

# IBM Security

## Technical Overview



Charlie Niemi, MSIA, CISSP  
Technical Specialist

A.B.A.C.U.S.  
SOLUTIONS

WE GET IT

HAWK BRIDGE

cm FIRST  
Rethink Modernization

ca  
technologies  
A Broadcom  
Company

helpsystems

SODiSA®

ptc®

AXON iVY  
digitalize your business

NGS  
New Generation  
Software, Inc.

IBM

# Agenda

## IBM Security Technical Overview

Overview of:

### Digital Trust

*-Key products*

### Threat Intelligence

*-Key products*

-IBM /AS/400/IBM Power Systems Security  
and Compliance tools



# Traditional security can't keep pace

# Too much to do

# Too many vendors



# Too much complexity



# Too many alerts



# Clients need a modern, open, unified approach to security

## Client's Security Challenges



Cloud  
Security



Advanced  
Threats



Compliance  
and Privacy

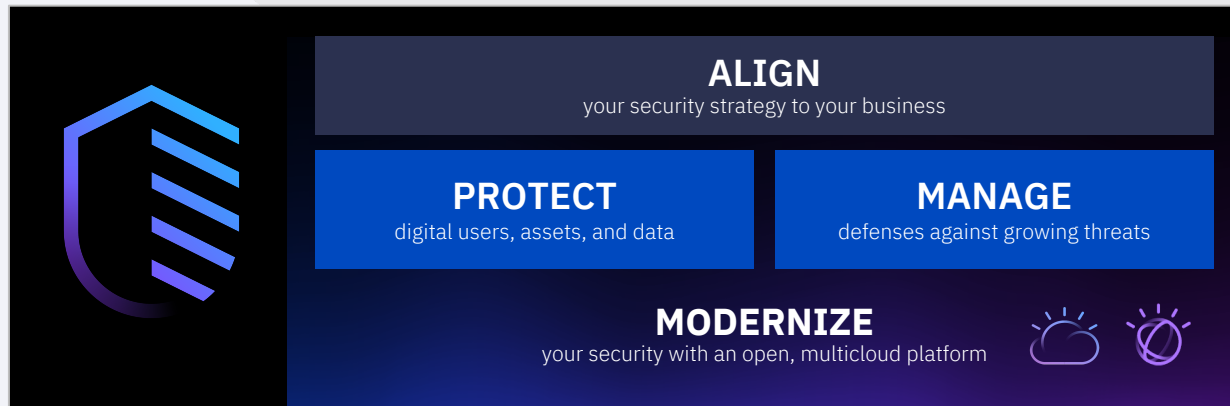


Skills  
Shortage



Mobile, Edge  
and IoT / OT

## IBM Solutions



## IBM Differentiation

Deep  
Expertise

Open  
Platform

AI-Driven  
Technology

Largest  
Ecosystem

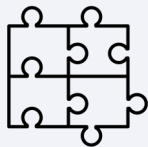


# IBM Differentiation



## Deep Expertise

- Trusted Advisors
- Command Centers
- Global Industry Expertise

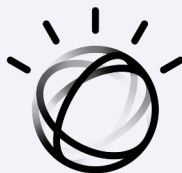


## Open Platform

Cloud Pak  
for Security



**Red Hat**



## AI-Driven Technology

- Manage growing threats
- Protect digital landscape
- Modernize security architecture



## Largest Ecosystem

- X-Force Exchange
- Solution and GTM



# The industry's broadest and most complete security portfolio



## STRATEGY AND RISK ALIGN

### *Advance Security Maturity*

- Strategy and Planning
- Risk Assessments
- Advisory Services

### *Build Leadership and Culture*

- IBM Security Command Center
- IBM Security Command Mobile
- IBM Security Command Onsite
- IBM Security Command Virtual



## DIGITAL TRUST PROTECT

### *Protect Critical Assets*

- SDLC Consulting
- Data Protection Services
- Guardium
- Data Risk Manager
- Multi-cloud Encryption
- Key Lifecycle Manager
- IBM Systems
- IBM Cloud Hyper Protect Services

### *Deliver Digital Identity Trust*

- Trusteer
- Verify

### *Govern Users and Identities*

- Identity Management Services
- Identity Governance
- Verify
- Verify Access
- Verify Privilege

### *Unify Endpoint Management*

- Endpoint Management Services
- MaaS360



## THREAT MANAGEMENT MANAGE

### *Stop Advanced Threats*

- Security Operations Consulting
- X-Force Threat Management Services
- X-Force Red
- QRadar

### *Orchestrate Incident Response*

- Resilient
- X-Force IRIS

### *Master Threat Hunting*

- i2 Intelligence Analysis
- QRadar Advisor with Watson

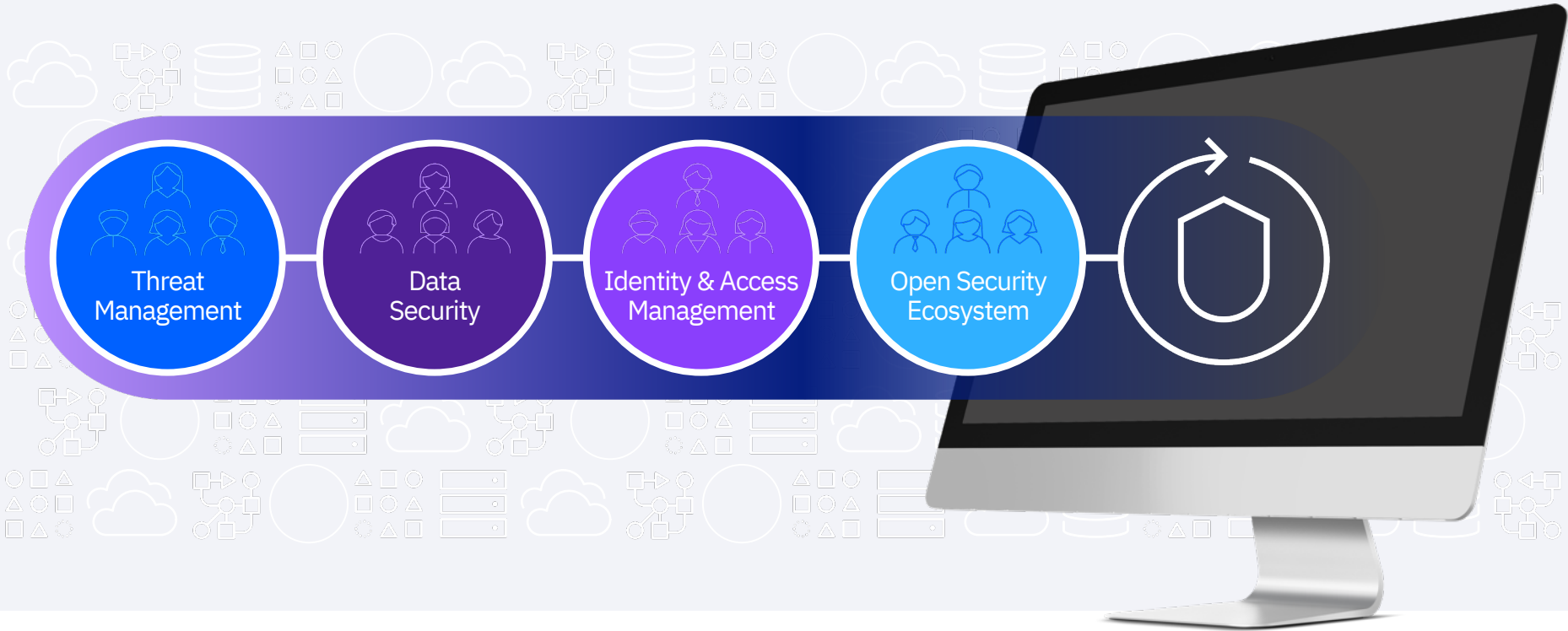
## MODERNIZE



# Hundreds of open integrations at the center of your ecosystem



# A unified and open approach for teams to connect data and workflows



# Who depends on IBM?

IBM Security secures

**100%**  
of the US Fortune 100

**95%**  
of the Global Fortune 500

## Finance

**49 out of 50** of the world's largest financial services and banking companies

## Tech

**13 out of 15** of the world's largest technology companies

## Healthcare

**14 out of 15** of the world's largest healthcare companies

## Telecom

**The 10 largest** telecom companies

## Automotive

**19 out of 20** of the world's largest motor vehicle and parts companies

## Airline

**8 out of 10** of the world's largest airline companies

## We are invested to be the best

**Proven security  
market leadership  
across 14 segments**

SIEM

Security Analytics

Fraud Reduction  
Intelligence Platform

Web Fraud Detection

Identity Governance

Access Management

Identity as a Service

Identity Management

Risk-Based Authentication

Data Security and Database Security

Data Center Backup and Recovery

Unified Endpoint Management

Managed Security Services

Cybersecurity Incident Response Services



# Where we are now

- Largest enterprise cybersecurity provider
- Leader in 14 security market segments
- 8,000+ security employees
- 20+ security acquisitions
- 70B+ security events monitored per day



# Security Eco System



Ensure access only to intended users



Implement Zero Trust security for increased Digital Trust



Limit access to specific roles



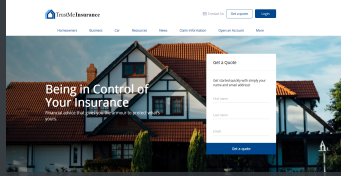
Enforce consistent security controls of Data and files across on prem & hybrid computing platforms



