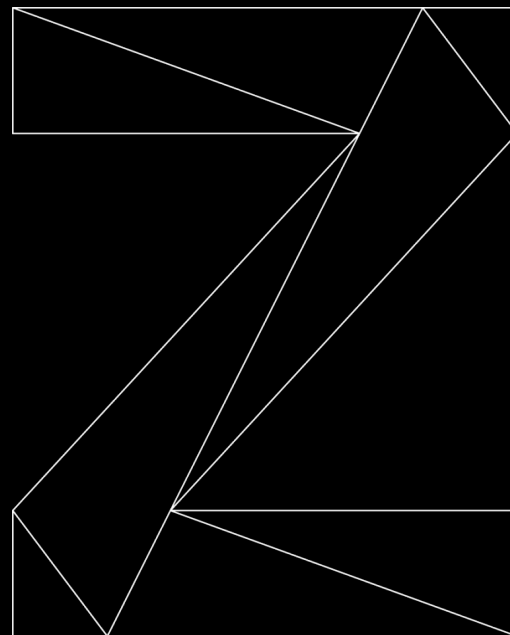


zCouncil

## Security Trends & Directions

June 4, 2020

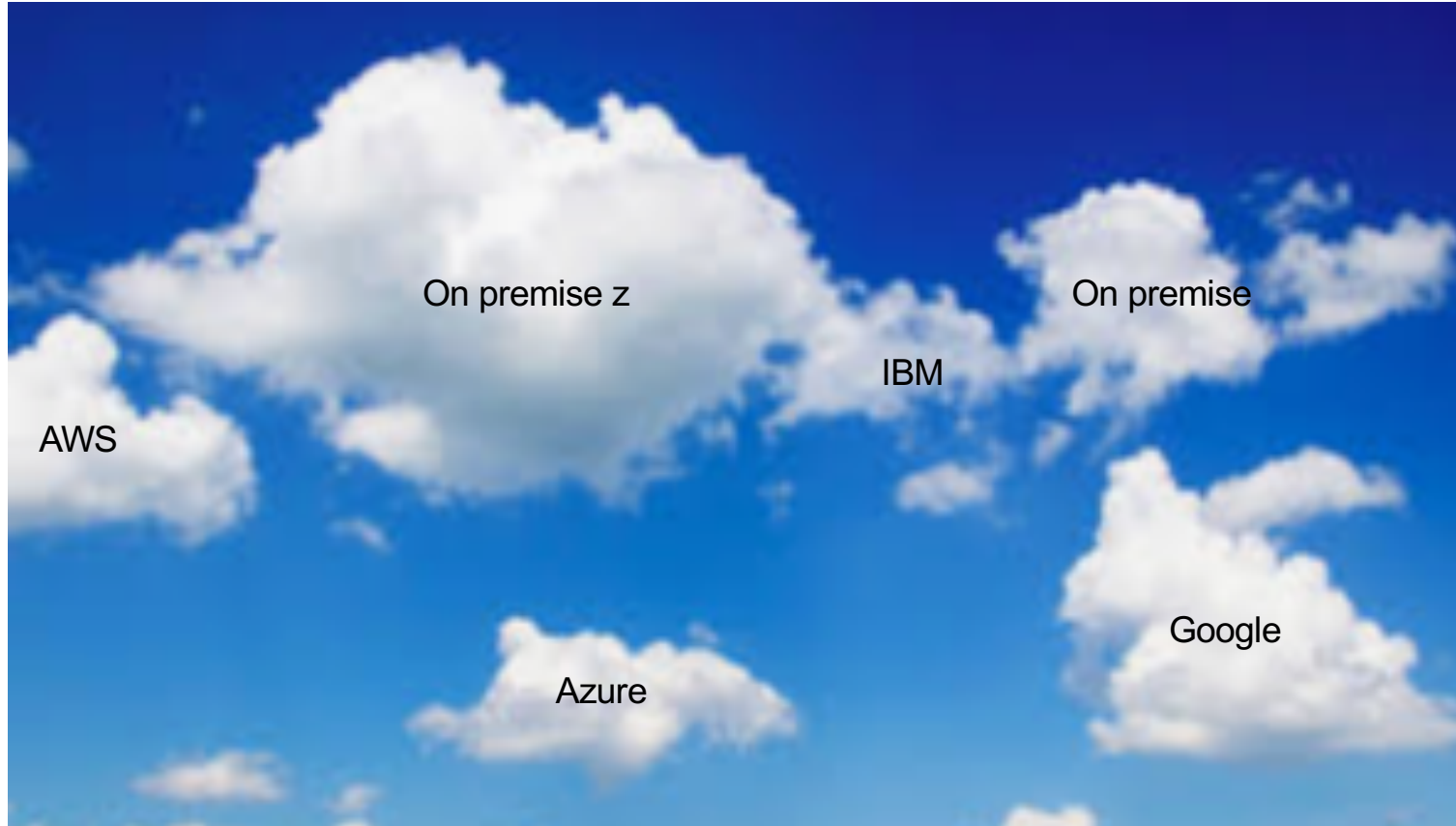
David Z Rossi  
Cyber Security Architect  
[dzrossi@us.ibm.com](mailto:dzrossi@us.ibm.com)



