



Identifying Security Risks Using the Mainframe Security Insights Platform

June 7th, 2022

Balamurugan Venkatachalam, Narender Sajnani
Product Management – Mainframe Security | Mainframe Software Division



| Agenda

- Increasing Cybersecurity Concerns
- Security Audit v/s Security Risk Assessments
- Mainframe Security Risk Assessment
- Who is responsible and challenges?
- Overview of Mainframe Security Insights Platform
- Use-Case Demo
- Where to Start?
- Q & A

Increasing Cybersecurity Concerns

Continuous evaluation of your Mainframe's Security Posture is Critical



- Supply chain attacks
- Targeted ransomware
- Attacks exploiting legitimate software ("Living-off-the-Land")



Security Audit Vs. Security Risk Assessment

Security Audit

Independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security and recommend the required changes

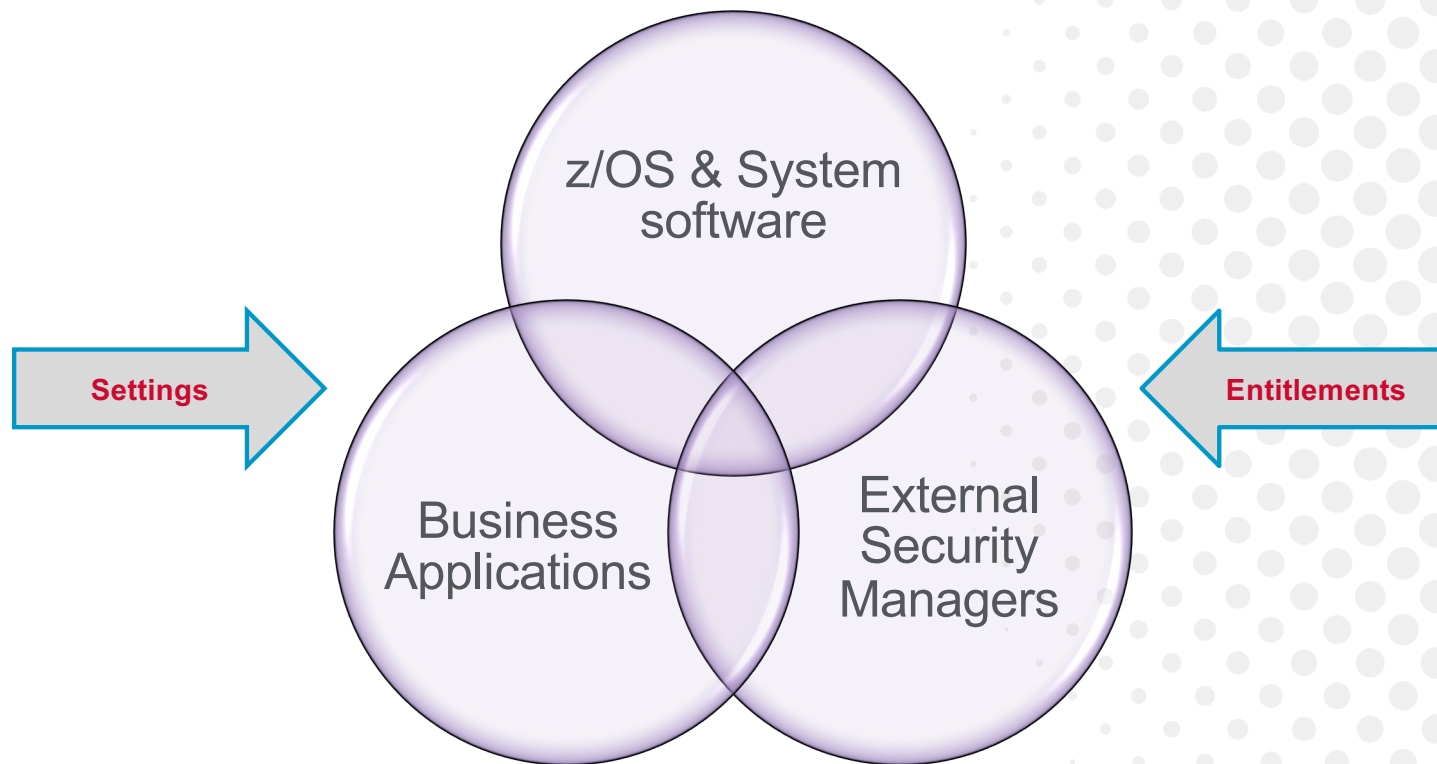
- Point in time check
- How well do system and practices meet the defined standards
- Self Audit is done by the dedicated internal team or a 3rd party service provider
- Outcomes are findings and corrective actions for existing security measures