Ensure Compliance with Regulatory Compliance access rules

# Digital Trust – Identity Verify

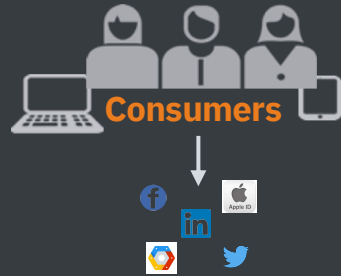
Build your own



API

# IBM Security Verify

SSO | MFA | Provisioning/Governance | Analytics



Enterprise Employees & Contractors



Gateway

Basic SSO



Access

Advanced SSO

or



Privilege

Manage Admin Accounts



Bridge

Basic Provisioning & Governance

or



Identity

Advanced provisioning & Governance



On Premise Apps

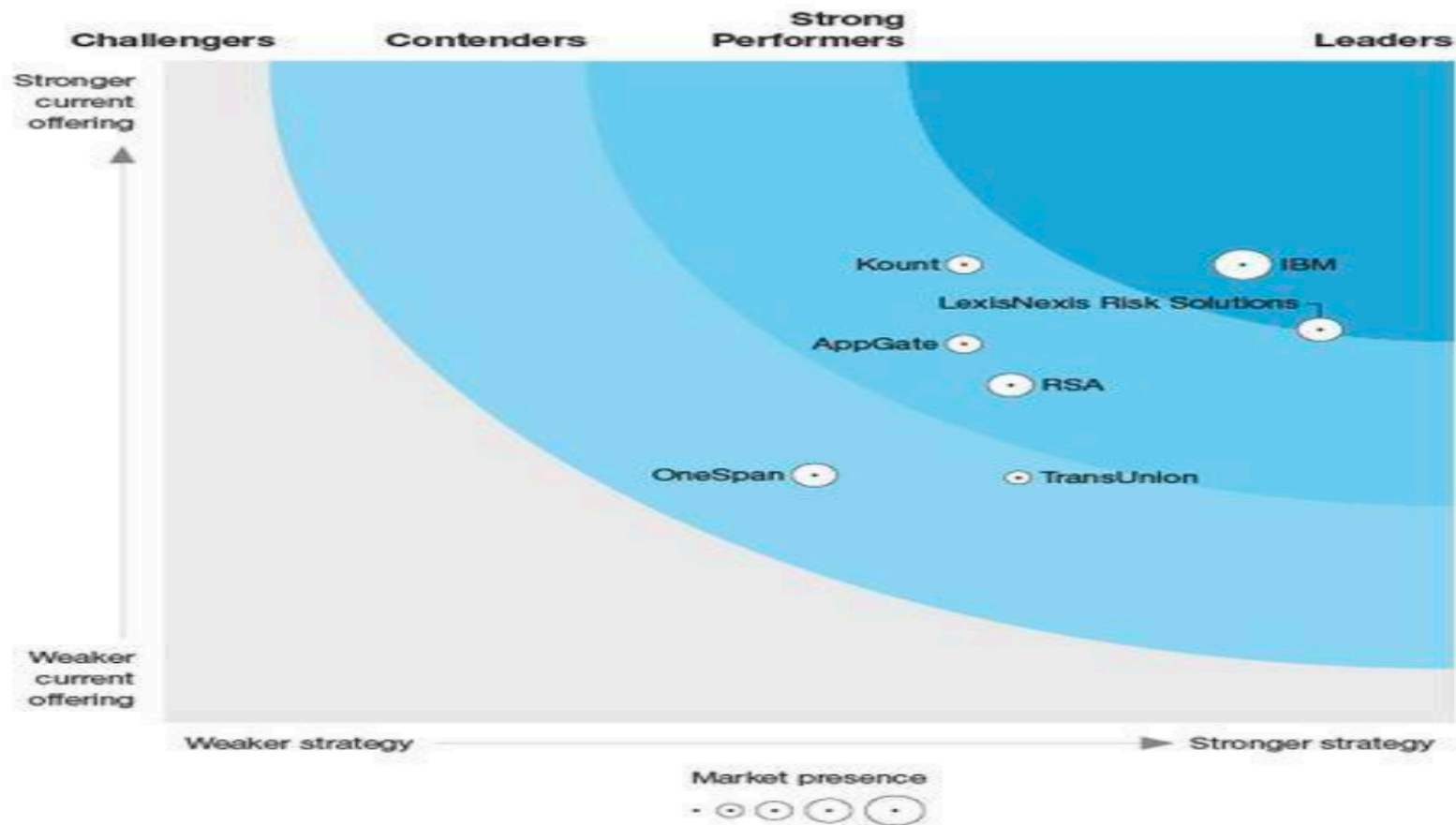


IBM Security IAM Architecture

# THE FORRESTER WAVE™

## Risk-Based Authentication

Q2 2020

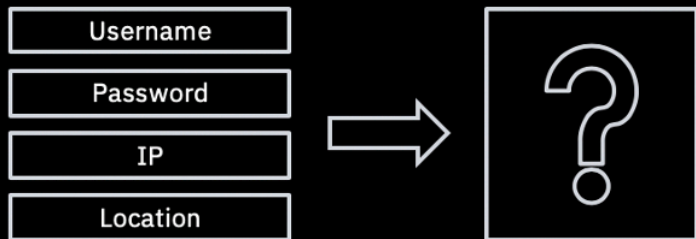




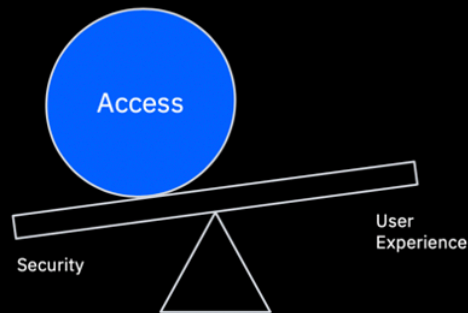
# Cloud Identity – Adaptive Access

[IBM Security Verify](#) with adaptive access is an intelligent access management platform that combines advanced risk detection with a robust access policy engine to assess the full context of a user's identity as they attempt to access a digital service.

Deep identity verification is a challenge.



How does a business balance user experience and risk?



## The Real Francine



### Personal Identifiable Information



Francine



Vargas



fran.vargas@work.com



(267)647-6030



San Francisco, CA



Social Security#



United States



Username



Mouse Speed



Password



Typing Speed



Login Geography



Device Usage



MAC Address



Online Behavior

## Analyzed Identity



### Personal Identifiable Information



Francine



Vargas



fran.vargas@work.com



(267)647-6030



Moscow



Social Security#



Russia



Username



Mouse Speed



Password



Typing Speed



Login Geography



Device Usage



MAC Address



Online Behavior

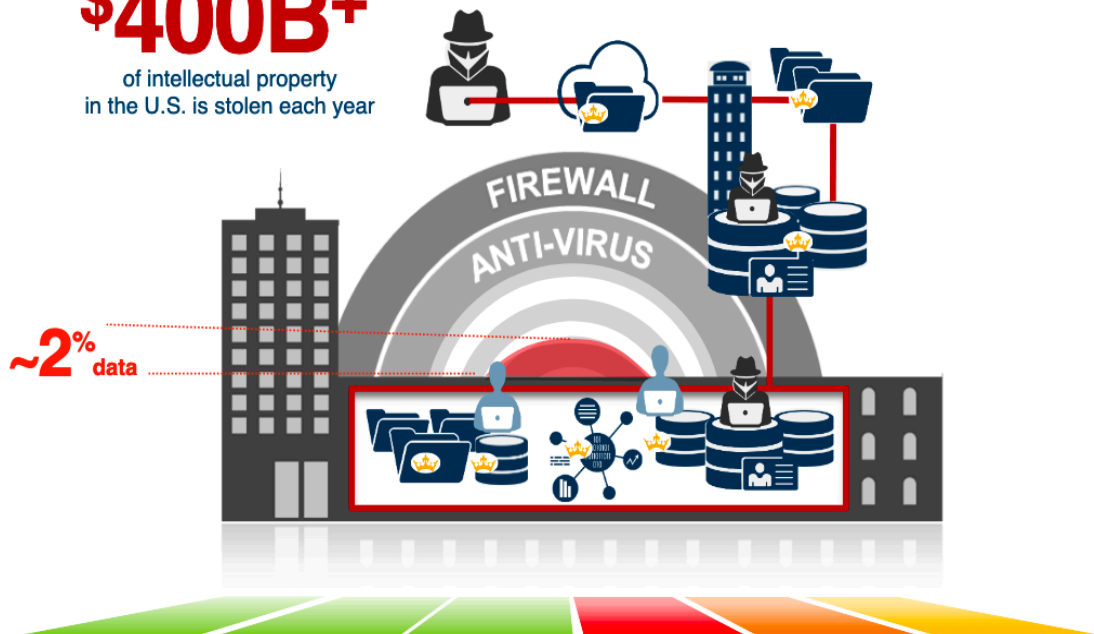
# Digital Trust – Guardium Suite

# The Data Protection Problem Today

Will you be doing enough to protect data that runs your business?