# Agenda

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

# Cloud



# From AGILE came DevOps which Enables Cloud

**PERIODIC TABLE OF DEVOPS TOOLS (V3)**

EMBED

1 Os <b>GI</b> GitLab																													2 En <b>Sp</b> Splunk
3 Fm <b>Gh</b> GitHub	4 En <b>Dt</b> Datadog																												
11 Os <b>Sv</b> Subversion	12 En <b>Db</b> DBMaestro																												
19 En <b>Cw</b> ISPW	20 En <b>Dp</b> Delphix	21 Os <b>Jn</b> Jenkins	22 Fm <b>Cs</b> Codeship	23 Os <b>Fn</b> FitNesse	24 Fr <b>Ju</b> JUnit	25 Fr <b>Ka</b> Karma	26 Fm <b>Su</b> SoapUI	27 En <b>Ch</b> Chef	28 Fr <b>Tf</b> Terraform	29 En <b>Xld</b> XebiaLabs XL Deploy	30 En <b>Ud</b> UrbanCode Deploy	31 Os <b>Ku</b> Kubernetes	32 Fm <b>Cc</b> CA CD Director	33 En <b>Pr</b> Plutora Release	34 Pd <b>Al</b> Alibaba Cloud	35 Os <b>Os</b> OpenStack	36 Os <b>Ps</b> Prometheus	5 En <b>Xlr</b> XebiaLabs XL Release	6 Fm <b>Aws</b> AWS	7 Pd <b>Az</b> Azure	8 En <b>Gc</b> Google Cloud	9 En <b>Op</b> OpenShift	10 Fm <b>Sl</b> Sumo Logic	13 Os <b>Dk</b> Docker	14 En <b>Ur</b> UrbanCode Release	15 Pd <b>Af</b> Azure Functions	16 Pd <b>Ld</b> Lambda	17 En <b>Ic</b> IBM Cloud	18 Os <b>Fd</b> Fluentd
37 Os <b>At</b> Artifactory	38 En <b>Rg</b> Redgate	39 Pd <b>Ba</b> Bamboo	40 Fm <b>Vs</b> VSTS	41 Fr <b>Se</b> Selenium	42 Fr <b>Jm</b> JMeter	43 Os <b>Ja</b> Jasmine	44 Pd <b>Sl</b> Sauce Labs	45 Os <b>An</b> Ansible	46 Os <b>Ru</b> Rudder	47 En <b>Oc</b> Octopus Deploy	48 Os <b>Go</b> GoCD	49 Os <b>Ms</b> Mesos	50 Pd <b>Gke</b> GKE	51 Fm <b>Om</b> OpenMake	52 Pd <b>Cp</b> AWS CodePipeline	53 Os <b>Cy</b> Cloud Foundry	54 En <b>It</b> ITRS												
55 Os <b>Nx</b> Nexus	56 Os <b>Fw</b> Flyway	57 Os <b>Tr</b> Travis CI	58 Fm <b>Tc</b> TeamCity	59 Os <b>Ga</b> Gatling	60 Fr <b>Tn</b> TestNG	61 Fm <b>Tt</b> Tricentis Tosca	62 Pd <b>Pe</b> Perfecto	63 En <b>Pu</b> Puppet	64 Os <b>Pa</b> Packer	65 Fm <b>Cd</b> AWS CodeDeploy	66 En <b>Ec</b> ElectricCloud	67 Os <b>Ra</b> Rancher	68 Pd <b>Aks</b> AKS	69 Os <b>Rk</b> Rkt	70 Os <b>Sp</b> Spinnaker	71 Os <b>Ir</b> Iron.io	72 Pd <b>Mg</b> Moogsoft												
73 Fm <b>Bb</b> BitBucket	74 En <b>Pf</b> Perforce HelixCore	75 Fm <b>Cr</b> Circle CI	76 Pd <b>Cb</b> AWS CodeBuild	77 Fr <b>Cu</b> Cucumber	78 Os <b>Mc</b> Mocha	79 Os <b>Lo</b> Locust.io	80 En <b>Mf</b> Micro Focus UFT	81 Os <b>Sl</b> Salt	82 Os <b>Ce</b> CFEngine	83 En <b>Eb</b> ElasticBox	84 En <b>Ca</b> CA Automtic	85 En <b>De</b> Docker Enterprise	86 Pd <b>Ae</b> AWS ECS	87 Fm <b>Cf</b> Codefresh	88 Os <b>Hm</b> Helm	89 Os <b>Aw</b> Apache OpenWhisk	90 Os <b>Ls</b> Logstash												