Security Risk Assessment

Risk assessments help organizations identify, estimate, and prioritize risk to their operations, assets, and people, the output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process

- More analytical/diagnostic approach
- Identify what needs to be protected, why, and who can assess it
- Assess the possibility of security exposures and impact
- Risk level and intensity to determine the priority

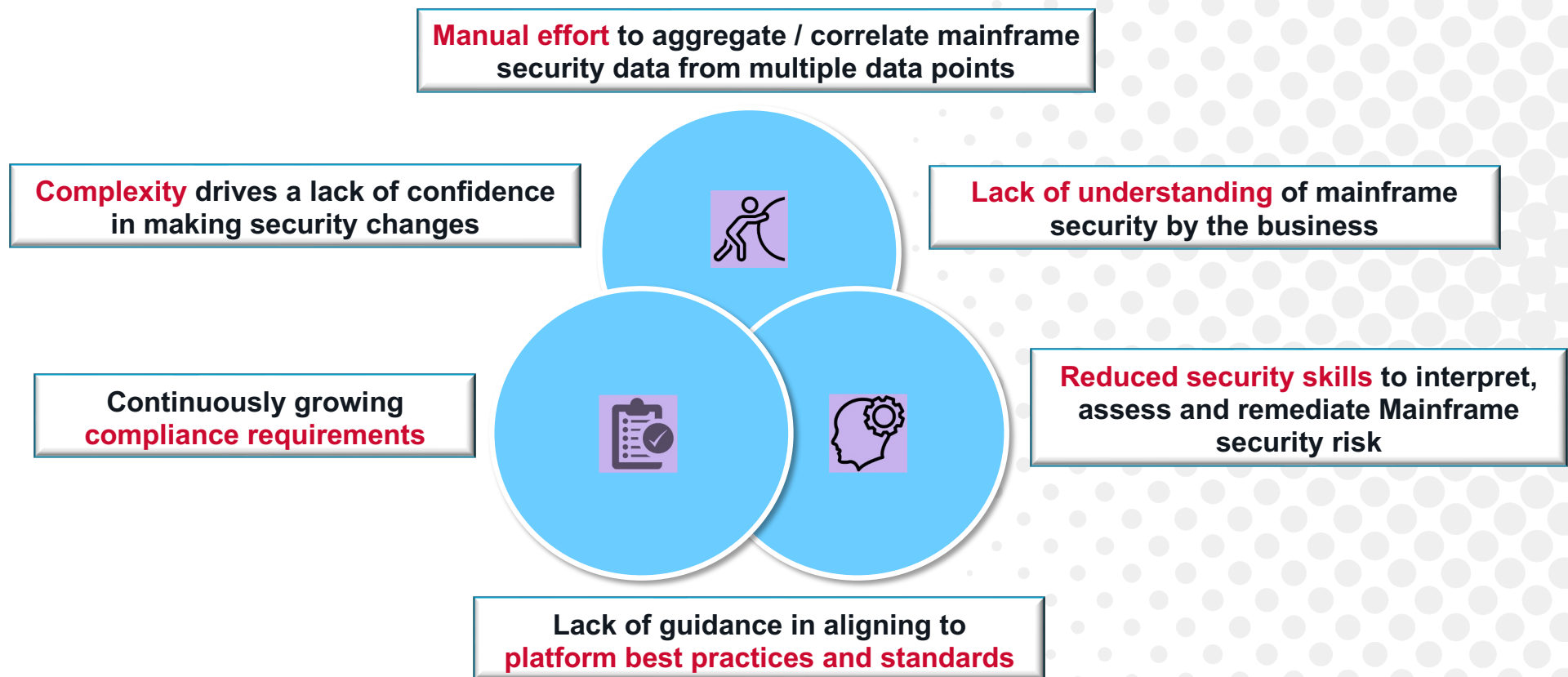
| Mainframe Security Risk Assessment



Responsibilities

Security Team	Business Application Owner	Internal Audit & Compliance Team
Responsibility: <ul style="list-style-type: none"> ➤ Who has access to System Critical Libraries? ➤ Is there any misconfiguration in z/OS, system software, and ESMs that may lead to security exposures? ➤ Run report for business , Are the business application data sources secured? 	Responsibility: <ul style="list-style-type: none"> ➤ Who has access to application data sets? ➤ Is Business-critical data encrypted? ➤ Where is the regulated / sensitive data? Who has access to that? 	