**\$400B+**

of intellectual property  
in the U.S. is stolen each year



Data  
Explosion

Mobile / IOT

Cloud

Attack  
Sophistication

Regulations

Skills  
Shortage

**Data security and compliance will get more difficult**

**70%** of your company's  
value likely lies in  
**intellectual property**  
*Customer data, product designs, sales  
information, proprietary algorithms,  
communications, etc.*

Source: TechRadar

**90+%** of breaches go after  
data in servers

*Regardless of the attach vector, the hacker's  
goal is to get privileged access to valuable  
data*

Source: Verizon Reports

**86%** of breaches take  
months-years to  
discover

*Enterprise data is easy to compromise and  
hard to monitor with traditional perimeter  
tools*

Source: Verizon Reports

**70%** Of enterprises do not  
know what privileged  
users are doing

*Privileged access goes unnoticed*

**\$5.8M** Cost of a US Data  
Breach

*Impact of data breaches increasing and affecting  
customer trust, liability, loss revenue, brand  
reputation*

Source: X-Force Report

# Guardium Security – It's a Journey

Discover

Harden

Monitor

Protect

Manage

## Data at Rest



Discovery  
Classification

Encryption

## Configuration



Vulnerability  
Assessment



Entitlements  
Reporting

## Data in Motion



Activity  
Monitoring

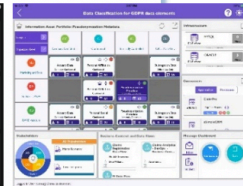
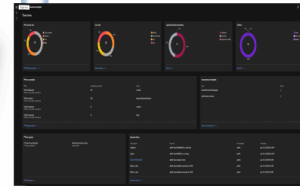


Blocking  
Quarantine



Dynamic Data  
Masking

## Insight and Data Risk





# Guardium Security – It's a Journey

Discover

Harden

Monitor

Protect

Manage

## Data at Rest

## Configuration

## Data in Motion

## Insight and Data Risk



**Discovery Classification**   **Encryption**

*Where is the sensitive data?*

*How to protect sensitive data?*



**Vulnerability Assessment**   **Entitlements Reporting**

*How to secure the repository?*

*Who can access?*

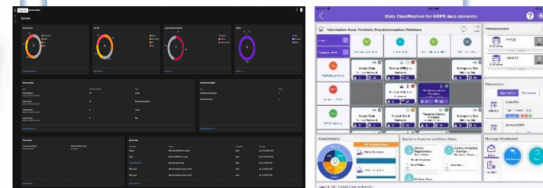


**Activity Monitoring**   **Blocking Quarantine**   **Dynamic Data Masking**

*What is actually happening?*

*How to prevent unauthorized activities?*

*How to protect sensitive data to reduce risk?*



*How to get early visibility on sensitive data risks?*

*How to effectively communicate and mitigate sensitive data risks?*

Guardium Data Protection

- Databases
- Files
- Cloud

Guardium Data Encryption

SKLM  
GCKM

Guardium Vulnerability Assessment (VA)

Guardium Data Protection

- Databases
- Files
- Cloud

Guardium Data Encryption

Data Risk Manager

Guardium Insights

# Threat Management

# The industry's broadest and most complete security portfolio



## STRATEGY AND RISK ALIGN

### *Advance Security Maturity*

- Strategy and Planning
- Risk Assessments
- Advisory Services

### *Build Leadership and Culture*

- IBM Security Command Center
- IBM Security Command Mobile
- IBM Security Command Onsite
- IBM Security Command Virtual



## DIGITAL TRUST PROTECT

### *Protect Critical Assets*

- SDLC Consulting
- Data Protection Services
- Guardium
- Data Risk Manager
- Multi-cloud Encryption
- Key Lifecycle Manager
- IBM Systems
- IBM Cloud Hyper Protect Services

### *Deliver Digital Identity Trust*

- Trusteer
- Verify

### *Govern Users and Identities*

- Identity Management Services
- Identity Governance
- Verify
- Verify Access
- Secret Server

### *Unify Endpoint Management*

- Endpoint Management Services
- MaaS360



## THREAT MANAGEMENT MANAGE

### *Stop Advanced Threats*

- Security Operations Consulting
- X-Force Threat Management Services
- X-Force Red
- QRadar

### *Orchestrate Incident Response*

- Resilient
- X-Force IRIS

### *Master Threat Hunting*

- i2 Intelligence Analysis
- QRadar Advisor with Watson

## MODERNIZE



# 4 pillars of an effective SIEM

## Complete Visibility



- Normalization
- Categorization
- Enrichment
- Network, endpoint, cloud, user and application

## Prioritized Threat Detection



- MITRE ATT&CK
- Models
- Behavior chaining
- Global threat intelligence

## Automated Investigations



- AI
- Data mining
- Supervised learning
- Unstructured data analysis
- Federated Search

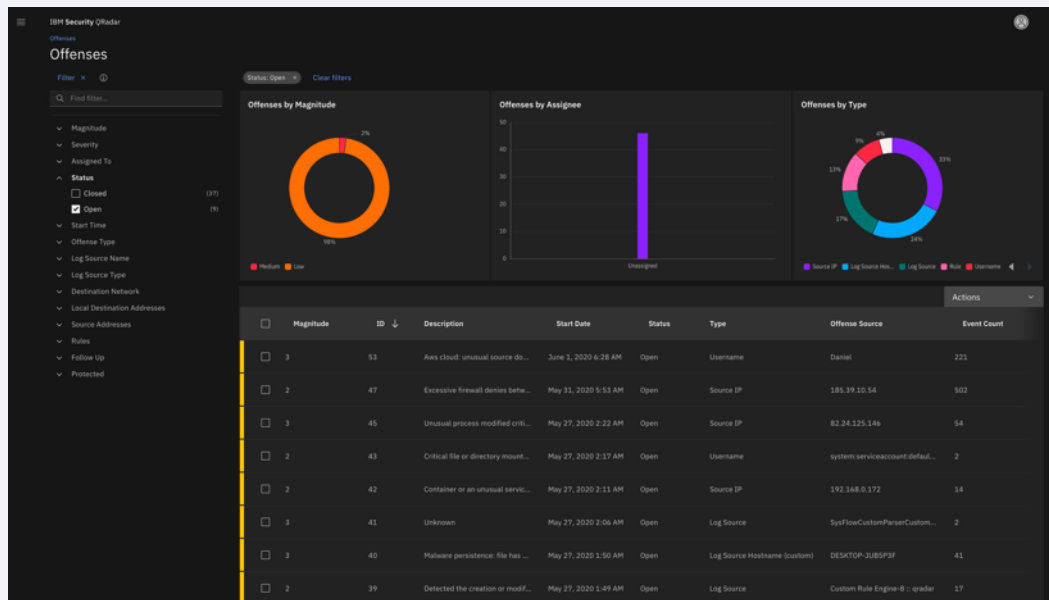
## Integrated Response



- Dynamic playbooks
- Automation
- Orchestration
- Privacy breach reporting

# IBM Security QRadar

- **Unify SOC workflows** by effectively addressing threats with an integrated visibility, detection, investigation and response platform
- **Augment security staff** with AI-assisted triage and automated response playbooks
- **Mature security operations** with visualized use case coverage, OOTB content, and expert threat intelligence powered by IBM's X-Force IRIS
- **Address regulatory risk** and report on compliance adherence with out-of-the-box content for GDPR, ISO 27001, HIPAA, and more





# Complete visibility

Visibility  
into cloud  
usage and  
risks

Real-time  
insights  
into user  
behavior

The screenshot displays the IBM Security QRadar console interface. The main panel shows a list of events with columns for Event Name, Log Source, Source IP, Destination IP, Event Count, and Event. The events are filtered by 'Unusual source' and show various AWS Cloud activities such as 'AWS Cloud: Detected an API call to...', 'Run Instances', 'Console Login', and 'Successful Login to AWS Console F...'. The right-hand panel provides a detailed view of a selected event, including 'Event Overview' (General Audit Event), 'Event Custom Properties' (Region: us-east-2), and 'Payload' (JSON data). The 'Source and destination information' section shows the Source IP as 213.178.155.78 and Destination IP as 127.0.0.1.

Expose  
threats as  
they move  
across the  
network

Endpoint  
visibility  
with  
Sysmon

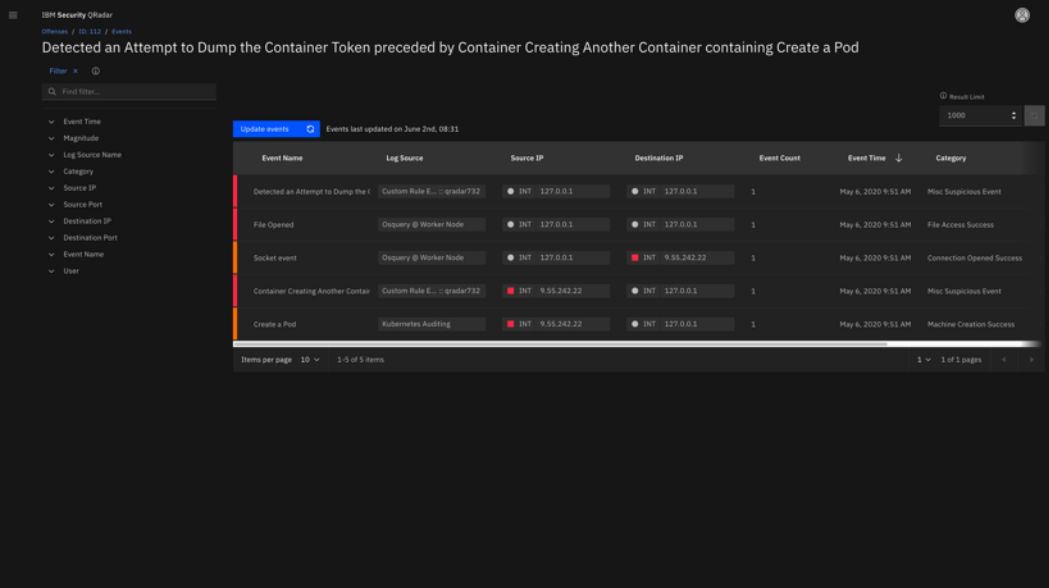
“QRadar drastically reduced the time it took us to connect our 100+hybrid multi-cloud accounts to QRadar. This made it easy to consume both events and network flow traffic from our AWS and other cloud environments.”

