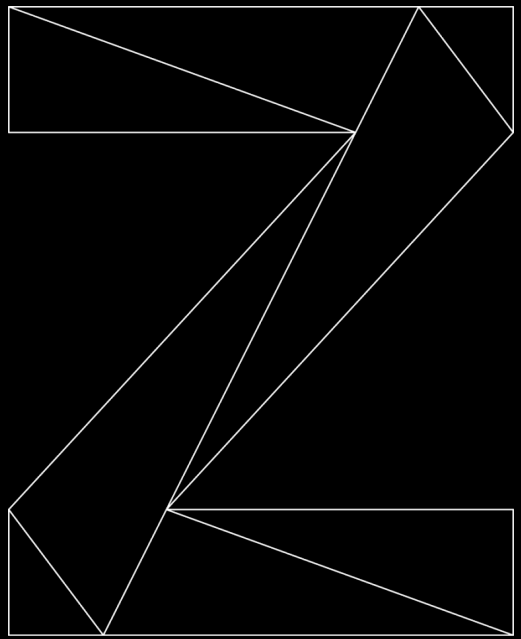
zCouncil

Security Trends & Directions

June 4, 2020

David Z Rossi
Cyber Security Architect
dzrossi@us.ibm.com

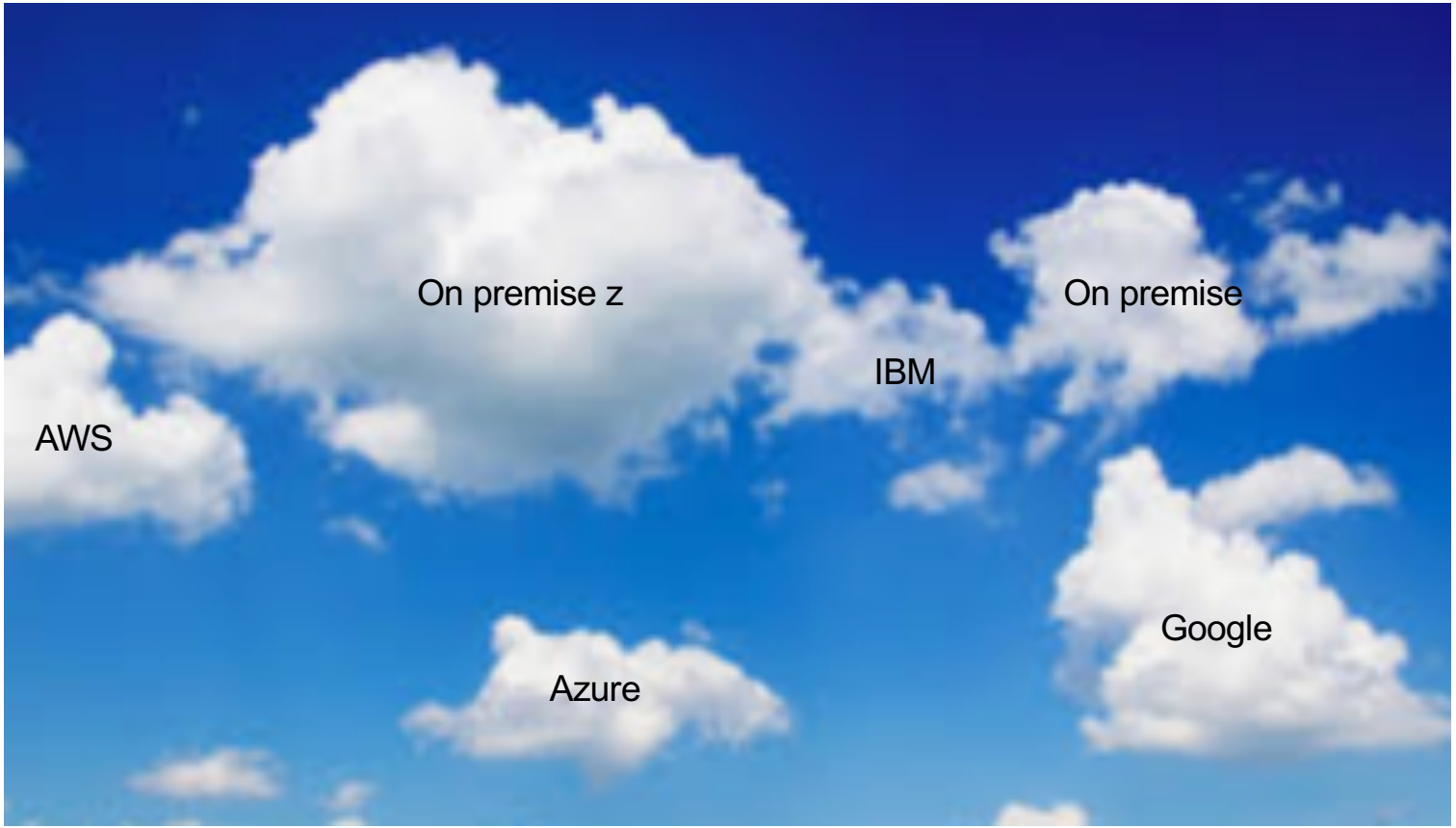


IBM

Agenda

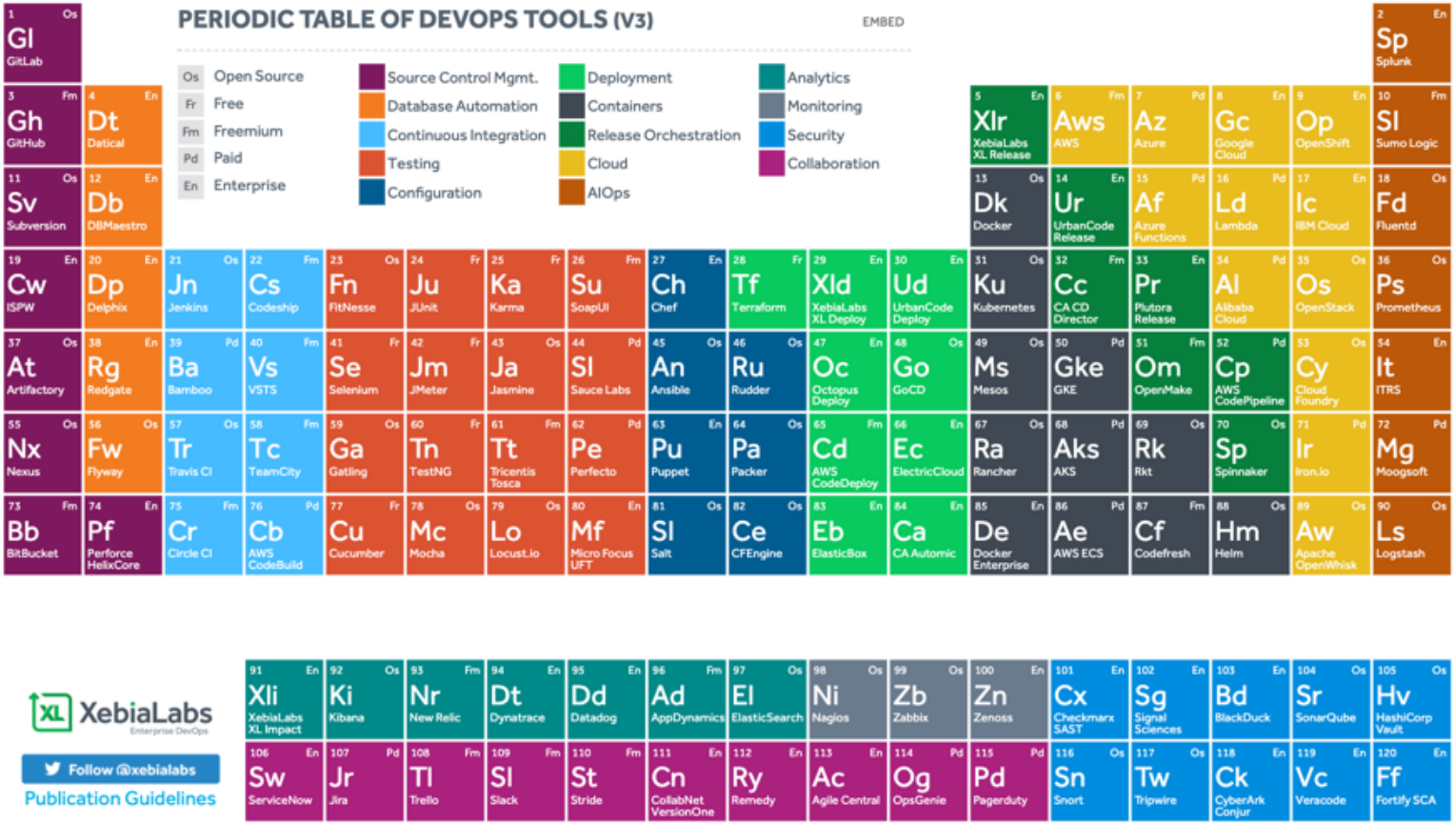
- Cloud Pak for Security
- Guardium Insights
- Data Privacy Passports
- EKMF-Web,
- MFA 2.1,
- zSecure 2.4