Os	Open Source	Source Control Mgmt.	Deployment	Analytics
Fr	Free	Database Automation	Containers	Monitoring
Fm	Freemium	Continuous Integration	Release Orchestration	Security
Pd	Paid	Testing	Cloud	Collaboration
En	Enterprise	Configuration	AIOps	

91 En <b>Xli</b> XebiaLabs XL Impact	92 Os <b>Ki</b> Kibana	93 Fm <b>Nr</b> New Relic	94 En <b>Dt</b> Dynatrace	95 En <b>Dd</b> Datadog	96 Fm <b>Ad</b> AppDynamics	97 Os <b>El</b> ElasticSearch	98 Os <b>Ni</b> Nagios	99 Os <b>Zb</b> Zabbix	100 En <b>Zn</b> Zenoss	101 En <b>Cx</b> Checkmarx SAST	102 En <b>Sg</b> Signal Sciences	103 En <b>Bd</b> BlackDuck	104 Os <b>Sr</b> SonarQube	105 Os <b>Hv</b> HashiCorp Vault
106 En <b>Sw</b> ServiceNow	107 Pd <b>Jr</b> Jira	108 Fm <b>Tl</b> Trello	109 Fm <b>Sl</b> Slack	110 Fm <b>St</b> Stride	111 En <b>Cn</b> CollabNet VersionOne	112 En <b>Ry</b> Remedy	113 En <b>Ac</b> Agile Central	114 Pd <b>Og</b> OpsGenie	115 Pd <b>Pd</b> Pagerduty	116 Os <b>Sn</b> Snort	117 Os <b>Tw</b> Tripwire	118 En <b>Ck</b> CyberArk Conjur	119 En <b>Vc</b> Veracode	120 En <b>Ff</b> Fortify SCA