Responsibility: <ul style="list-style-type: none"> ➤ Identify the critical resources and entitlement ➤ Ensure the control setting are protected ➤ Where is the business-critical data, is that protected with the least privileged model?
Challenge: <ul style="list-style-type: none"> ❖ Manual task - need to run ESM commands and aggregate data to derive findings that requires SME skills 	Challenge: <ul style="list-style-type: none"> ❖ Require help from Security Team to obtain access information ❖ Security attestations are tedious and time-consuming 	Challenge: <ul style="list-style-type: none"> ❖ Require help from Security and Application team to interpret information and identify audit findings

| Challenges



| Mainframe Security Insights Platform

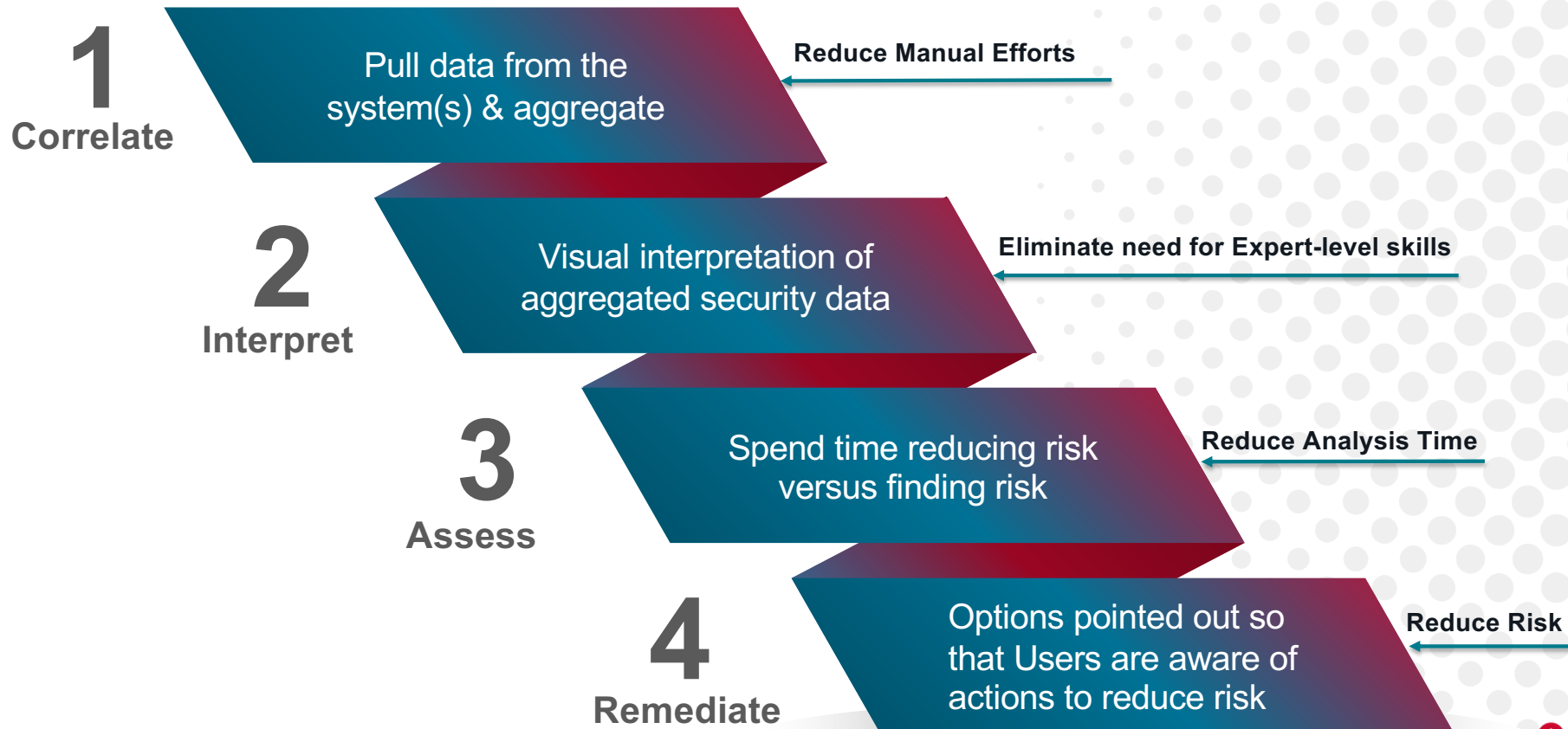
A hand is shown pointing at a futuristic digital interface. The interface features a central circular element with a gear-like icon, surrounded by concentric circles and various data visualizations like bar charts and line graphs. The background is a deep blue with a subtle pattern of white dots.