Cloud



XebiaLabs
Enterprise DevOps

From AGILE came DevOps which Enables Cloud



XebiaLabs
Enterprise DevOps

Follow @xebialabs

Publication Guidelines

Implications on Security

- New threats
- More fragmented

Driving “Hybrid View”

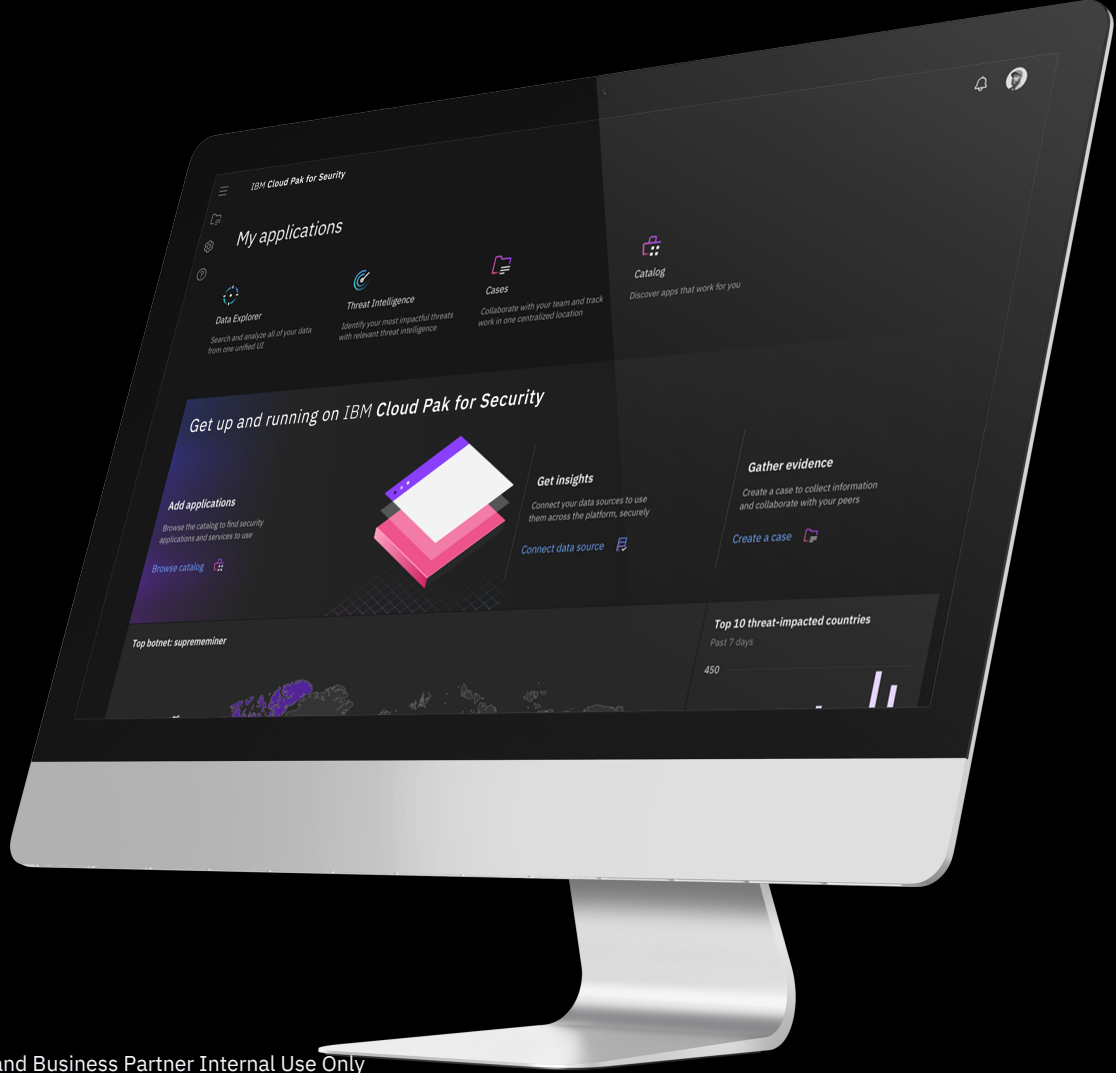
- new level of abstraction
- open and plugable

Clould Pak for Security (CP4S)

Introducing IBM Cloud Pak for Security

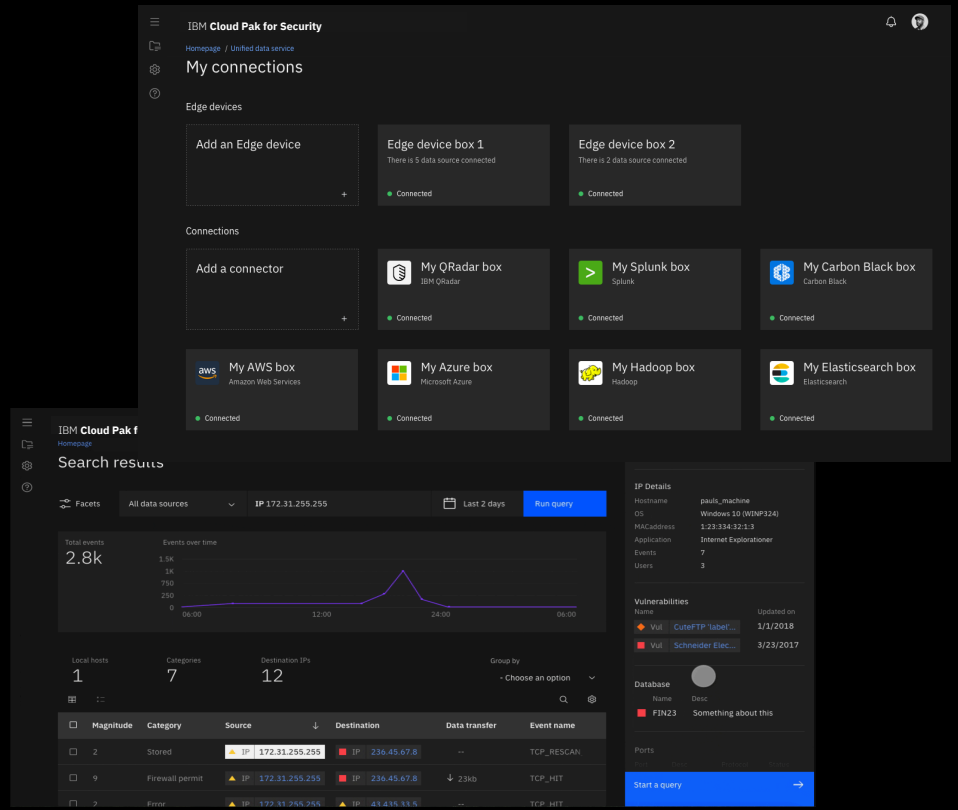
A platform to more quickly integrate your existing security tools to generate deeper insights into threats, orchestrate actions and automate responses—all while leaving your data where it is.