**Large US-based Insurance Company**

# Threat detection

Identify  
known and  
unknown  
threats

Real time  
detection  
across  
100's of  
security  
use cases



The screenshot displays the IBM Security QRadar console interface. At the top, a header bar shows the title 'IBM Security QRadar' and a breadcrumb trail 'Offenses / 10:112 / Events'. Below this, a main heading reads 'Detected an Attempt to Dump the Container Token preceded by Container Creating Another Container containing Create a Pod'. A search bar with the placeholder 'Find filter...' is visible. On the left, a sidebar contains a list of filters: Event Time, Magnitude, Log Source Name, Category, Source IP, Source Port, Destination IP, Destination Port, Event Name, and User. The main content area features a table of events, with a 'Result Limit' of 1000. The table has columns for Event Name, Log Source, Source IP, Destination IP, Event Count, Event Time, and Category. The events listed are: 'Detected an Attempt to Dump the C...' (Log Source: Custom Rule E...; :qradar732), 'File Opened' (Log Source: Osquery @ Worker Node), 'Socket event' (Log Source: Osquery @ Worker Node), 'Container Creating Another Contain...' (Log Source: Custom Rule E...; :qradar732), and 'Create a Pod' (Log Source: Kubernetes-Auditing). The table also shows event counts and timestamps for each event. At the bottom, there is a pagination bar indicating 'Items per page: 10' and '1-5 of 5 items'.

Event Name	Log Source	Source IP	Destination IP	Event Count	Event Time	Category
Detected an Attempt to Dump the C...	Custom Rule E...; :qradar732	INT 127.0.0.1	INT 127.0.0.1	1	May 6, 2020 9:51 AM	Misc Suspicious Event
File Opened	Osquery @ Worker Node	INT 127.0.0.1	INT 127.0.0.1	1	May 6, 2020 9:51 AM	File Access Success
Socket event	Osquery @ Worker Node	INT 127.0.0.1	INT 9.55.242.22	1	May 6, 2020 9:51 AM	Connection Opened Success
Container Creating Another Contain...	Custom Rule E...; :qradar732	INT 9.55.242.22	INT 127.0.0.1	1	May 6, 2020 9:51 AM	Misc Suspicious Event
Create a Pod	Kubernetes-Auditing	INT 9.55.242.22	INT 127.0.0.1	1	May 6, 2020 9:51 AM	Machine Creation Success

Dynamically  
adjust  
as attacks  
unfold

Automatic  
ally link  
multiple  
malicious  
behaviors

“IBM QRadar improves the speed and effectiveness of detecting threats by nearly 75%.”

**Forrester**

# Automated investigation

Let Watson  
automatically  
determine  
threat  
priorities

Map  
investigations  
to MITRE  
ATT&CK tactics  
and techniques

The screenshot shows the IBM Security QRadar Search results page. At the top, there's a 'Query Builder' section with a SQL query: `SELECT magnitude, sourceip, destinationip, QIDSCRIPTID, qid, AS 'Event Name', LOGSOURCENAME 'Log Source', CONCAT(CATEGORYNAME 'HighLevelCategory', ':', CATEGORYNAME) 'category' AS 'Category Name', DATEFORMAT(startTime, 'MM/DD/YYYY') AS 'Start Time' FROM events WHERE TEXT SEARCH '213.178.155.78' LIMIT 1000 LAST 3 Days`. Below the query builder, there's a 'Filter' section with a 'Log Source Name' filter set to 'AWS'. The main part of the screen is a table of search results with columns: magnitude, sourceip, destinationip, destinationport, Event Name, Log Source, and Category Name. The table contains 10 rows of data, all with a magnitude of 2 and source IP of 213.178.155.78. The events include 'Amazon AWS Cloud Trail Store...', 'Get Object', 'List Buckets', and 'Run Instances'.


magnitude	sourceip	destinationip	destinationport	Event Name	Log Source	Category Name
2	213.178.155.78	127.0.0.1	0	Amazon AWS Cloud Trail Store...	AWS	Unknown Stored
2	213.178.155.78	127.0.0.1	0	Get Object	AWS	Audit Object Download Attempt
2	213.178.155.78	127.0.0.1	0	List Buckets	AWS	Audit Read Activity Attempted
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...

Understand the  
source and  
impact of the  
attack so you can  
respond  
effectively

Hunt threats via  
a search

“QRadar offers strong support for incident investigation by providing context enrichment from internal and external sources, suggesting next steps based on attacker actions and prioritizing alerts for further action.”

Gartner

A background image showing two women in a professional setting. One woman with dark hair is looking towards the other woman, who has blonde hair and is wearing glasses, gesturing with her hands as if speaking.

# Wouldn't it be great if you could...

## Minimize

duration and impact of  
cyber-attacks

## Optimize

SecOps and reduce  
staff burnout

## Address

breach reporting  
requirements and  
show compliance

## Maximize

security investments  
and scale insights  
across teams

# IBM Security Resilient



Respond with confidence



Automate with intelligence



Collaborate with consistency

# Respond to incidents with confidence

## Guide and empower your **security teams** with knowledge

### *Features and capabilities:*

- Capture and digitize industry and organizational knowledge in incident playbooks
- Empower existing staff to adapt response processes to meet attacks
- Meet compliance requirements with leading knowledgebase of global breach reporting requirements
- Prioritize incident response with a clear picture of the relationships between artifacts and incidents

The screenshot displays the Resilient interface for an incident titled '[POTENTIAL PHISH] - Completely\_Free\_Act\_Now'. The incident is in the 'Incidents' tab, created by Andrew Wadsworth on 01/23/2020. The incident type is 'Phishing'. The incident details include a description, a list of related artifacts, and a list of related incidents. The related artifacts table lists various items such as 'Malware SHA-1 Hash', 'IP Address', 'Email Recipient', 'Email Sender', 'Email Subject', and 'URL'. The related incidents table lists other incidents related to the same event.

Type	Value
Malware SHA-1 Hash	296b81de7fac82014324e...
Malware SHA-1 Hash	c14625785a1b0f93704b...
Malware MD5 Hash	079eb1365e9aef46710aa51e78...
Malware Sample	SKMBT_C20171116424367...
System Name	wm-c34ad485-ACL
IP Address	103.15.233.228
IP Address	192.168.254.3
IP Address	54.71.108.255
Email Recipient	wadsworth@us.ibm.com
Email Sender	admin@washingtonref.com
Email Subject	Request for Quotation
URL	http://businessstobuy.net/uc/cryptin...
URL	http://businessstobuy.net
URL	http://washingtonref.com/images/wa...

The screenshot displays the Resilient interface for the 'Privacy' page. The page contains a search bar, a 'Privacy' tab, and a list of privacy-related documents. The documents are organized into sections: 'U.S. States & Territories', 'U.S. Federal and Trade Organizations', and 'U.S. Special Jurisdictions'. Each section lists various laws and regulations, such as the 'Bank Secrecy Act', 'CAMS (Dept of Defense)', 'Fannie Mae', 'FDIC', 'Federal Reserve', 'FERPA', 'EPA', 'FISMA', 'FTC (Health)', 'GLB Act', 'HIPAA/HITECH Act', 'NACHA', 'NCLIA', 'OCC', 'OMB', 'PCI-DSS (Issuers)', 'PCI-DSS (Merchants)', 'SEC', 'US Dept of Treasury', 'California (Health)', 'Texas (Health)', 'Virginia (Health)', 'California (Insurance)', 'Connecticut (Insurance)', 'Maryland (Insurance)', 'Montana (Insurance)', 'New Hampshire (Insurance)', 'Ohio (Insurance)', 'Rhode Island (Insurance)', 'Washington (Insurance)', 'Wisconsin (Insurance)', 'Arkansas (Mortgage Bankers and Loan Officers)', 'Arkansas (Insurance)', 'Texas person/entity/state agency', 'New York (Department of Financial Services)', 'Illinois (State Agencies)', 'Montana (State Agencies)', 'Vermont (Data Brokers)', 'Virginia (Income Tax Preparers)', 'California (CCPA)', and 'Canadian Provinces'.

## Large, global pharmaceutical organization

Action	Before Resilient	With Resilient	Example
Escalate via SIEM, EDR, or NGFW	5 min	<b>10 sec</b>	Escalate suspicious endpoint activity incident from QRadar
Identify affected assets — CMDB/AD/IAM	5–10 min	<b>10 sec</b>	CMDB lookup on laptop and Active Directory user lookup
Check IOCs against Threat Intelligence Feeds	5 min	<b>10 sec</b>	Incident includes hash that is tied to known Locky variant
Correlate historical incidents and data	10–20 min	<b>instant</b>	2 other incidents in the last month have the same hash and outbound traffic, pointing to a larger campaign
Manual Enrichment — Pull activity from endpoints, external networks, VPN logs, DNS records, network infrastructure, and endpoint forensics.	30–55 min	<b>30 sec</b>	Use carbon black to pull process tree from laptop, DNS from web proxy to find C2 server
Incident Tracking — Maintain detailed notes and tasks throughout the incident lifecycle	N/A	<b>instant</b>	Resilient automatically tracks tasks and actions completed as part of an incident response, all analyst notes are stored in the platform
Maintain audit trail and logging — Maintain a courtroom-admissible audit trail of an incident response	N/A	<b>instant</b>	Everything done in Resilient is logged and cannot be modified. When subpoenaed in court, management can just print out the log
Report incident status and provide visibility to management	N/A	<b>instant</b>	Executive dashboards and external notifications give management real-time insight without any extra effort from the SOC
<b>Total</b>	<b>85 min</b>	<b>1 min</b>	

# Meet privacy breach reporting demands with Resilient



170+ global regulations— in product to help customers to remain compliant with the complex breach notification requirements