## Implications on Security

- New threats
- More fragmented

## Driving “Hybrid View”

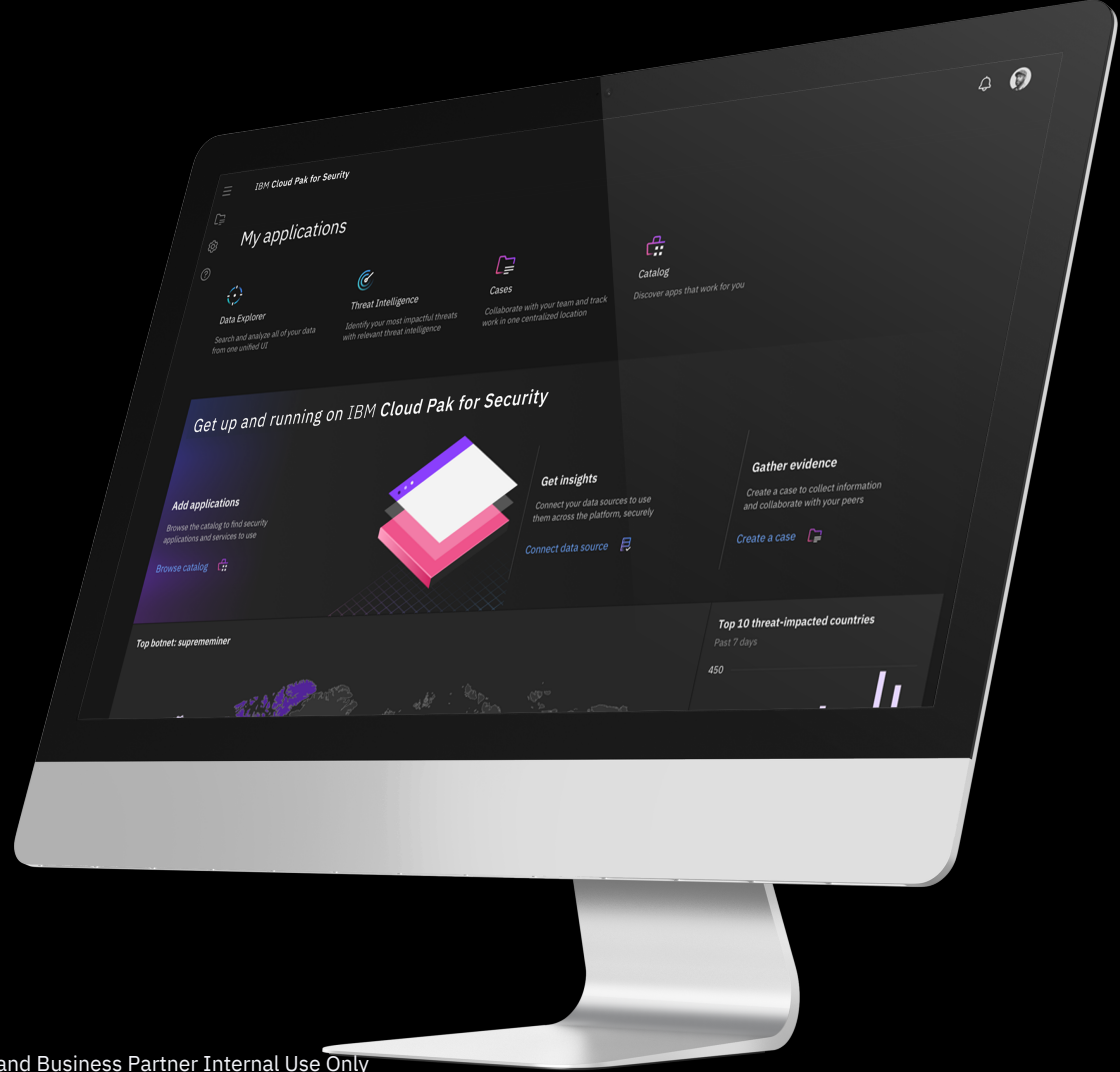
- new level of abstraction
- open and plugable

# Cloud 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

The screenshot displays the IBM Cloud Pak for Security interface. The top section, 'My connections', shows a grid of connected data sources including Edge devices, My QRadar box, My Splunk box, My Carbon Black box, My AWS box, My Azure box, My Hadoop box, and My Elasticsearch box. The bottom section, 'Search results', shows a search query for IP 172.31.255.255 over the last 2 days. It includes a line graph of 'Events over time' showing a peak at 24:00, and a table of search results with columns for Magnitude, Category, Source, Destination, Data transfer, and Event name.

Magnitude	Category	Source	Destination	Data transfer	Event name
2	Stored	IP: 172.31.255.255	IP: 236.45.67.8	--	TCP_RESET
9	Firewall permit	IP: 172.31.255.255	IP: 236.45.67.8	↓ 23kb	TCP_HIT
2	Firewall	IP: 172.31.255.255	IP: 43.435.33.4	--	TCP_HIT