- Hybrid, multicloud architecture
- Connected, open ecosystem
- Automation & orchestration



Key Value

- Investigate faster with federated search across QRadar, Splunk, Elastic, AWS, Azure, Carbon Black, BigFix, Data Lake, McAfee and IBM Cloud
- Simplify work with a single investigation and search tool for a multi-hybrid cloud and MSSP environment
- Seamlessly track investigations with case management
- Respond faster and more thoroughly with robust orchestration and automation capabilities
- Deploy anywhere through hybrid, multicloud architecture
- Expand data sources and capabilities with SDK for partners and customers to create new connectors and apps



IBM Cloud Pak for Security - 2019

Run anywhere | Gain complete insights | Take action faster

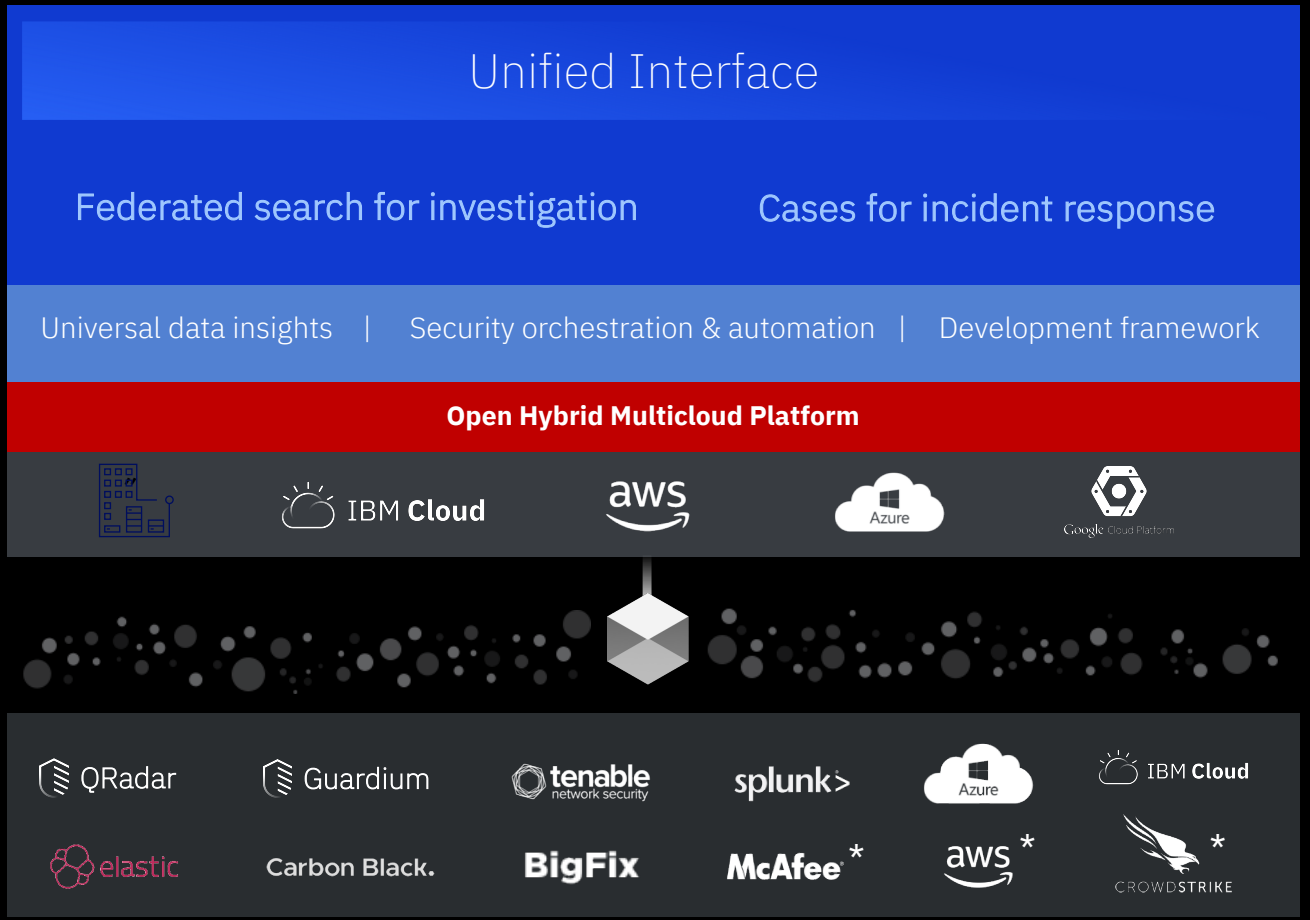
Cross-cutting security solutions

Core platform services

Hybrid multicloud architecture

Open integration with existing security tools

*Available post-GA



Guardium Insights

Guardium Insights vision – a unified and flexible data security & compliance solution