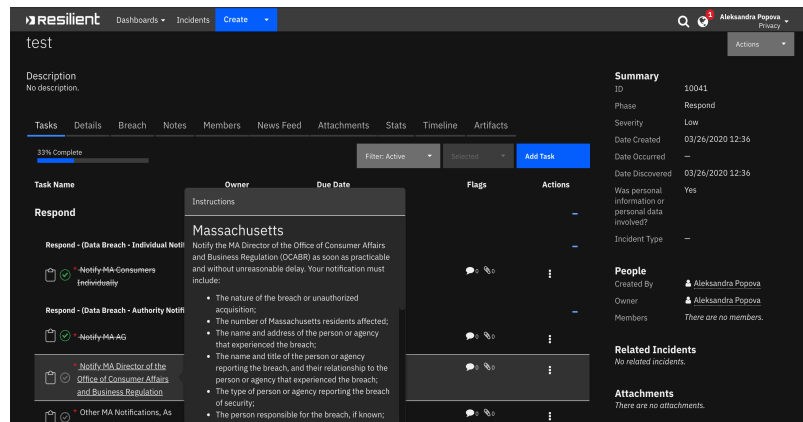
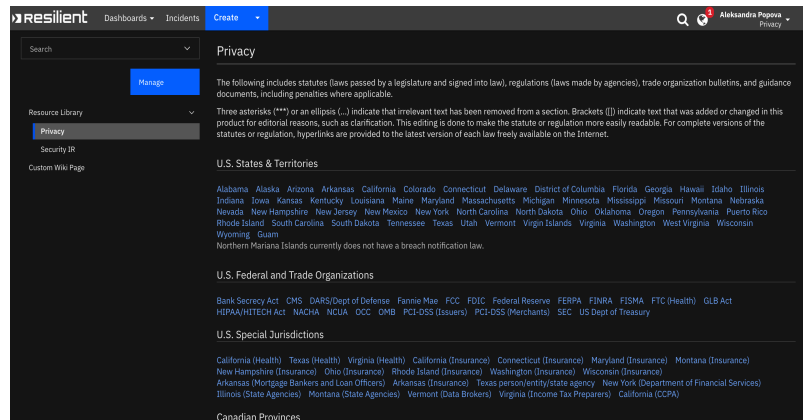
Integrated breach notification and data subject request with the wider Cyber Security Incident Response plan — one central place of incident management



Full simulation and table-top capabilities to train Privacy & IR teams on consistent, repeatable procedures



GDPR, PIPEDA, HIPAA, CCPA and all 50 states breach notifications rules included in the solution





# IBM Cloud Pak for Security

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

- **Gain security insights**

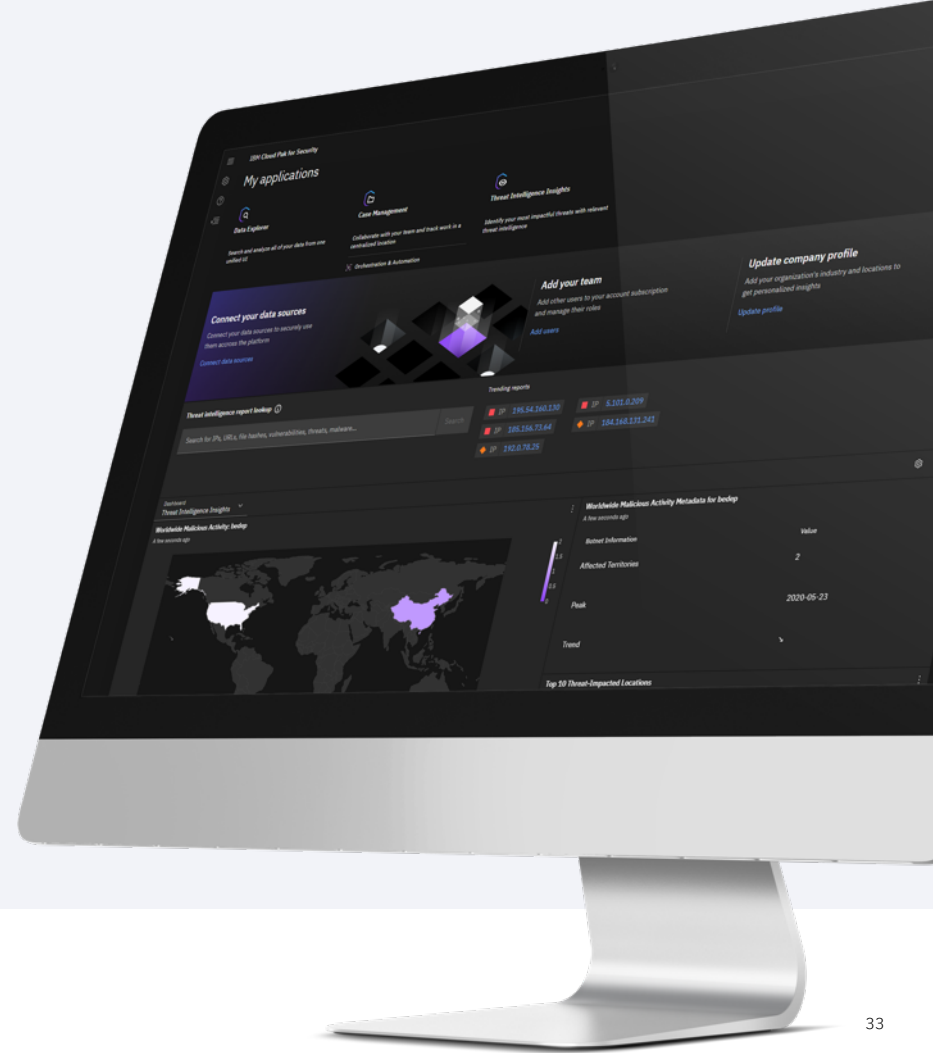
With a unified console that provides visibility and analytics across IBM and 3rd party security tools, data, and clouds

- **Take action faster**

With AI and automation, simplify operations and streamline response, to save time and lower risk

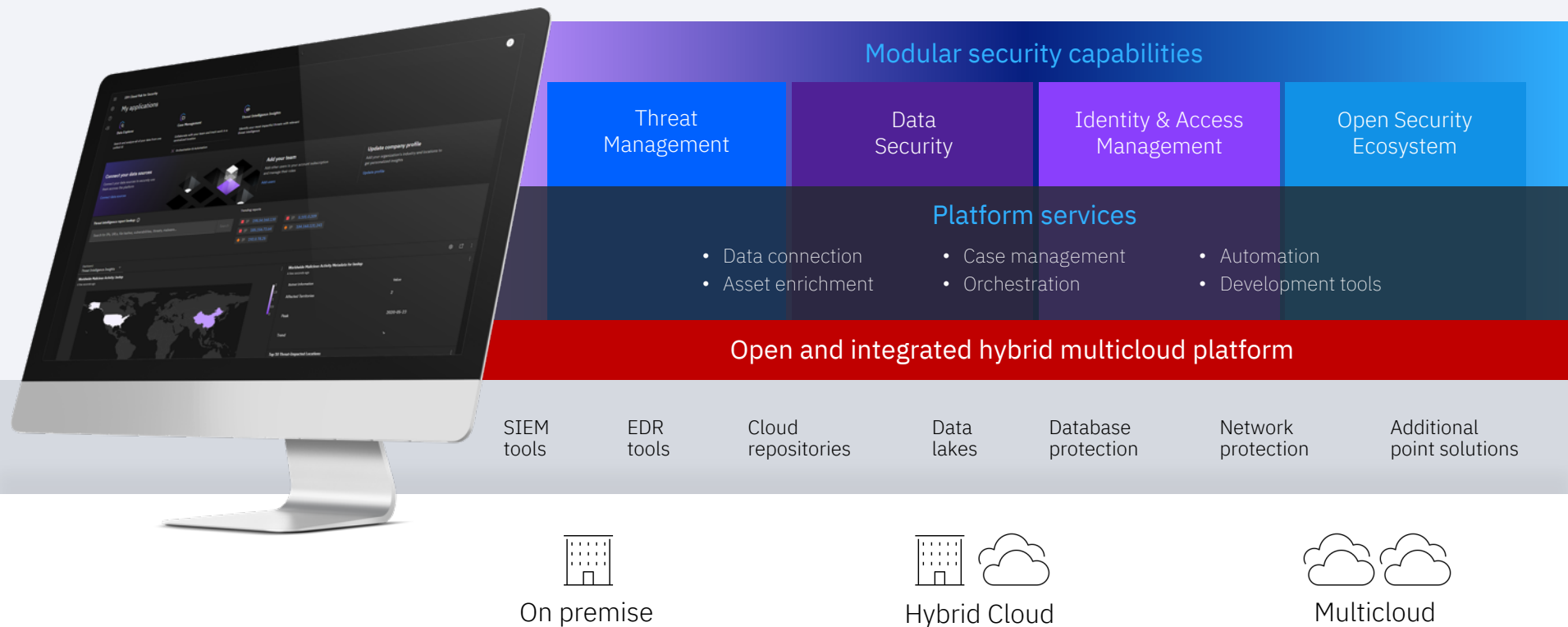
- **Modernize your architecture**

Modernize your architecture and run anywhere with open, multicloud platform that gives you flexibility, extensibility and avoids lock-in



# IBM Cloud Pak for Security

An open multicloud platform to gain security insights, take action faster, and modernize your architecture



IBM /AS/400/IBM Power Systems Security.