The Mainframe Security Insights Platform will do the heavy lifting of aggregating data by providing a visual representation of security posture by **interpreting** the security lifecycle and environmental data, **assessing** the data, and making **recommendations** to enable reduction of security risk within your Mainframe environment.

Protection Throughout the Security Lifecycle

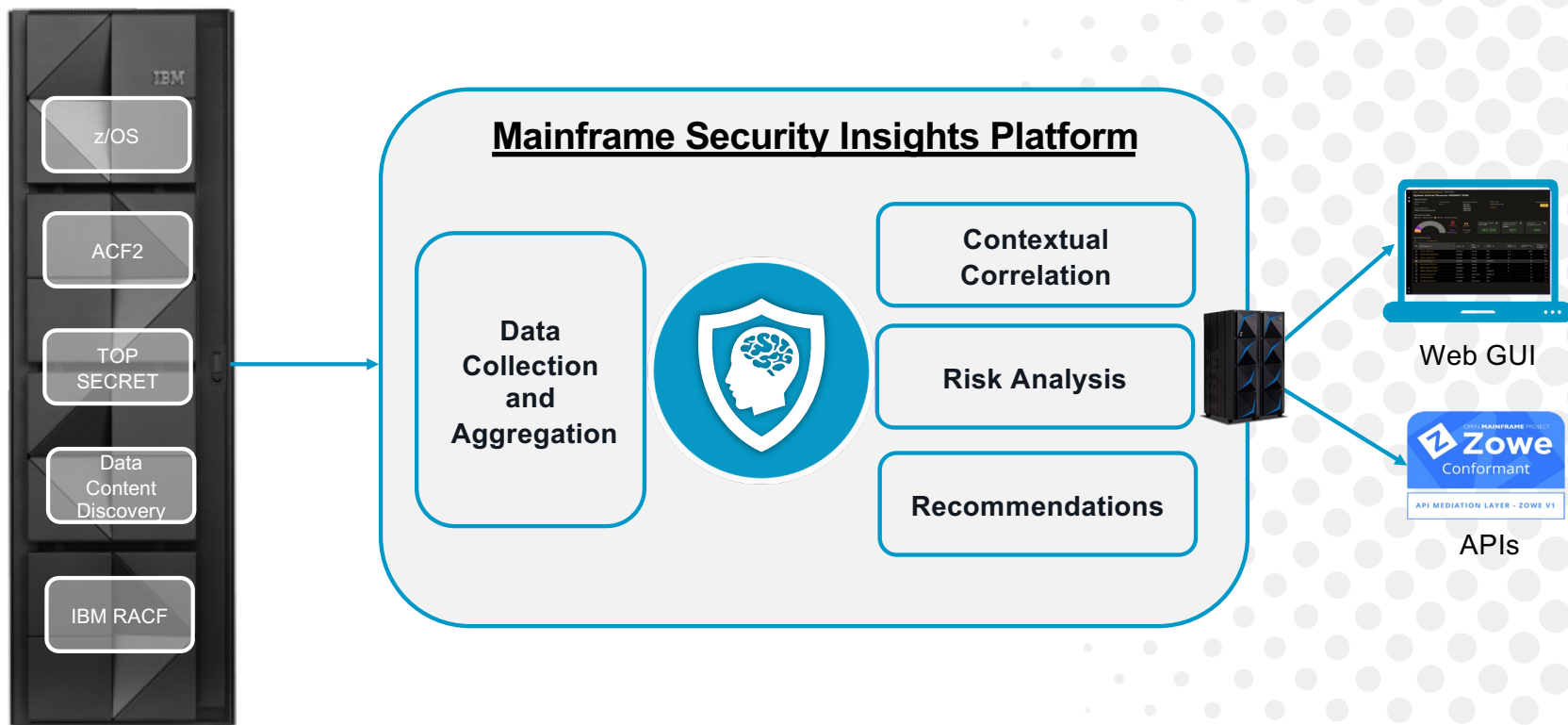


Simplifying your Day-to-Day Efforts



Mainframe Security Insights Platform

How it works



Identify Access to System-Critical Resources

Discover > Correlate with Entitlements > Analyze Risk > Report Risk & Remediation

As a Security Administrator, I want to identify who has access to system-critical resources (e.g., APF Libraries), so that I can align permissions to adhere to principle of least access privilege model.