Data Security Hub

Deploy: On-premises or in the cloud

Big Data

Guardium Data Protection

DBaaS

Unstructured Cloud sources

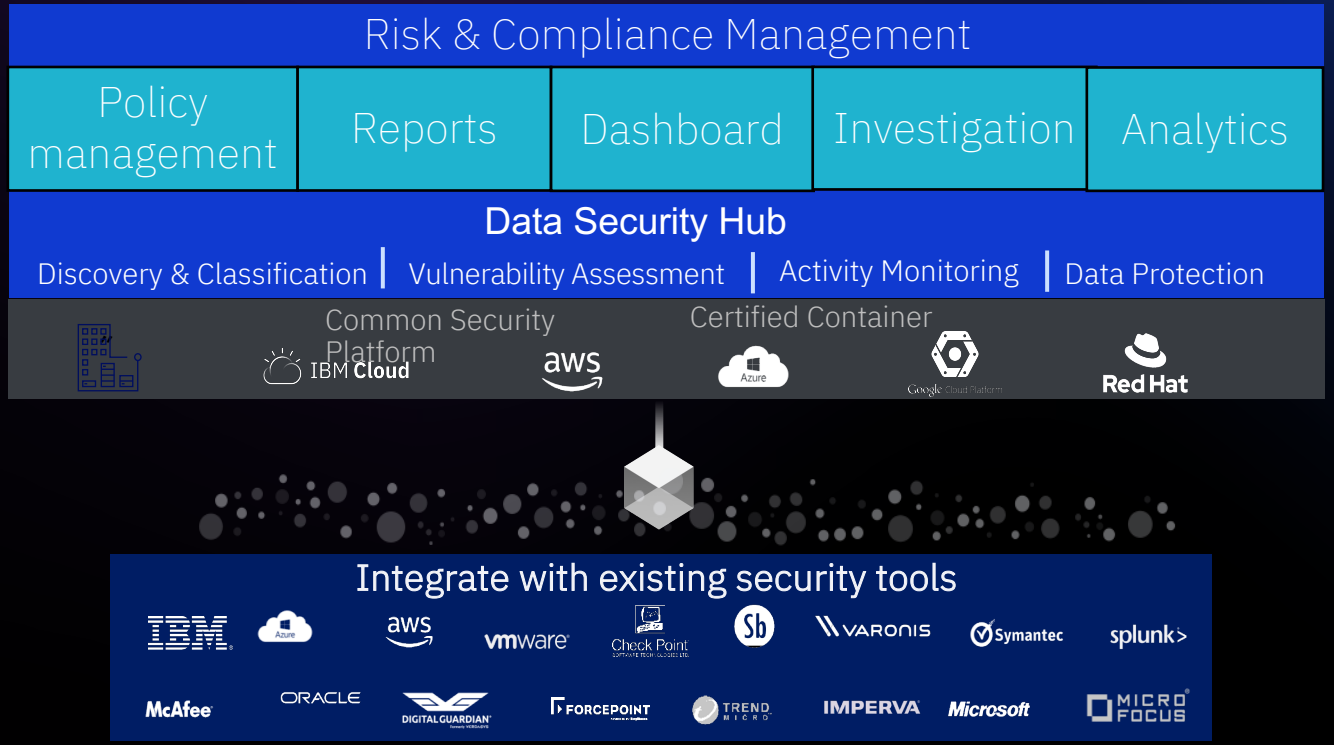
Smarter protection...

- Comprehensive data security & compliance visibility
- Risk-based scoring and alerts
- Predictive analytics with pattern recognition
- Centralized policy management

Faster action...

- Identify threats faster
- Assess risk across environments
- Proactively protect & respond to alerts
- Create & share consolidated reports
- Reduce unnecessary risk costs

Guardium vision: Data security that frees you to thrive in the age of cyber uncertainty



- ✓ Comprehensive visibility, control & threat hunting
- ✓ Meet long-term compliance requirements
- ✓ Open integration & enrichment
- ✓ Orchestrated response & policy management
- ✓ Risk insights, advanced analytics & automated response
- ✓ Reduce operational expense & streamline architecture
- ✓ Modernize & deploy on-premises, in public cloud or in private cloud

IBM **Security**

AWS Security Hub

IBM Z Security

Make the most securable platform the most secure

Strategy and Risk

- Threat Modeling
- Penetration Testing
- Vulnerability testing/tracking
- Security Assessments
  - » Standards
  - » Services
- Security Hygiene
  - » Continuous monitoring
  - » Reporting
  - » Maintenance

Digital Trust

- Data Protection
  - » Database monitoring
  - » Encryption
- Identity Management
  - » Lifecycle management
  - » PAM
- Advanced Authentication

Threat Management

- Automated Threat Detection
  - » Security event monitoring
  - » Security Intelligence platform
  - » CP4S
- Triage platform
- Incident response

Data Privacy Passports

Data Security

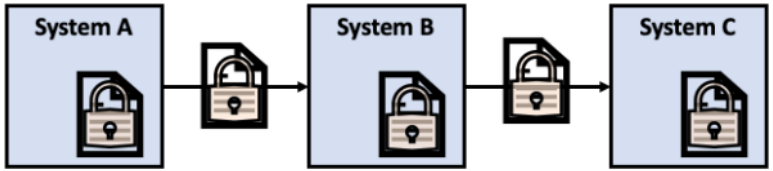
Data Privacy

Appropriate use of data

Data Centric Protection

point-to-point

Data is protected via encrypted network sessions.
Encryption & decryption occurs at each point as data traverses the network.
Any data stored at endpoints and intermediate points must be explicitly encrypted.



end-to-end

data itself is encrypted at the starting point and remains encrypted until it reaches the end point.
data stored at endpoints and intermediate points is implicitly encrypted and managed through centralized policy

Extending Pervasive Encryption value

e.g. TLS, AT-TLS, IPSec, SFTP, IBM MQ Advanced Message Security, IBM Connect:Direct Secure Plus, etc.

Smart, Secure Data Movement
Application transparent protection for data protected by IBM LinuxONE

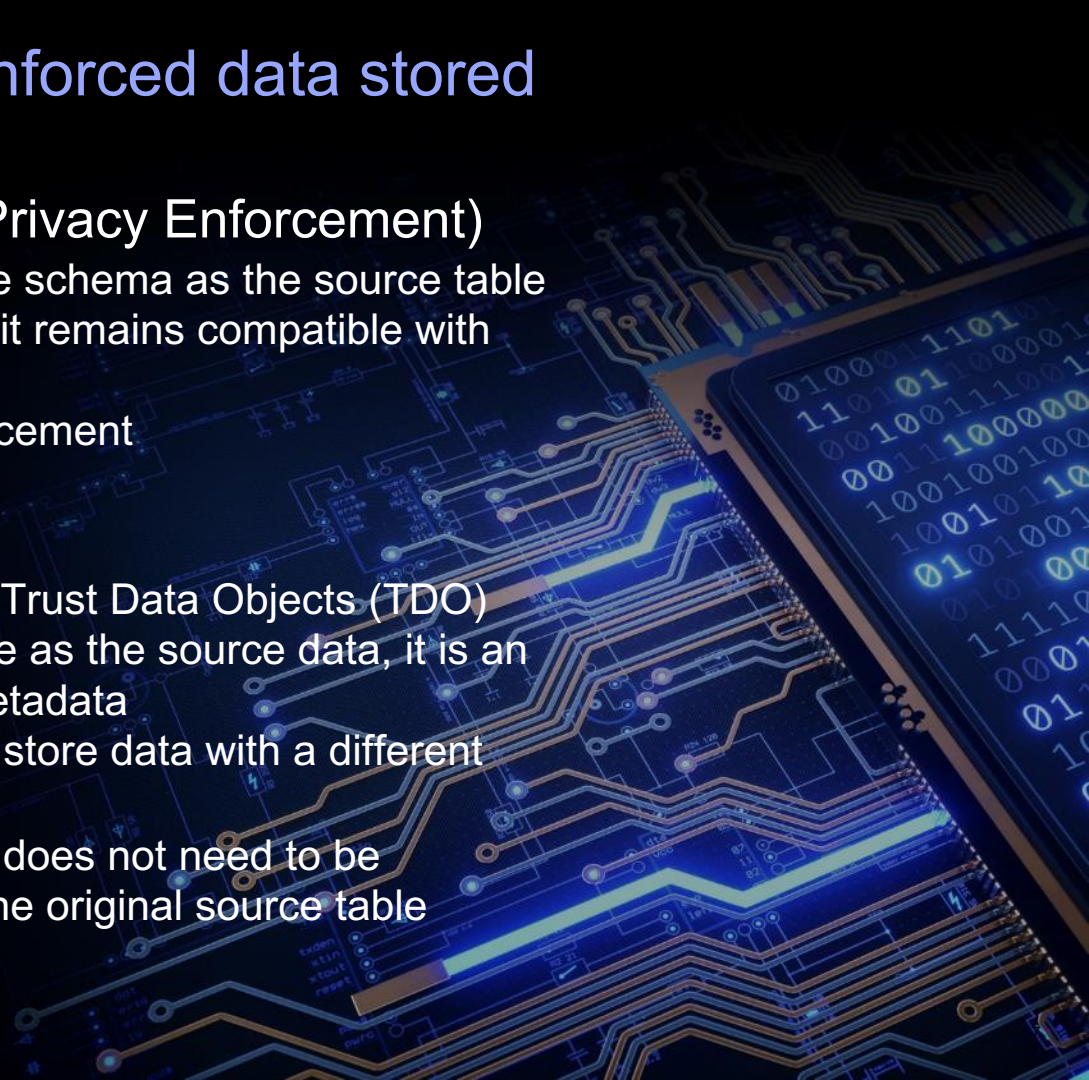
Where is the protected or enforced data stored