# Security and Compliance Tools for IBM i

Service offerings from IBM Systems Lab Services

Tools / Feature	Function	Benefit
<b>Compliance Automation and Reporting with Event Monitoring Tool (CART)</b>	Daily compliance dashboard report/s at LPAR, system or enterprise level with event monitoring	Enables compliance officer to demonstrate adherence to pre-defined security policies
<b>Security Diagnostics</b>	Reports detailing security configuration settings and identifying deficiencies	Reduces operator time involved in remediating security exposures
<b>Privileged Elevation Tool (FIRECALL)</b>	Controls the number of privileged users	Ensures compliance with industry guidelines on privileged users
<b>Access Control Monitor</b>	Monitors security deviations from application design	Prevents user application failures due to inconsistent access controls
<b>Network Interface Firewall for IBM i Exit Points</b>	Controls access to Exit Point interfaces such as ODBC, FTP, RMTCMD, Command Restrictions, etc	Reduces threat of unauthorized security breach and data loss
<b>SYSLOG Reporting Manager</b>	Simplifies QAUDJRN / IFS file change events to syslog (CEF)	Utility to allow the IBM i to participate with SIEM solutions
<b>Certificate Expiration Manager</b>	Simplifies management of digital certificates expiration	Helps operators prevent system outages due to expired certificates
<b>Password Synchronization</b>	Aids users with enhanced PWD management	Maintains consistent PWDs and SVRAUTE
<b>Advanced Authentication</b>	Service Program to enable MFA in applications	Includes PWD Reset and Signon utilities
<b>Single Sign On (SSO) Suite</b>	Simplifies implementation of SSO and password synchronization	Reduces password resets and simplifies end user experience

## Centralized reporting of IBM i security

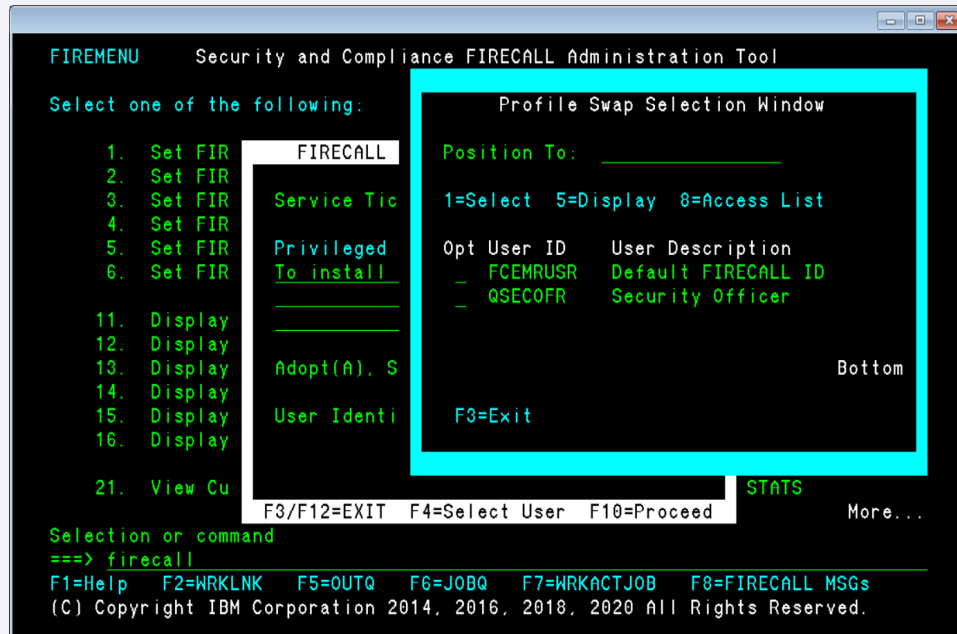
- 
- Overall Status of Systems in the Enterprise**
- Geographic Information**
- Policy Type:
- By Region**
- | Region  | System Count |
|---------|--------------|
| North   | 1            |
| South   | 2            |
| East    | 3            |
| West    | 1            |
| Central | 2            |
| Other   | 2            |
- Report generated On: Jun 10, 2012 at 12:12:00
- By Data Center**
- | Data Center | System Count |
|-------------|--------------|
| DC1         | 2            |
| DC2         | 2            |
| DC3         | 2            |
| DC4         | 2            |
| DC5         | 2            |
| DC6         | 2            |
- Report generated On: Jun 10, 2012 at 12:12:00
- By Country**
- | Country | System Count |
|---------|--------------|
| USA     | 2            |
| UK      | 2            |
| France  | 2            |
| Germany | 2            |
| Italy   | 2            |
| Spain   | 2            |
- Report generated On: Jun 10, 2012 at 12:12:00
- System Attributes**
- By UAT/OAT**
- | UAT/OAT | System Count |
|---------|--------------|
| UAT     | 2            |
| OAT     | 2            |
| Both    | 2            |
- Report generated On: Jun 10, 2012 at 12:12:00
- By System Purpose**
- | System Purpose | System Count |
|----------------|--------------|
| Development    | 2            |
| Testing        | 2            |
| Production     | 2            |
- Report generated On: Jun 10, 2012 at 12:12:00
- By Operating System Version**
- | OS Version | System Count |
|------------|--------------|
| Windows 7  | 2            |
| Windows 8  | 2            |
| Windows 10 | 2            |
- Report generated On: Jun 10, 2012 at 12:12:00
- Parameters**
- Rating Type:
- Region:
- 
- 1 of 1 records, Page 1 of 1
- Overall Policy Status by System for Data Center: UK**
- Enterprise Wide: High, Medium, Low  
 Specific: High, Medium, Low  
 Priority: High, Medium, Low  
 Policy: High, Medium, Low  
 System: High, Medium, Low  
 Version: High, Medium, Low  
 Backup: High, Medium, Low  
 Configuration: High, Medium, Low
- Report generated On: Jun 10, 2012 at 12:12:00
- Graded System Attribute Details for Policy Rating**
- Region: Europe  
 Data Center: UK  
 System: CYCLOST
- | Attribute         | Sub-attribute | Value  | Rating |
|-------------------|---------------|--------|--------|
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |
| Policy Attributes | Sub-policy    | Low    | Red    |
| Policy Attributes | Sub-policy    | High   | Green  |
| Policy Attributes | Sub-policy    | Medium | Yellow |

# Privileged Elevation Tool (FIRECALL)

Ensures compliance to industry guidelines on privileged users

Without careful control, privileged users can pose a risk to your system security. This tool enables the security administrator to reduce privileged accounts, with a mechanism to temporarily elevate privileges to users when needed.

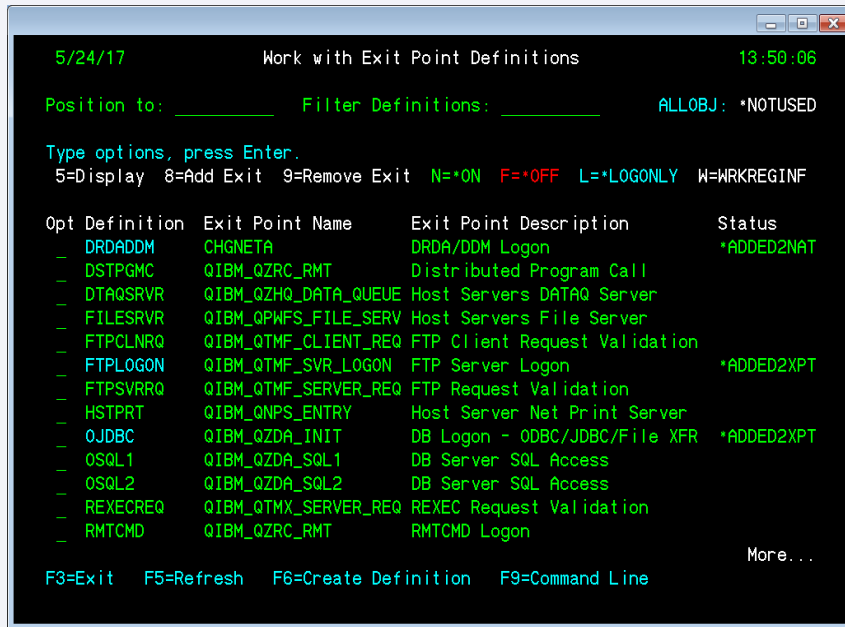
- Service Ticket Manager
- Option to change identity for troubleshooting, IFS access and object ownership requirements
- Fully audited
- Automated email notifications sent to distribution list when tool is invoked that includes a log of activities performed
- Customizable



# Network Interface Firewall for IBM i Exit Points

## Reduces threat of unauthorized network access

- Exit programs allow system administrators to control which activities a user account is allowed for each of the specific servers. This easy to use interface addresses the most commonly used network interfaces.



The screenshot shows a terminal window titled "Work with Exit Point Definitions" with a date of 5/24/17 and time of 13:50:06. It displays a list of exit points with columns for Opt, Definition, Exit Point Name, Exit Point Description, and Status. The list includes various services like DRDADDMM, DSTPGMC, DTQSRVR, FILESRVR, FTPCLNRQ, FTPLGON, FTPSVRQ, HSTPRQ, QJDBC, OSQ1, OSQ2, REXECREQ, and RMTCMD. Some entries are marked as "ADDED2NAT" or "ADDED2XPT". At the bottom, there are function keys: F3=Exit, F5=Refresh, F6=Create Definition, and F9=Command Line.