Steps Involved

- Determine libraries in APFLIST
- For every library, determine who has access
- Aggregation done manually or using a custom script
- Manual interpretation of risk factors (entitlements)
- SMEs to identify next steps for reducing risk

```
//TSSAUDIT EXEC PGH=TSSAUDIT,REGION=0M
//AUDITOUT DD DSN=QAPRN,CHANGE,XE180RR,DISP=(NEW,CATLG,DELETE),
// UNIT=3390,SPACE=(CYL,(10,5),RLSE),VOL=SER=QATSS2
//* DCB=(RECFM=FBA,LRECL=133,BLKSIZE=2660)
//SYSDUMP DD SYSOUT=*
//AUDITIN DD *
APF
N 16.0
```

AUDIT UTILITY

----- LISTING OF APF LIBRARIES TO BE SEARCHED -----

ORIGIN	VOLSER	LIBRARY
DEFAULT		
IN-CORE APF TABLE	R23R02	SYS1.LPALIB
IN-CORE APF TABLE	R23R02	SYS1.LINKLIB
IN-CORE APF TABLE	SCAC12	SYS1.SVCLIB
		TSSMVS.CCS.R1500.CAWLINK

TSS WH00WNS DSN(apf_library)

```
DATASET = SYS1
XAUTH = SYS1.LINKLIB
ACCESS = ALL
ACTION = AUDIT
XAUTH = SYS1.SVCLIB
ACCESS = ALL
ACTION = AUDIT
XAUTH = SYS1.LINKLIB
ACCESS = READ
```

OWNER(SYSDEPT1)
ACID(SYSPROG1)

ACID(SYSPROG1)

ACID(*ALL *)

*** TSS0300I WHOHAS FUNCTION SUCCESSFUL ***

DATA SOURCE	VOLUME SERIAL	DATA SOURCE STATUS	LISTED UNDER	GLOBAL ACCESS	ENTITLEMENT COUNT
SYS1.SVCLIB	MVR24A	Found	APFLIST	Read	3
SYS1.OCGLIB	MVR24A	Found	APFLIST, LINKLIST	-	4
SYS1.OCGLIB	MVR24A	Found	APFLIST, LINKLIST	-	4
SYS1.LPALIB	MVR24A	Found	APFLIST, LPALIST	Create, Scratch, Update, Write	6
SYS1.PARMLIB	MVR24D	Found	PARMLIB	-	0
SYS1.LINKLIB	MVR24A	Found	APFLIST	-	3
SYS1.LINKLIB	MVR24A	Found	APFLIST, LINKLIST	-	6
SYS1.ASGLIB	MVR24A	Found	APFLIST, LINKLIST	Read	3
SYS1.PARMLIB	MVR24C	Found	PARMLIB	Create, Scratch, Update, Write	6

Addressing with Security Insights

Sample System Critical Access Report

Report Criteria

System (PAR) PLEX.TSO

Access Level ALL

SCRATCH UPDATE WRITE

System-Critical Resources APFLIST LPALIST LINKLIST PARMLIB

Risk Configuration Resource_Access_Default

Report Date 03-30-2022 16:42

Download Summary View CSV

Download Full Report CSV

External Security Manager Status COMPLETED

Creator SIDEMO

Email Notification sidemo@example.com

RISK LEVEL	IF	DATA SOURCE	IT	VOLUME SERIAL	IT	DATA SOURCE	IT	LISTED UNDER	IT	GLOBAL ACCESS	IT	ENTITLEMENT	IT
Significant High		SYS2.ENDV.USER.EXITS		MVSP6		Not Found		APFLIST		Scratch		4	
Significant High		TCPIP.SEZALNK2		MVSDC1		Found		APFLIST, LINKLIST		Write		10	
Significant High		SYS1.PLEX.PARMLIB		MVCAC1		Found		PARMLIB		Create, Scratch, Update, Write		6	
Significant High		SYS1.LPALIB		MVR24A		Found		APFLIST, LPALIST		Create, Scratch, Update, Write		6	
Significant High		SYS2.ACF2.CICLOAD		*SMS*		Not Found		APFLIST		---		0	
Significant High		XCOM.PROD.CARLIB		*SMS*		Not Found		APFLIST		---		4	
Significant High		TCPIP.SEZALOAD		MVSDC1		Found		APFLIST		Update		4	