Enforced Data (Dynamic Data Privacy Enforcement)

- Can be stored in a table with the same schema as the source table
- Data can be enforced in a way where it remains compatible with the original source schema
- Easy for application transparent enforcement

Protected Data

- Data elements can be packaged into Trust Data Objects (TDO)
- The TDOs do not share the same size as the source data, it is an encrypted package with additional metadata
- The target tables needs to be able to store data with a different schema than the source table
- This table can be on any system and does not need to be managed by the same database as the original source table



Single source of protected data

IBM Data Privacy Passports enables clients to create a single, protected table, using a policy on IBM Z, that can grant multiple views of data from a single data source.

Data lake

Passport Controller

Data scientist

first_name	last_name	s_num	phone	zip_code
Brian	Acosta	999999999	669 707 2691	99999
William.	Adams	999999999	710 105 9538	99999
…	…	…	…	…

PHONE and ZIP_CODE values are unencrypted and displayed as a one-time masked value.

Data owner

first_name	last_name	s_num	phone	zip_code
Brian	Acosta	128967796	669 707 2691	94016
William.	Adams	409791779	710 105 9538	94131
…	…	…	…	…

All protected fields are unencrypted and displayed.

DPP Administrator

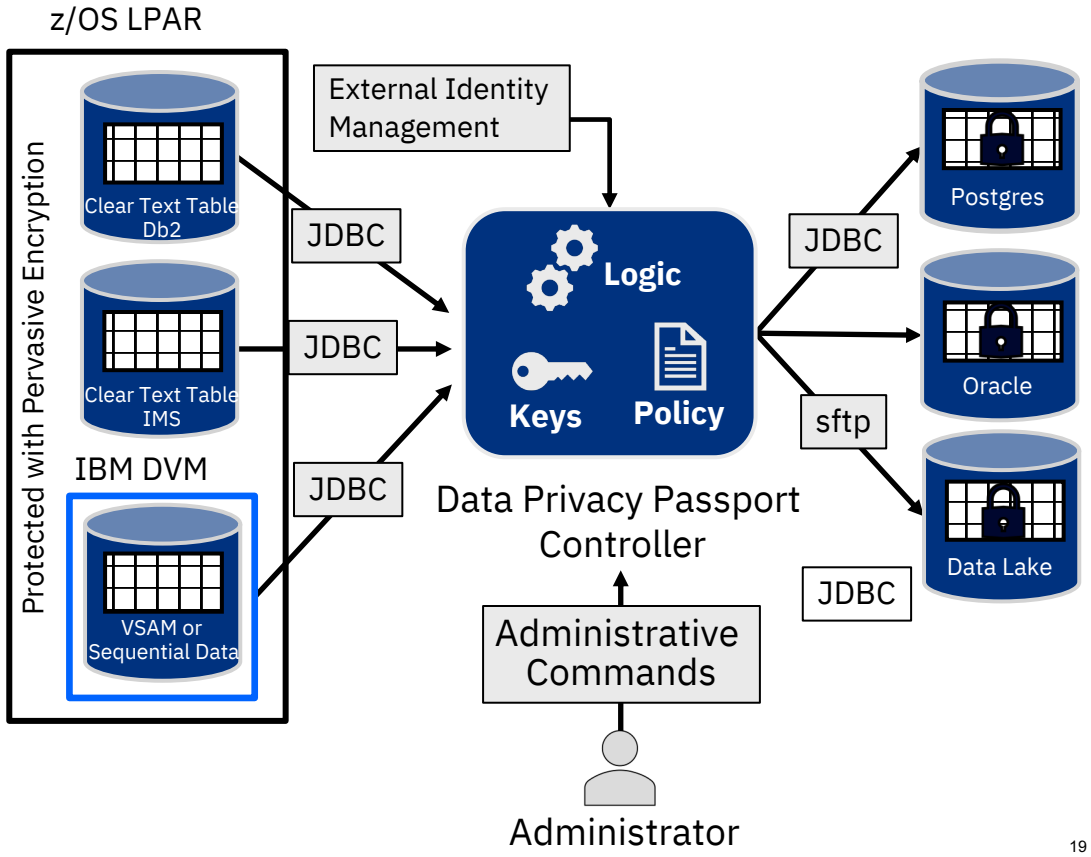
first_name	last_name	s_num	phone	zip_code
Brian	Acosta	999999999	999 999 9999	99999
William	Adams	999999999	999 999 9999	99999
…	…	…	…	…

PHONE and ZIP_CODE values are unencrypted and displayed as a one-time masked value and s_num is nullified.

Introducing IBM Data Privacy Passports

- The data is protected at the point of extraction and is enforced at the point of consumption
- Move data from IBM Z to distributed as Trusted Data Objects – Start with SQL data sources on IBM Z
- Passport Controller deployed in an SSC LPAR
- Policy for enforcement can be changed dynamically to revoke to entitle users to data
- **Create a single protected table to provide multiple views of data**

Only runs on IBM z15



Key Management with EKMF

Types of keys to consider

KEKs are keys that protect (e.g. encrypt, wrap) other keys

Datasets are Encrypted with Operational Keys which are protected by KEKs and Master Keys

Master Keys

Master keys are used only to encipher and decipher keys.

Master keys are stored in secure, tamper responding hardware.

Master key encrypted keys are considered secure keys.

Master keys should be changed periodically.

All master keys are optional. Secure keys are only supported when their associated master key is active.

Operational Keys

Operational keys are used in various cryptographic operations (e.g. encryption).

Operational keys may be stored in a key store (e.g. data set, file, database) or returned back to the caller.

Operational keys may be clear, secure or protected.

Symmetric KEKs

Encrypt symmetric keys with another symmetric key.

Asymmetric KEKs

Encrypt symmetric keys with RSA public keys

Use ECC key pairs to derive a symmetric key. Use the derived symmetric key to encrypt another symmetric key.

IBM Key Management tools

Integrated Cryptographic Services Facility (ICSF)

ICSF provides callable services and utilities that generate, store, and manage keys, and also perform cryptographic operations.

Supports Master Keys and Operational Keys

Trusted Key Entry (TKE) Workstation

TKE securely manages multiple Cryptographic Coprocessors and keys on various generations of IBM Z from a single point of control.

Supports Master Keys and Operational Keys

Enterprise Key Management Foundation (EKMF)

EKMF securely manages keys and certificates for cryptographic coprocessors, hardware security modules (HSM), cryptographic software, ATMs, and point of sale terminals.

Supports Operational Keys

Security Key Lifecycle Manager (SKLM)

SKLM v2.7 provides key storage, key serving and key lifecycle management for IBM and non-IBM storage solutions using the OASIS Key Management Interoperability Protocol (KMIP) and IBM Proprietary Protocol (IPP).

Supports Operational Keys for Self Encrypting Devices (SEDs)

EKMF Web for Pervasive Encryption on IBM Z

When implementing pervasive encryption it is very important that a **robust key management system** is in place.