# IBM Cloud Pak for Security - 2019

Cross-cutting security solutions

Core platform services

Hybrid multicloud architecture

Open integration with existing security tools

*\*Available post-GA*

Run anywhere

Gain complete insights

Take action faster

Unified Interface

Federated search for investigation

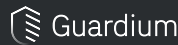
Cases for incident response

Universal data insights

Security orchestration & automation

Development framework

Open Hybrid Multicloud Platform



IBM and Business Partner Internal Use Only

# Guardium Insights

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



## Data Security Hub

*Deploy: On-premises or in the cloud*



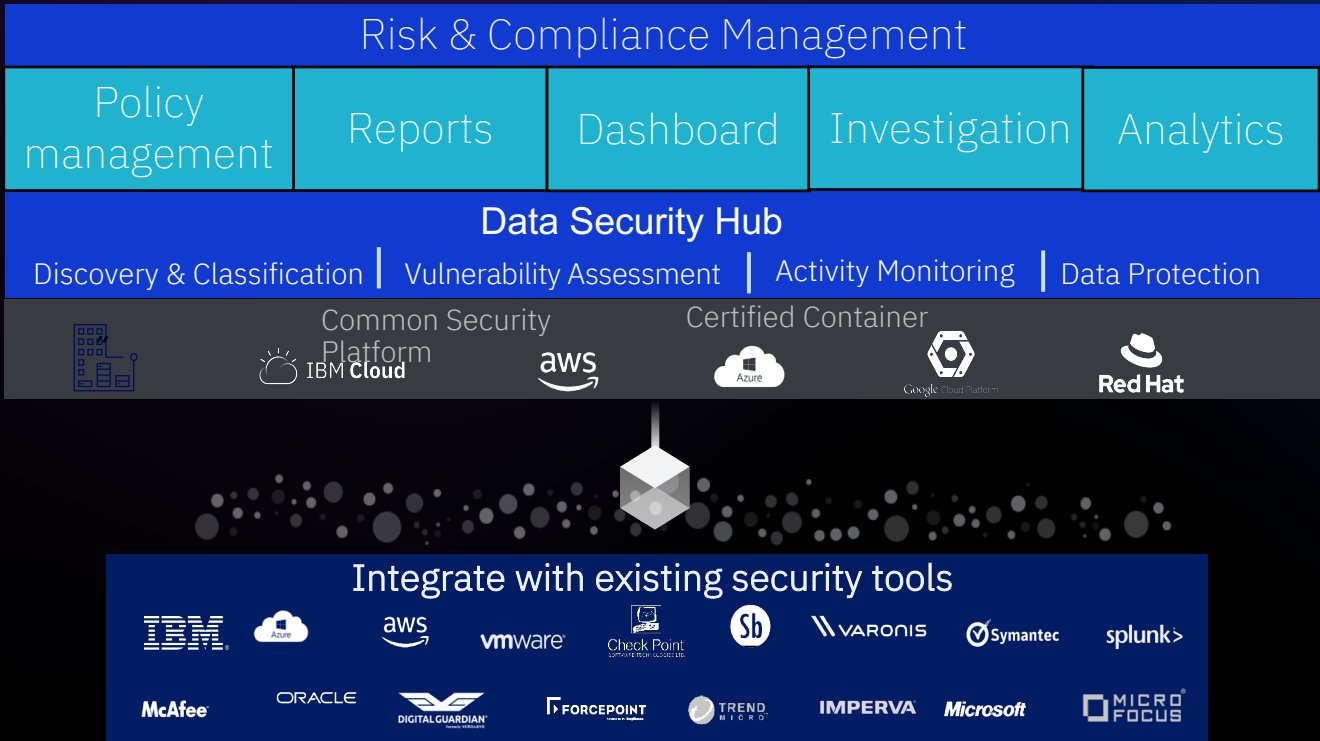
## Smarter protection...

- 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



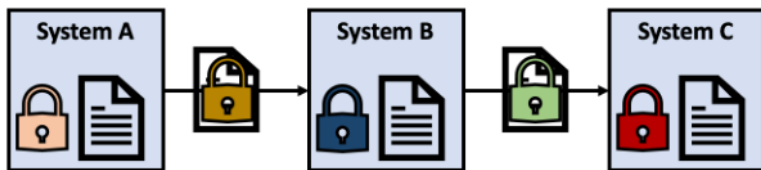
## Threat Management

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

# Data Privacy Passports

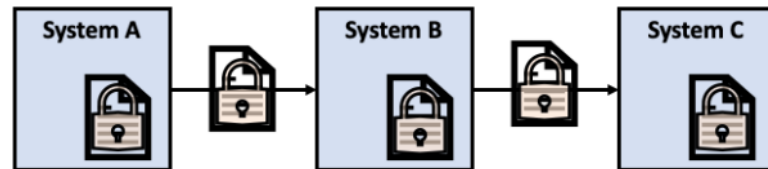


# Data Centric Protection



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
...	...	...	...	...