APFLIST

LINKLIST

LPALIST

PARMLIB

Identify Access to Specified Resources

Discover > Correlate with Entitlements > Analyze Risk > Report Risk & Remediation

As a business application owner, I want to identify who has access to my business-critical data, so that I can provide information needed for regular attestation and internal audit processes

Steps Involved

- Define an inventory of business-critical libraries
- For every library, determine who has access
- Aggregation done manually or using a custom script
- Manual interpretation of risk factors (entitlements)
- SMEs to identify next steps for reducing risk

OPERATIONS → FINANCE.NA.*
FINANCE.APJ.*
SALES.DIV.*
OPS.HRMS

```
TSS WHOHAS DSN(FINANCE.NA.*)
DATASET = FINANCE OWNER(OPSDEPT)
XAUTH = FINANCE.NA.AUDIT ACID(USER001)
ACCESS = ALL
ACTION = AUDIT
XAUTH = FINANCE.NA.GOVERNC ACID(BUPROD02)
ACCESS = ALL
ACTION = AUDIT
XAUTH = FINANCE.APJ. ACID(*ALL *)
ACCESS = READ
...
*** TSS0300I WHOHAS FUNCTION SUCCESSFUL
```

DATA SOURCE	VOLUME	SERIAL	DATA SOURCE	STATUS	LISTED UNDER	GLOBAL ACCESS	ENTITLEMENT COUNT
SYS1.SVCLIB	MWR24A	Found	APPLIST	Read			3
SYS1.OMGLIB	MWR24A	Found	APPLIST, LINKLIST	-			4
SYS1.CSGLIB	MWR24A	Found	APPLIST, LINKLIST	-			4
SYS1.LPALIB	MWR24A	Found	APPLIST, LPAALIST	Create, Scratch, Update, Write			6
SYS1.PARGLIB	MWR24D	Found	PARGLIST	-			0
SYS1.DMAGLIB	MWR24A	Found	APPLIST	-			3
SYS1.LINKLIB	MWR24A	Found	APPLIST, LINKLIST	-			6
SYS1.MIGLIB	MWR24A	Found	APPLIST, LINKLIST	Read			3
SYS1.PLEX.PARGLIB	MWR24C1	Found	PARGLIB	Create, Scratch, Update, Write			6

Addressing with Security Insights

Sample Specified Resource Access Report_TSS

Sample System Critical Access Report

Report Criteria

System (LPA)	Access Level	Data Sets Selected	Risk Configuration	Report Date	Download Summary View
PLEX TSS	ALL CREATE FETCH READ	FINANCE.NA.* SALES DIVISION * SALES * ARCHIVE FINANCE APJ DATA* DOMMY OPSDEPT LIB OPS HRMS PVA GOOD000	Resource Access_Default View Risk Configuration	03-30-2022 16:42 Report	CSV Download Full Report CSV

External Security Manager Status COMPLETED Creator SIDEMO Email Notification sidemo@example.com

Add Filter

RISK LEVEL	IT	DATA SOURCE	IT	GLOBAL ACCESS	IT	ENTITLEMENT COUNT	IT
Significant High		SALES DIVISION *		Create, Scratch, Update, Write		11	
Significant High		FINANCE.NA.SOUTH.ZONE		Scratch		6	
Significant High		FINANCE.NA.*		Update		1	
Significant High		OPS.TOM LIB		Update		4	
Significant Medium		FINANCE.NA.EAST.ZONE		Read		6	
Significant Medium		FINANCE.EMEA.DATA.DOMMY		Read		4	

Mainframe Security Insights Platform

Key Features



Web-based

Access results through an easy-to-use web interface



zIIP-eligible and runs 100% on the platform
Critical data never leaves the z/OS platform