IBM Enterprise Key Management Foundation (EKMF) has a proven record of meeting the key management requirements you find in large financial companies like banks and card processors.

IBM offers EKMF Web for Pervasive Encryption that helps you **manage the keys involved in dataset encryption**.

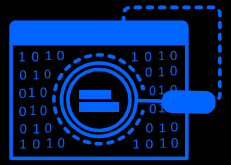
EKMF Web for PE features

Single central key repository

- Stores metadata (activation dates, usage, etc.)
- Single-point backup and recovery

Key Management

- On-demand generation based on policies
- According to NIST recommendations
- Using Hardware Security Modules (HSM)



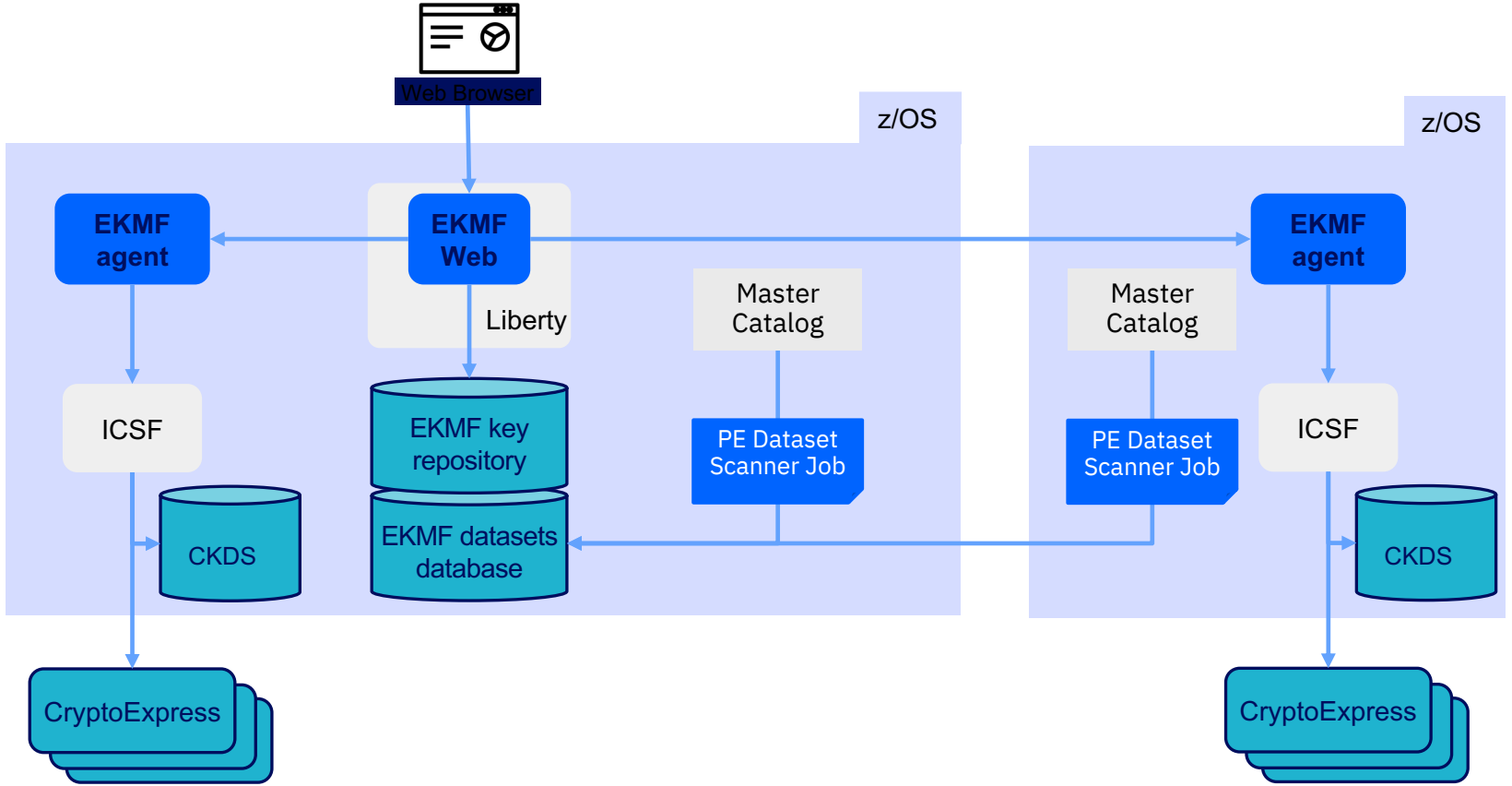
Pervasive Encryption Support

- Dataset dashboard
- Import and management of existing PE keys
- Central support for multiple z/OS systems

Security & Compliance

- Role-based access
- Dual control implemented using separation of privileges
- Audit logging

EKMF Web Architecture



MFA 2.1

IBM Z Multi-Factor Authentication

Raise the assurance level of critical applications, data, identities and hosting environments

Achieve regulatory compliance and meet best practices (PCI-DSS, DISA-STIG…)

Gain flexibility with support and integration for the broadest array of factors and vendors

Extend IBM RACF with no changes to authenticate users with multiple factors

Fast, **flexible**, deeply integrated, easy to deploy, manage and use

IBM Z Multi-Factor Authentication (5655-MA1)
IBM Z Multi-Factor Authentication S&S (5655-MA2)

What is multifactor authentication?

SOMETHING THAT YOU KNOW

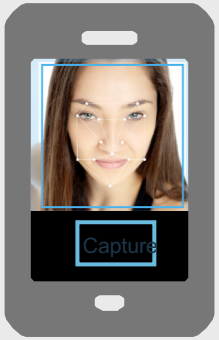
- Usernames and passwords
- PIN Code

SOMETHING THAT YOU HAVE

- ID Badge
- One time passwords
  - Time-based

SOMETHING THAT YOU ARE

- Biometrics



What works with IBM Z MFA?

In-Band

Proprietary Protocol: RSA

RADIUS Based Factors: IBM, yubico, Microsoft Azure, gemalto security to be free, DUO, RSA, callsign, ONE IDENTITY, Symantec. VIP, okta, VASCO TRUST FOR THE DIGITAL WORLD

TOTP Support: IBM, IBM, Google, FreeOTP, DUO Mobile, AUTHY, RAPIDIDENTITY OTP with RapidIdentity Mobile App

Out-of-Band

Certificate Authentication:

Password/Passphrase: RACF Password/Passphrase can be used in conjunction with all in-band authentication methods.

New Operating System – z/VM

- In addition to z/OS we now support z/VM
- Leverages Out-of-Band channel
- Most factors that are supported on z/OS will work on z/VM
- **One Solution – One License**
- Innovative Packaging
  - Order via ShopZ, get both operating systems
  - Pick and choose which one to install

Why is this important?

- z/VM is not exempt from MFA requirements
- IBM is the only vendor who can support both z/OS and z/VM with the same solution
- One vendor is more desirable
- Leverage existing MFA infrastructure

Protection beyond the z/OS Sysplex Boundary

- Support the production of secure credentials that can be used both within and beyond the boundary of the sysplex where the credential was generated.
- New factor AZFCKCTC

Why is this important?