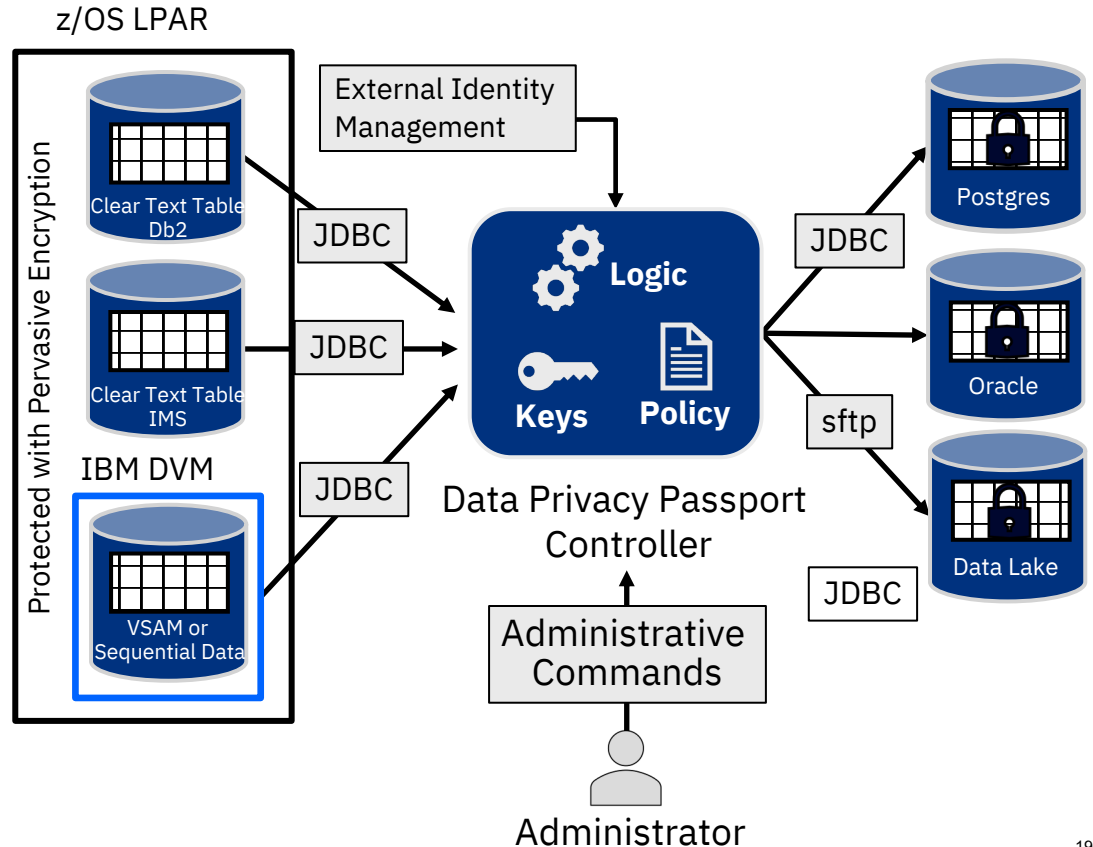


PHONE and ZIP\_CODE values are unencrypted and displayed as a one-time masked value and s\_num is nullified.