Broad coverage
Supports ACF2, Top Secret and IBM RACF environments



Aggregates Data
Collects and consolidates data from multiple LPARs



Enables Self Service
Tool for Security, Application, and Internal Audit Teams



Risk Modeling
Out-of-the-box risk model also supports customizations



Generate Reports
Reports can be exported as a CSV

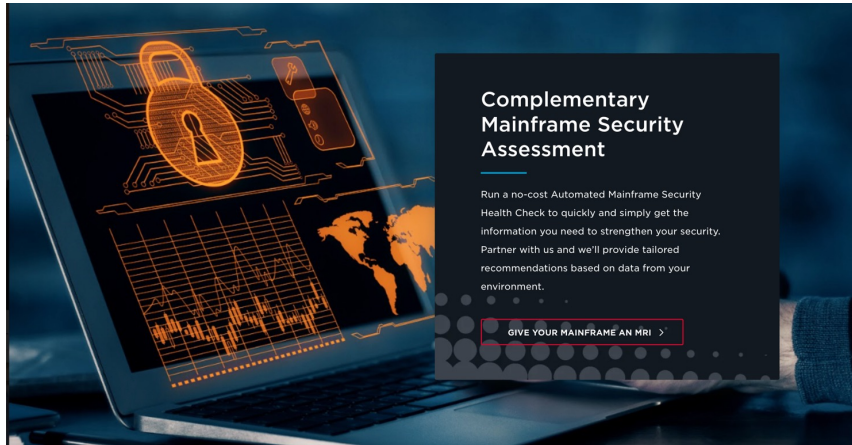


Secure
Leverages native security authorizations of the user



Recommendations
Remediation steps that helps reduce risk

How Broadcom can help start your Journey



Cybersecurity Thinking Workshop

Focused conversation about your Cyber-Security challenges on the Mainframe

Mainframe Security Health Assessment

Automated Mainframe Security Health Checks

Cybersecurity Thinking Workshop

Avoid Becoming the Next Cybersecurity Headline

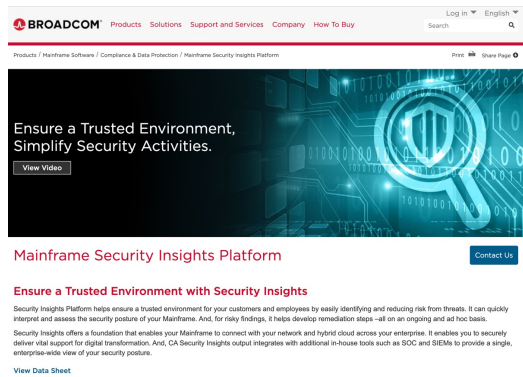
GET STARTED

MRI Security Assessment & Cyber-Security Thinking Workshops are available to you at no cost

Start with Proof of Concept...

Resources

Product Home



BROADCOM Products Solutions Support and Services Company How To Buy Log in English Search

Products / Mainframe Software / Compliance & Data Protection / Mainframe Security Insights Platform Print Share Page

Ensure a Trusted Environment, Simplify Security Activities. View Video

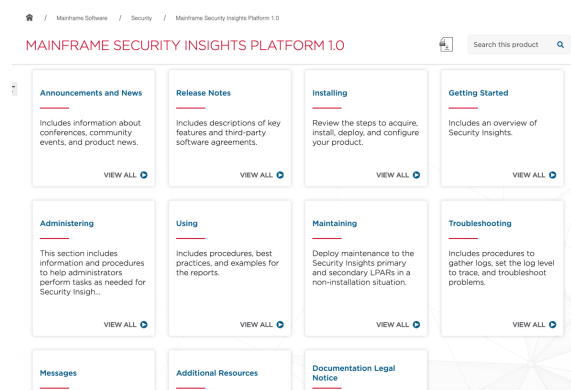
Mainframe Security Insights Platform Contact Us

Ensure a Trusted Environment with Security Insights

Security Insights Platform helps ensure a trusted environment for your customers and employees by easily identifying and reducing risk from threats. It can quickly interpret and assess the security posture of your Mainframe. And, for risky findings, it helps develop remediation steps – all on an ongoing and ad hoc basis. Security Insights offers a foundation that enables your Mainframe to connect with your network and hybrid cloud across your enterprise. It enables you to securely deliver vital support for digital transformation. And, CA Security Insights output integrates with additional in-house tools such as EDC and SIEMs to provide a single, enterprise-wide view of your security posture.