- Most clients will be interested in cross sysplex support
- Simplifies MFA configurations in large environments

zSecure 2.4

What’s new in zSecure 2.4.0

- Command Ticket Logging
- File Integrity Monitoring
- z/OS 2.4 support
  - Custom data for general and dataset resource profiles
  - SMF Enhancements
  - Privilege escalation detection (new alert added)
- Compliance
  - Show differences (progress or regression?)
  - Compliance ACF2 252/357 circa 70%, new report type ACF2_SENSRESOURCE_ACCESS
  - STIG Currency
  - More IMS security settings made available, including OTMA
- QRadar events ICSF statistics, MFA audit trail (83-7)

Command and Ticket Logging

- What is it?
  - New feature in zSecure Admin.
  - Provides a mechanism for administrators to record the approval record associated with a given change.

- Client Value
  - Auditors will ask “What was the change request number?”. Prior to this support it was a manual process to get the answer, if they could at all.
  - With this support, very easy to provide the answer.

- Also available in 2.3.1 – PTFs UA99126,UA99127,UA99128

File Integrity Monitoring

- What is it?
  - New feature in zSecure.
  - Provides a mechanism to show administrators and auditors if a file has been changed or tampered with.

- Client Value
  - Intrusion detection
  - Integrity validation
  - Several regulations benefit from FIM for compliance!
    - PCI-DSS
      - 10.5.5: data log integrity
      - 11.5: critical file comparison
    - HIPAA
    - GDPR

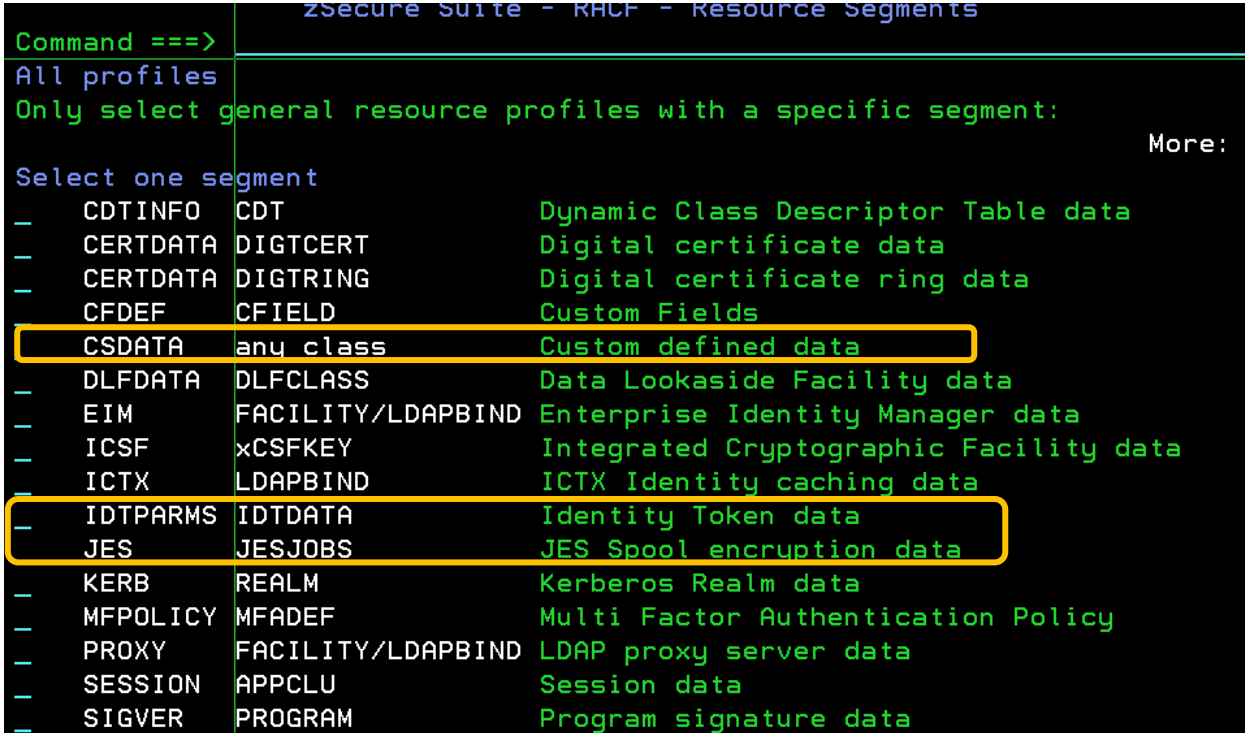
RACF 2.4 has new general resource segments

Select on presence, absence, display of 3 new general resource segment types:

CSDATA
adds custom data fields

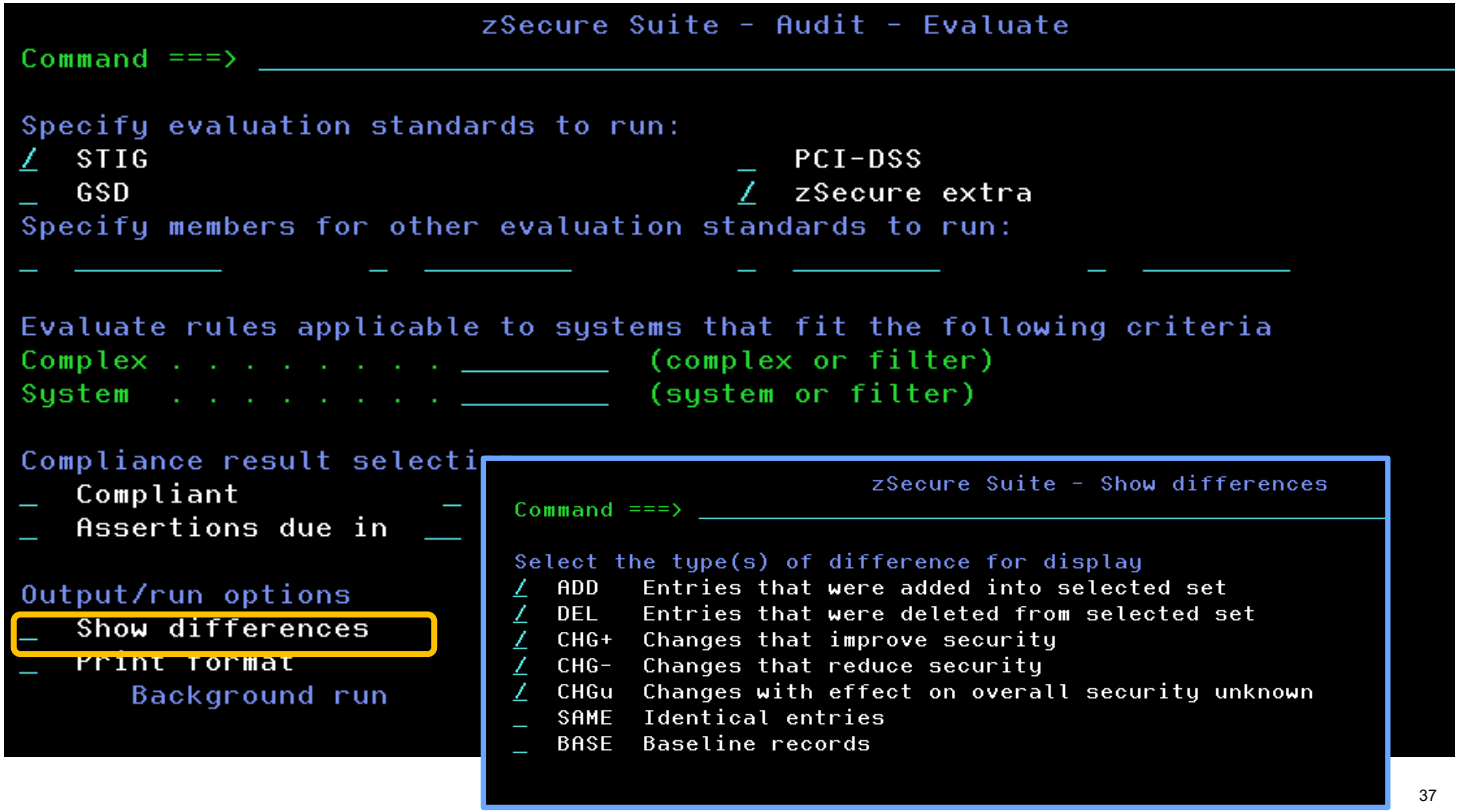
IDTPARMS
defines how to authenticate identity tokens