# 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 or 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



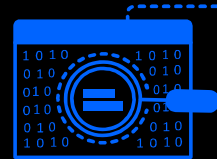
## Single central key repository

- 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

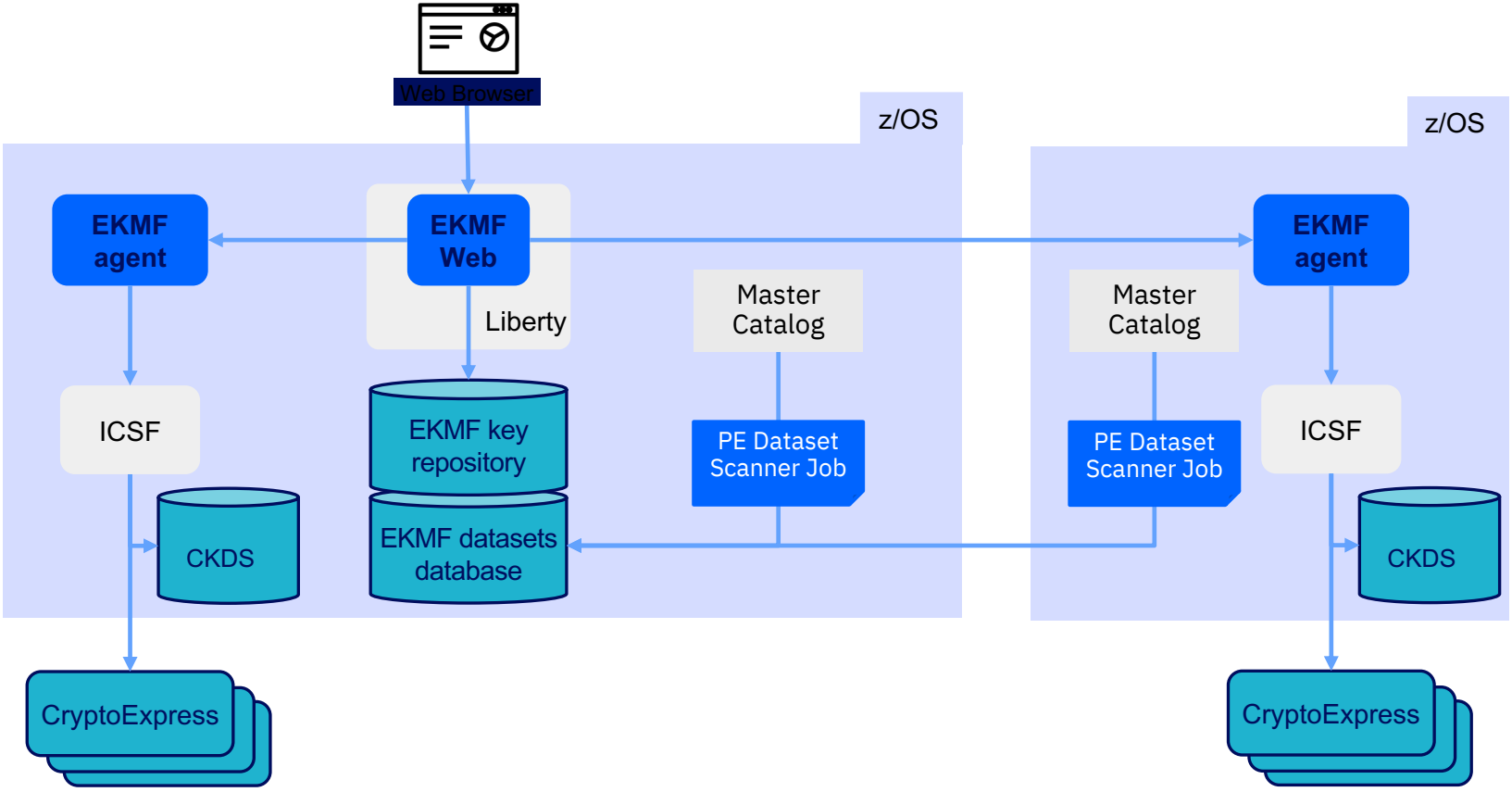


## Security & Compliance

- 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

# What is multifactor authentication?

## SOMETHING THAT YOU KNOW

- Usernames and passwords
- PIN Code



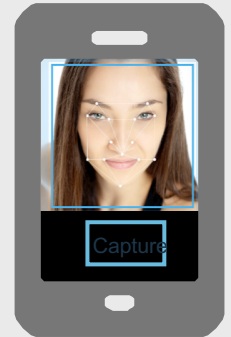
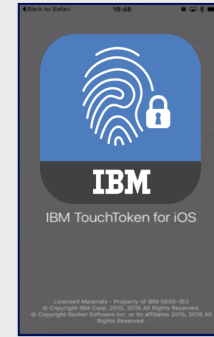
## SOMETHING THAT YOU HAVE