View Data Sheet

Technical Documentation

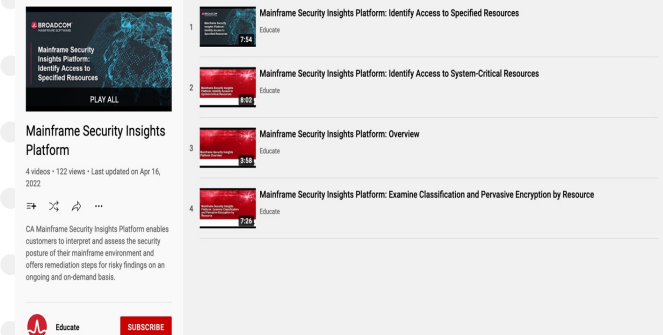


Home / Mainframe Software / Security / Mainframe Security Insights Platform 1.0 Search this product

MAINFRAME SECURITY INSIGHTS PLATFORM 1.0

Announcements and News Includes information about conferences, community events, and product news. VIEW ALL	Release Notes Includes descriptions of key features and third-party software agreements. VIEW ALL	Installing Review the steps to acquire, install, deploy, and configure your product. VIEW ALL	Getting Started Includes an overview of Security Insights. VIEW ALL
Administering This section includes information and procedures to help administrators perform tasks as needed for Security Insights. VIEW ALL	Using Includes procedures, best practices, and examples for the reports. VIEW ALL	Maintaining Deploy maintenance to the Security Insights primary and secondary LPARs in a non-installation situation. VIEW ALL	Troubleshooting Includes procedures to gather logs, set the log level to trace, and troubleshoot problems. VIEW ALL
Messages	Additional Resources	Documentation Legal Notice	

Use-Case Videos



Mainframe Security Insights Platform: Identify Access to Specified Resources Educate 7:44

Mainframe Security Insights Platform: Identify Access to System-Critical Resources Educate 1:52

Mainframe Security Insights Platform: Overview Educate 5:38

Mainframe Security Insights Platform: Examine Classification and Pervasive Encryption by Resource Educate 7:28

Mainframe Security Insights Platform
4 videos • 122 views • Last updated on Apr 16, 2022
Educate SUBSCRIBE

Did you know that you can get the Mainframe Security Insights Platform @ no additional cost?
Yes, Broadcom's Mainframe Security customers can obtain Security Insights as part of their existing license!

To learn more information about Broadcom Mainframe Security solutions, visit - <https://mainframe.broadcom.com/security>

Broadcom's Mainframe Education & Vitality Program

Partnering to Solve Mainframe Skills Shortage

Interested in improving existing employee's skills?

Experienced Mainframe Professionals

Traditional product education, web-based and instructor-led trainings for those who would like to refresh or expand their Mainframe product knowledge.



Mainframe eLearning Library

- Low-cost, high-quality, Mainframe product and vendor-agnostic training
- Thousands of hours of quality online training on over 350 Broadcom and IBM topics
- Earn official skills, credentials and digital badges from IBM and Broadcom
- Self-paced delivery, instantly available anywhere, anytime
- Web-Based Product Training

[Explore library](#)



Web-Based Product Training

- Self-paced Mainframe product education at no cost for active maintenance customers
- [Access Mainframe Course Catalog](#)
- [Access Learning@Broadcom](#)
- [Earn Broadcom Mainframe Digital Badges for product knowledge](#)
- [Learning Paths](#)

[Accessing Broadcom Mainframe Training Quick Reference Guide](#)



Instructor-Led Product Training

- Virtual or onsite Mainframe product education
- Delivered by Broadcom Subject Matter Experts or Education Partners

[Contact Broadcom Software](#)

Mainframe Software Education

Let Broadcom hire, train and mentor new talent to become part of your Mainframe team.



Mainframe Vitality Program

Broadcom STIGs

Security Technical Implementation Guides (STIGs)

Broadcom STIGs

- ACF2
- TOP Secret
- Cleanup
- SYSVIEW
- Endevor
- OPS/MVS
- Common Services
- IDMS

Broadcom STIGs

Using STIG Articles

Includes mainframe security standard review and implementation guidelines.

New Section in
Techdocs

[VIEW ALL](#) 



Thank you

Balamurugan Venkatachalam
Product Manager
Mobile: +1 469 750 8364
balav@broadcom.com

Narender Sajnani
Product Owner
Mobile: +1 331 255 6639
NarenderEshwar.Sajnani@broadcom.com