JES
defines how to encrypt JES spool – *for future use*



AU.R enhancement - comparison

TYPE=COMPLIANCE* newlist types have been enhanced to support comparison



SMF Enhancements

Success logging now includes CRITERIA

– Field RECORDDESC extended:

RACF ACCESS success for CRMBJU1: (READ,READ) with criteria SMS=DSENCRYPTION on CSFKEYS ZSECKEY8

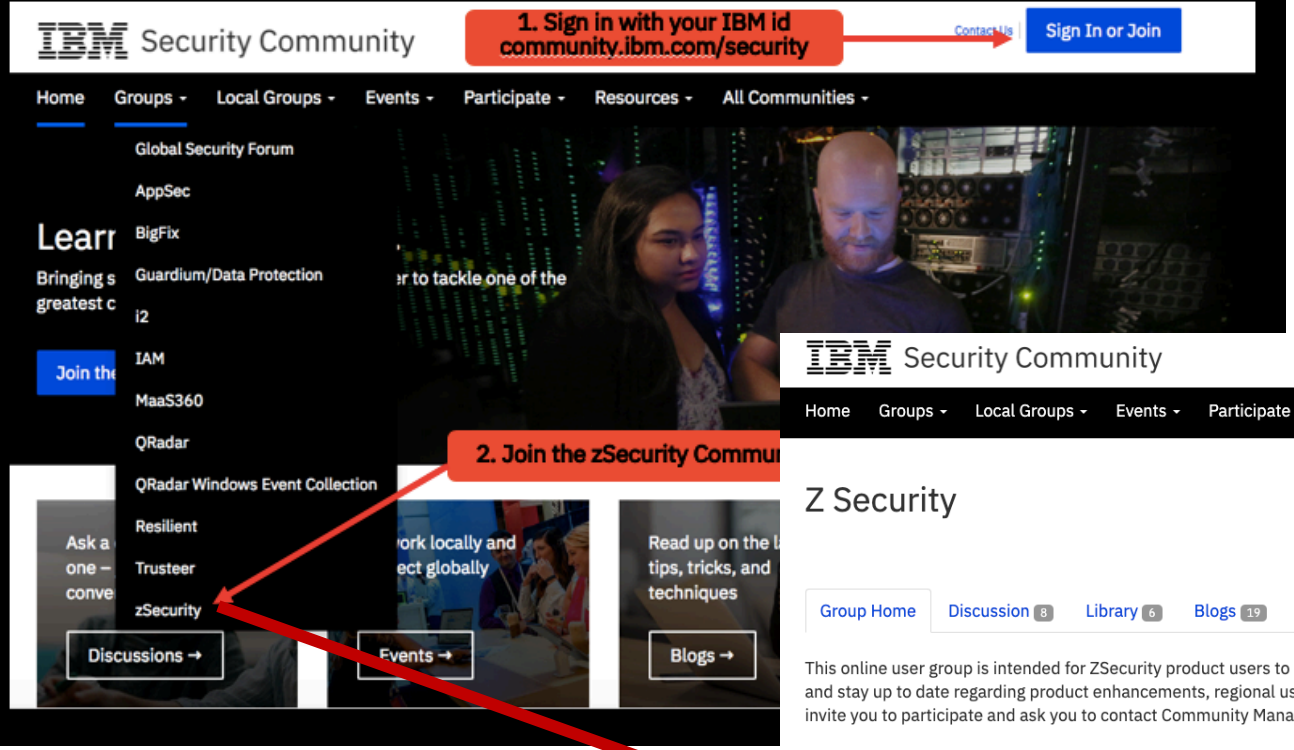
- New TYPE=SMF field CRITERIA shown with default prefix header:

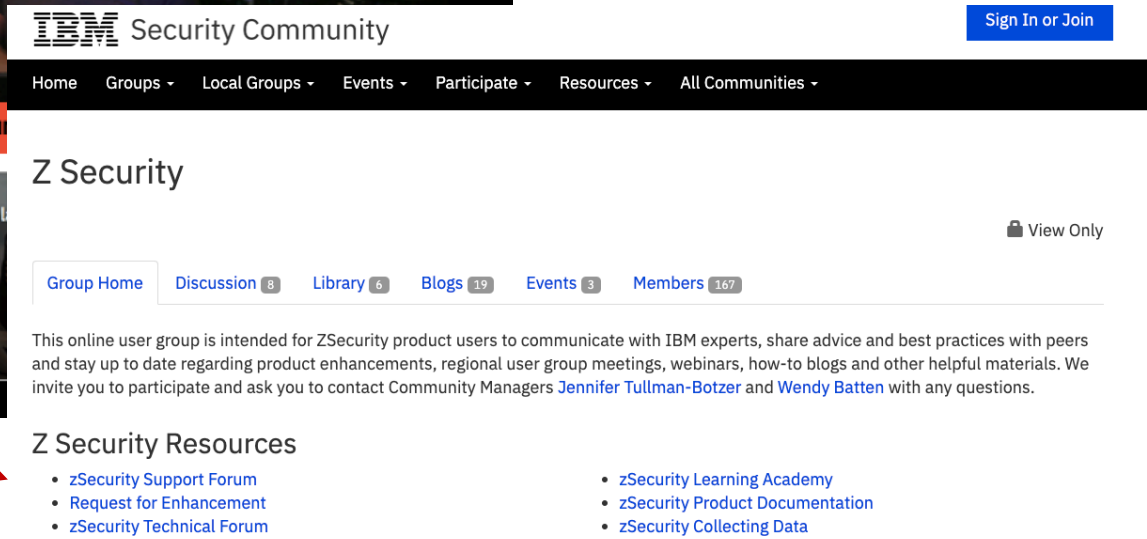
Criteria condition satisfied SMS=DSENCRYPTION

More ICSF record detail

SMF 83-7 MFA record

– New TYPE=SMF fields MFA_FACTOR, MFA_POLICY, populate 5 fields





https://community.ibm.com/community/user/security/communities/community-home?CommunityKey=44eb7c0d-9bc2-419b-9158-ad693e734065

Announcement Letters

zSecure 2.4 July 23th 2019
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=an&subtype=ca&appname=gpateam&supplier=649&letternum=ENUSA19-0557

Guardium Insights Nov 5th 2019
https://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/5/897/ENUS219-485/index.html&request_locale=en

Cloud Pak for Security Nov 12th 2019
https://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/3/897/ENUS219-133/index.html&lang=en&request_locale=en

Data Privacy Passport March 10th 2020
https://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/2/897/ENUS220-062/index.html&request_locale=en

EKMF Web April 7th 2020
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=an&subtype=ca&appname=gpateam&supplier=897&letternum=ENUS220-108

MFA 2.1 May 19th 2020
https://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/9/877/ENUSZP20-0209/index.html&lang=en&request_locale=en

Thank you

David Rossi
IBM z CyberSecurity Archtiect
—
dzrossi@us.ibm.com
908 347 8094