- ID Badge
- One time passwords
- Time-based



## SOMETHING THAT YOU ARE

- Biometrics



# What works with IBM Z MFA?

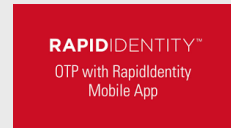
Proprietary Protocol:



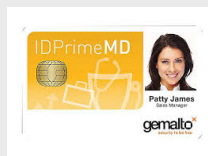
RADIUS Based Factors:



TOTP Support:



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*

zSecure Suite - RACF - Resource Segments		
Command ==>		
All profiles		
Only select general resource profiles with a specific segment:		
More:		
Select one segment		
—	CDTINFO	CDT Dynamic Class Descriptor Table data
—	CERTDATA	DIGTCERT Digital certificate data
—	CERTDATA	DIGTRING Digital certificate ring data
—	CFDEF	CFIELD Custom Fields
—	CSDATA	any class Custom defined data
—	DLFDATA	DLFCLASS Data Lookaside Facility data
—	EIM	FACILITY/LDAPBIND Enterprise Identity Manager data
—	ICSF	xCSFKEY Integrated Cryptographic Facility data
—	ICTX	LDAPBIND ICTX Identity caching data
—	IDTPARMS	IDTDATA Identity Token data
—	JES	JESJOBS JES Spool encryption data
—	KERB	REALM Kerberos Realm data
—	MFPOLICY	MFADEF Multi Factor Authentication Policy
—	PROXY	FACILITY/LDAPBIND LDAP proxy server data
—	SESSION	APPCLU Session data
—	SIGVER	PROGRAM Program signature data

# AU.R enhancement - comparison

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

```
zSecure Suite - Audit - Evaluate
Command ==> _____

Specify evaluation standards to run:
/ STIG          _ PCI-DSS
_ GSD           / zSecure extra
Specify members for other evaluation standards to run:
_ _____ _ _____ _ _____ _ _____

Evaluate rules applicable to systems that fit the following criteria
Complex . . . . . _____ (complex or filter)
System  . . . . . _____ (system or filter)

Compliance result selection
_ Compliant          _
_ Assertions due in  _

Output/run options
_ Show differences
_ Print format
_ Background run

zSecure Suite - Show differences
Command ==> _____

Select the type(s) of difference for display
/ ADD  Entries that were added into selected set
/ DEL  Entries that were deleted from selected set
/ CHG+ Changes that improve security
/ CHG- Changes that reduce security
/ CHGu Changes with effect on overall security unknown
_ SAME Identical entries
_ BASE Baseline records
```

# 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

Global Security Forum

AppSec

BigFix

Guardium/Data Protection

i2

IAM

MaaS360

QRadar

QRadar Windows Event Collection

Resilient

Trusteer

zSecurity

Discussions →

Events →

Blogs →

2. Join the zSecurity Community

# Z Security

View Only

Group Home Discussion 8 Library 6 Blogs 19 Events 3 Members 167

This online user group is intended for ZSecurity product users to communicate with IBM experts, share advice and best practices with peers and stay up to date regarding product enhancements, regional user group meetings, webinars, how-to blogs and other helpful materials. We invite you to participate and ask you to contact Community Managers [Jennifer Tullman-Botzer](#) and [Wendy Batten](#) with any questions.

## Z Security Resources

- [zSecurity Support Forum](#)
- [Request for Enhancement](#)
- [zSecurity Technical Forum](#)
- [zSecurity Learning Academy](#)
- [zSecurity Product Documentation](#)
- [zSecurity Collecting Data](#)

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

# Announcement Letters

zSecure 2.4 July 23<sup>th</sup> 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 5<sup>th</sup> 2019

[https://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep\\_ca/5/897/ENUS219-485/index.html&request\\_locale=en](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 12<sup>th</sup> 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](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 10<sup>th</sup> 2020

[https://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep\\_ca/2/897/ENUS220-062/index.html&request\\_locale=en](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 7<sup>th</sup> 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 19<sup>th</sup> 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](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 Archtitect

—

[dzrossi@us.ibm.com](mailto:dzrossi@us.ibm.com)  
908 347 8094