Opt	Definition	Exit Point Name	Exit Point Description	Status
—	DRDADDMM	CHGNETA	DRDA/DDM Logon	*ADDED2NAT
—	DSTPGMC	QIBM_QZRC_RMT	Distributed Program Call	
—	DTQSRVR	QIBM_QZHQ_DATA_QUEUE	Host Servers DATAQ Server	
—	FILESRVR	QIBM_QPWFS_FILE_SERV	Host Servers File Server	
—	FTPCLNRQ	QIBM_QTMF_CLIENT_REQ	FTP Client Request Validation	
—	FTPLGON	QIBM_QTMF_SVR_LOGON	FTP Server Logon	*ADDED2XPT
—	FTPSVRQ	QIBM_QTMF_SERVER_REQ	FTP Request Validation	
—	HSTPRQ	QIBM_QNPS_ENTRY	Host Server Net Print Server	
—	QJDBC	QIBM_QZDA_INIT	DB Logon - ODBC/JDBC/File XFR	*ADDED2XPT
—	OSQ1	QIBM_QZDA_SQL1	DB Server SQL Access	
—	OSQ2	QIBM_QZDA_SQL2	DB Server SQL Access	
—	REXECREQ	QIBM_QTMX_SERVER_REQ	REXEC Request Validation	
—	RMTCMD	QIBM_QZRC_RMT	RMTCMD Logon	

Users denied by default for greater security

Users allowed are added via menu

Allow access through Group Profiles

Restrict by IP Address, Range

Log only mode

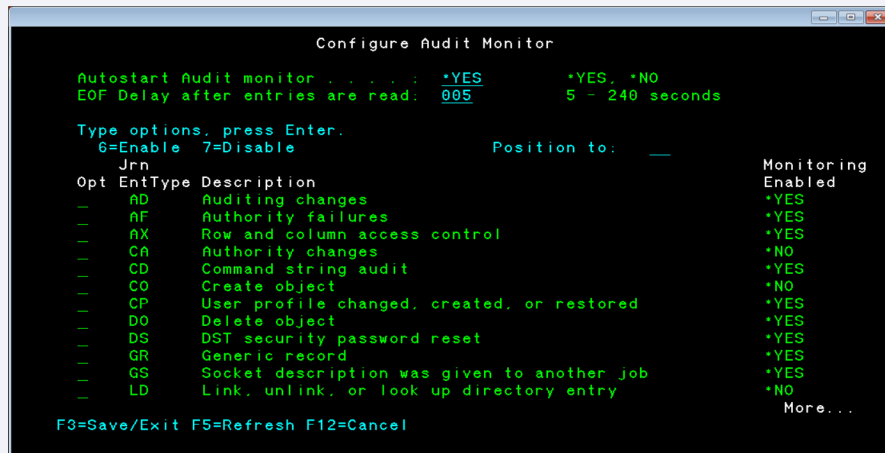
Current exit point coverage:

- DRDA / DDM
- IFS
- FTP
- ODBC/JDBC/File Transfer
- REXEC

# SYSLOG Reporting Manager

Simplifies the management and reporting of IBM i SIEM events

- Monitors QAUDJRN, QHST Messages, MSGQs, IFS stream file changes, and more!
- Formats events to Common Event Format (CEF and LEEF) for Security Information and Event Management consumption
- Reports events via syslog messages in near real time!
- Easy setup



```
Mar 30 20:29:51 p4.ai.stgt.spc.ihost.com auth|security:info : <38>1 2018-03-30T20:29:44.792240+02:00 i5osp4.ai.stgt.spc.ihost.com - - - CEF:0|IBM|IBM i|7.3|QSYS-QAUDJRN|T-CD|Low|reason=Command string audit msg=Command run interactively from a command line or by choosing a menu option that runs a CL command - QSH fileType=*CMD cs1Label=objName cs1=QSHELL/QSH suser=BARLEN sproc=212409/BARLEN/QPADEV0002 shost=I5OSP4

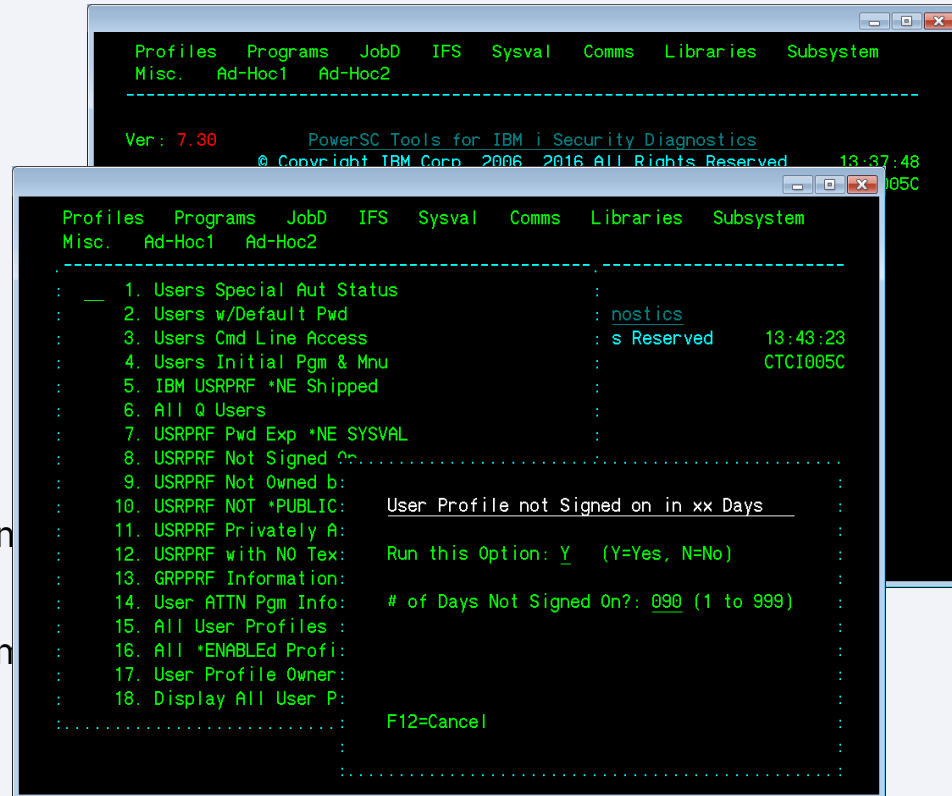
Mar 30 20:30:36 p4.ai.stgt.spc.ihost.com local2:info : <150>1 2018-03-30T20:30:26.686016+02:00 i5osp4.ai.stgt.spc.ihost.com - - - CEF:0|IBM|IBM i|7.3|IFS|IFS File Monitor Journal Entry Type B-WA|3|act=B-WA Write, after-image event sproc=212658/BARLEN/QZSHSH suser=BARLEN shost=I5OSP4 filePath=/home/barlen/ifsmon/weblog1.log fileType=*STMF cs1Label=changedData cs1=Web server configuration changed for instance HRINFORM
```



# Security Diagnostics

## In depth security collection and reporting

- Reduces security administrator time involved in remediating exposures
- Reports on:
  - User profiles
  - Adopted authority
  - Trigger programs
  - Work Management
  - Auditing configuration
  - Network attributes
  - Integrated File System
  - Password Analysis
  - Over 70 reports



```
Profiles  Programs  JobD  IFS  Sysval  Comms  Libraries  Subsystem
Misc.    Ad-Hoc1    Ad-Hoc2

-----

Ver: 7.30      PowerSC Tools for IBM i Security Diagnostics
               @ Copyright IBM Corp. 2006-2016 All Rights Reserved      13:37:48
                                           CTCT005C

Profiles  Programs  JobD  IFS  Sysval  Comms  Libraries  Subsystem
Misc.    Ad-Hoc1    Ad-Hoc2

-----

:  1. Users Special Aut Status      :
:  2. Users w/Default Pwd          : nostics
:  3. Users Cmd Line Access        : s Reserved      13:43:23
:  4. Users Initial Pgm & Mnu      : CTCI005C
:  5. IBM USRPRF *NE Shipped       :
:  6. All Q Users                  :
:  7. USRPRF Pwd Exp *NE SYSVAL    :
:  8. USRPRF Not Signed On        :
:  9. USRPRF Not Owned b:         :
: 10. USRPRF NOT *PUBLIC:         User Profile not Signed on in xx Days
: 11. USRPRF Privately A:         :
: 12. USRPRF with NO Tex:         Run this Option: Y (Y=Yes, N=No)
: 13. GRPPRF Information:         :
: 14. User ATTN Pgm Info:         # of Days Not Signed On?: 090 (1 to 999)
: 15. All User Profiles:         :
: 16. All *ENABLEd Profi:         :
: 17. User Profile Owner:         :
: 18. Display All User P:         :
:.....:         F12=Cancel
:.....:
```

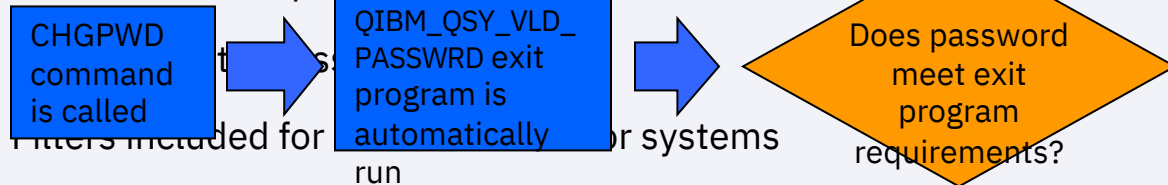
# IBM i Password Synchronization

## Enhanced protection through strict password criteria

Checks the password to see if it contains:

- Any words from a maintainable dictionary of disallowed words. Seeded with top 10,000 passwords found in reported breaches
- Previous passwords from all LPARs

Federated DB of profiles across all LPARs



- Server authentication entries updated
- Assures the security administrator that passwords being entered are not trivial
- Checks against the password rules of each system
- Fully audited

# IBM i Password Synchronization (continued)

## Enhanced protection through additional password checking

Checks the password to see if it contains:

- Any words from a maintainable dictionary of disallowed words. Seeded with the top 10,000 passwords found in globally reported breaches

- Originally written for customers unable to move from V5R4, it is useful

50 Most Used Passwords				
password pepper access starwars qwerty biteme dragon p***y baseball football	letmein monkey secret abc123 mustang michael shadow master jennifer hello	zaq12ws x jordan superma n harley abcd123 4 f*****e hunter f*****u trustno1 ranger	buster thomas tigger robert soccer f**k batman test pass killer	hockey george charlie andrew michelle love sunshine jessica a****le asdfgh

# Advanced Authentication

Limit access to applications/systems to properly authenticated users

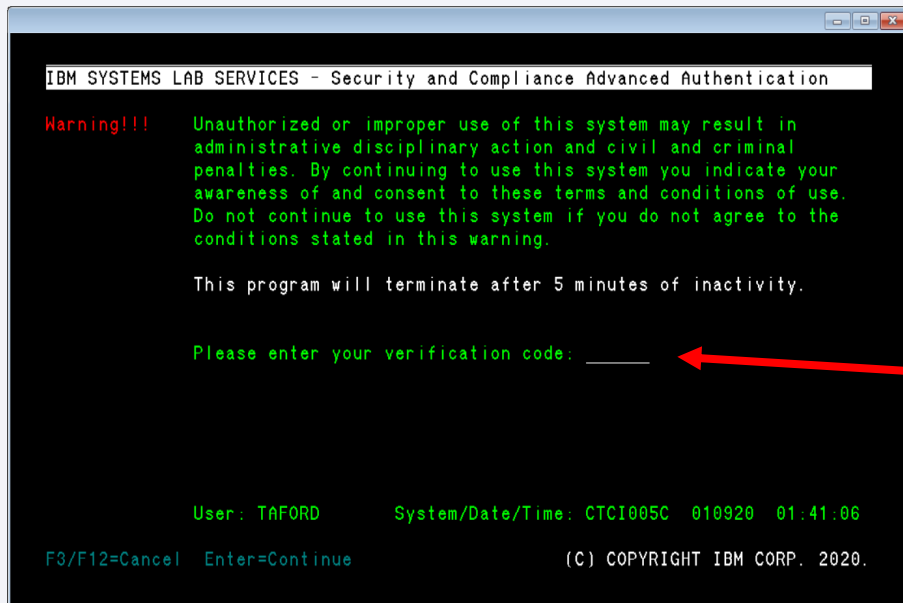
Generates highly secure RFC6238 based one-time passwords (TOTP) ensuring that only properly authenticated users are authorized access to critical applications and data.

IBM i based QR code generator

No internet connection required

Audit of registration and use

Use as a sign on application, password reset tool, service in own



# Access Control Monitor

## Monitor security deviations from application design

Ad hoc or scheduled reporting to check and report on application objects that are out of corporate security policy standards, data classifications, or other security related configurations

Prevents user application failures due to inconsistent access controls

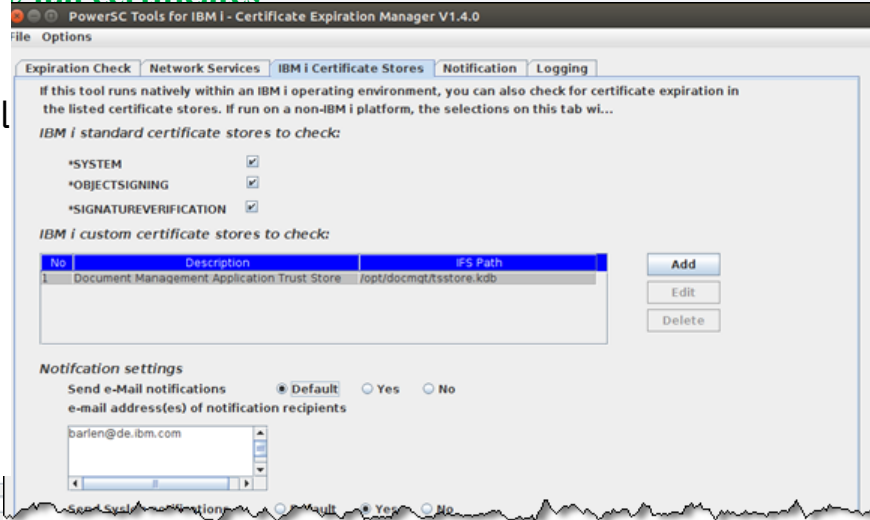
Object Authority Exceptions										
	KEY	LIBRARY	OBJECT	TYPE	USER	OBJECT AUTHORITY	OBJECT AUTHORIT STANDARD		OBJECT AUDIT VALUE	OBJECT AUDIT STANDARD
-	AUD CHG	BADINGB	XCLMERG	*FILE	-	-	-	-	*NONE	*CHANGE
-	AUT CHG	BADINGB	QQMQRYSRC1	*FILE	*PUBLIC	*EXCLUDE	*USE	-	-	-
-	AUT CHG	BADINGB	TEST2	*FILE	*PUBLIC	*CHANGE	*EXCLUDE	-	-	-
-	AUT CHG	BADINGB	TEST3	*FILE	*PUBLIC	*CHANGE	*EXCLUDE	-	-	-

- Monitors compliance of libraries, objects, and authorization Lists
- Customer extensible to allow automation of objects back into compliance

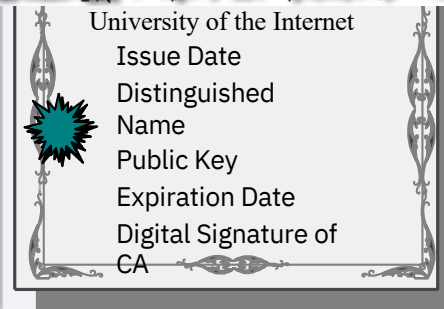
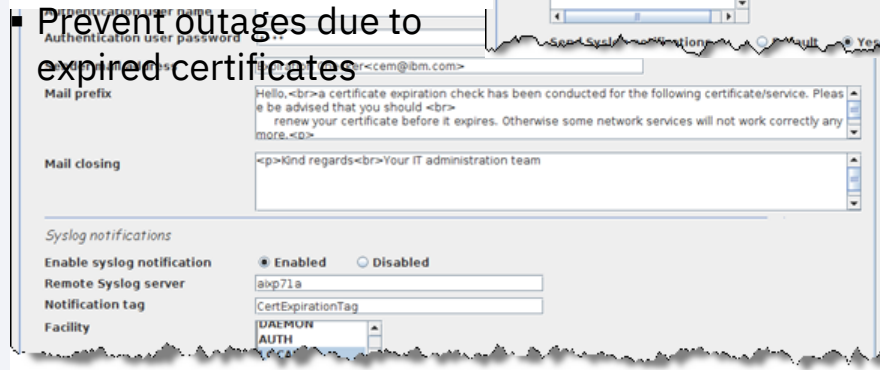
# Certificate Expiration Manager (CEM)

Simplifies the management of digital certificates

- Maintains a log of all expiration activities
- Sends notification via eMail and Syslog message.
- Easy to use configuration GUI is included for managing the XML settings.
- Runs on any platform that supports Java.



Prevent outages due to expired certificates



# Single Sign On (SSO) Suite

## Simplify SSO implementation reducing help desk costs

Suite of tools sold individually or à la carte with or without implementation services:

### Single Sign On (SSO) Suite for EIM

- ✓ EIM CL Commands
- ✓ EIM Populator
- ✓ EIM Management Utility
- ✓ EIM Based Password Reset
- ✓ EIM Based CRTUSRPRF
- ✓ Windows AD Profile Synchronization

### SSO Password Synchronization Tool

An effective alternative to manual configuration

The screenshot shows a Windows-style dialog box titled "Import EIM Entries from C:\Documents and Settings\Administrator\My Documents\Download...". It contains several sections for configuring the import of EIM entries from a CSV file.

**CSV File Entries:** A list box contains "Employee name", "Windows AD account", and "Series user profile". To the right, there are radio buttons for "Full Field" (selected), "First x chars", and "Last x chars". A "Number of characters" field is set to "1".

**Key Codes:** A section explaining field codes: "F = Full field", "Lx = Left x chars", "Rx = Right x chars", and "@x = using field number x in CSV list".

**Create EIM ID / Find EIM ID by Alias:** Two tabs are present. The "Find EIM ID by Alias" tab is active, showing fields for "EIM Identifier" and "EIM Description", each with a "Select" button and a "Define EIM Entry" button.

**Add Alias(es) for above EIM ID:** A section with "Select Field" and "Select Value" buttons, an "Alias" text field, an "Add EIM Alias" button, and a "Remove selected items" button.

**Add Associations for the EIM ID above:** A section with "Association type" (Source), "Registry" (CTC2003.IBM.COM), and "User" (with a "Select" button). It includes an "Add EIM Association" button and a "Remove selected items" button.

**Buttons:** At the bottom, there are buttons for "Generate Report ONLY", "Populate EIM", and "Cancel".

# And it all ties together...

From the Digital Trust segment of the IBM Security portfolio

- We can protect the DB2 database instances on i Series platforms
  - Using Guardium Activity monitor
  - This application performs Data Activity Monitoring (via S-TAPS)



# And it all ties together...continued

From the Threat management segment of the IBM Security portfolio.

We can tie the i Series to our SIEM platform for event correlation using SYSLOG Reporting Manager.

The manager sends along audit journal entries, history log events, custom events, IFS file change events, message queue events, and database table change events to a remote syslog / SIEM server via UDP or TCP protocol

# Thank you

Follow us on:

[ibm.com/security](https://ibm.com/security)

[securityintelligence.com](https://securityintelligence.com)

[ibm.com/security/community](https://ibm.com/security/community)

[xforce.ibmcloud.com](https://xforce.ibmcloud.com)

[@ibmsecurity](https://twitter.com/ibmsecurity)

[youtube.com/ibmsecurity](https://youtube.com/ibmsecurity)

© Copyright IBM Corporation 2020. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.